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

石黒正揮[†] 鈴木裕信[††]
村瀬一郎[†] 篠田陽一[†††]

近年，インターネット上のワーム感染などによる被害が相次いでいる．本研究では，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アドレスにおいて観測される不正なパケットの変化を分析することで，ワームなどのインターネット上の脅威を検知するための手法を提案する．インターネット上には，特徴の異なる多様な脅威が存在するため，異なる特徴量に基づく複数の分析手法を組み合わせて，多角的に分析することが重要である．本研究では，ワームの活動の周期性の変化に基づく異常検知手法と，感染ホスト数の増加と脆弱なポートへのワームの効率的な感染に着目した脅威の評価法を示す．これら時間と空間に関する対称的な特徴量に基づく新しい手法により，従来の検知手法を補完し，脅威検知の範囲を広げることができる．また，検出手法の特徴に応じて，検出された脅威の性質や原因を分析するための参考情報として利用することができる．

Internet Threat Analysis Methods Based on Spacial and Temporal Features

Masaki Ishiguro,[†] Hironobu Suzuki,[††] Ichiro Murase[†] and Yoichi Shinoda[†††]

Recently, network incidents caused by Internet worms has been increasing. We propose Internet threat analysis methods based on malicious packets observed at several IP's over the Internet. There exist various kinds of Internet threats with different natures and behaviors. Therefore it is important to analyze Internet threats based on several kinds of different approaches. We propose two methods based on periodical behavior of worms and based on increase of infected hosts and efficiency of worm infection. These two methods are based on temporal and spacial features and complement traditional detection methods for Internet threat detection. They also provide information for analyzing the nature and causes of threats from the new perspectives.

1. はじめに

近年，インターネット上のワームやボットなどの感染によるシステム障害，個人情報流出などの被害が相次いでいる．このような不正なコードの感染活動は，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（未使用のIPアドレス）に届くパケットによって観測することができる．ネットワークサービスを提供しないIPアドレスには，本来，ネットワークサービスの利用を目的とした外部からのアクセスは来るはずがないためである．このような不正なパケット（以下，不正パケットと呼ぶ）を観測することでインターネット上の脅威を検知することを目的としたインターネット定点観測システム（定点観測システムと呼ぶ）の開発が行われている[1)~6)]．定点観測システムは，自サイト内のトラフィックなどを観測するIDSとは異なり，インターネット上を広く複数のアドレスにおいて観測することにより，インターネット上での新種のワームの発生などの検知を目指している．

本研究では，インターネット上で観測される不正パケットの時系列データに対して周波数成分の変化に基づく検知手法と，不正パケットの送信元，送信先によって構成されるグラフの構造変化に基づき脅威評価する手法を提案し，従来の異常検知手法を補完して，イン

† 株式会社三菱総合研究所情報セキュリティ研究グループ
Information Security Research Group, Mitsubishi Research Institute, Inc.
†† 早稲田大学理工学術院
Faculty of Science and Engineering, Waseda University
††† 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

ターネット上の脅威を多角的に分析するための方法を提案する．

本論文の構成は以下のとおりである．2 章では，関連研究をまとめる．3 章では，インターネット脅威分析システムの全体構成についてまとめる．4 章では，提案する 2 つの脅威分析手法とその適用結果を示す．5 章では，提案手法の関係と利用法を示す．6 章では，グラフの構造に基づく脅威分析法に関する考察をまとめる．7 章で，本研究の成果をまとめる．

2. 関 連 研 究

インターネット上の脅威分析を目的とした定点観測システムは，不正パケットの観測方法と観測データの分析方法によって以下の節で示すとおり分類することができる．

2.1 定点観測法

不正パケットの観測方法は，観測するパケットに対する応答の有無およびセンサの配置方法によって分類できる．応答の有無に関しては，外部からのポートアクセスに対していっさい応答を返さない受動観測（passive monitoring）と，特定のパケットに対して応答を返し，その反応を観測する能動観測（active monitoring）がある．前者として，CAIDA telescope[1]，Internet Storm Center[2]，Internet Motion Sensor[7]，JPCERT/CC の ISDAS[6]，WCLSCAN[5]，DShield[3] などがあげられ．後者として，Princeton 大学の研究[8] や，Honeynet Project の Honeypot[9] などがあげられる．

一方，センサの配置方法については，連続した IP アドレスを観測する CAIDA telescope[1] などのような連続アドレス型と，不連続なアドレスを観測する Internet Storm Center[2] などのような分散アドレス型に分類することができる．連続アドレス型の場合，連続的な IP アドレスへのアクセスパターンから攻撃の種類を判別するのに有効であるが，ワームに多く見られる確率的な伝搬パターンを持つ攻撃に対しては，分散アドレス型の方が検知時間について性能が高いことが Johns Hopkins 大学の研究[10] によって示されている．

本研究では，受動型の分散アドレス配置型の定点観測を行い，脅威分析に必要なデータを SQL を用いて時間やセンサの種別，パケットの送信元，送信先などの条件を指定して柔軟に取得できる環境を構築している．

2.2 脅威分析手法

定点観測データの分析手法は，インターネット上の不正パケットの送信元を集団としてとらえ，集団の特徴に対する統計的な推測を行う集団特徴分析型と，送信元別のアクセスイベントの順列パターンなどから攻撃者の振舞いパターンに注目する振舞い分析型に分類できる．また，集団特徴分析型と振舞い分析型は，それぞれ特徴量自体に時系列情報を持つか否かで，時系列特徴量分析型と空間特徴量分析型（非時系列特徴量分析型）に分類される．

集団特徴分析型では，不正パケット数の時系列データから推定される特徴量と実際に観測される特徴量の統計的な偏差などを評価する．Zou らは，ワームの拡散モデルに基づき，インターネット上のワームの感染率をカルマンフィルタを用いて推定し，感染率の推定値が一定以上の値で収束する場合を脅威と見なす手法を提案している[11]．Lakhina らは，送信先に対するパケット数の時系列データに対して主成分分析を適用し，パケット頻度を主要成分と残差成分に分離し，残差成分（異常成分）の増減によって異常を検知する方法を提案している[12]．また，不正パケット数の時系列データから統計的な偏差（Z スコア）に対してベイズ推定を適用することにより危険度に対する推定値を学習する方法[13] や，パケット頻度の自己回帰分析による推定値からの分布の偏差に対してシャノン情報量に基づき変化点の検出を行う方法[14),15] など統計分布に基づく分析などがある．Wagner らは，不正パケットのアクセス先の分布をエントロピーで評価することにより，分布のランダム性や偏りに関する変化からワームの発生を検知する方法[16] を提案している．これらの手法は，時系列データから特徴量を推定し，観測値とのずれを評価しているが，個々の特徴量自体に時系列性を持たないため，ここでは空間特徴量分析型に分類する．

振舞い分析型に関しては，送信元別に観測される送信先ポートへのアクセスパターンや，それらのクラスタリングにより，これまでに観測されていない新しいパターンの発見を行うものがある．振舞い分析型のうち，空間特徴量分析型のものには以下のような方法がある．Theriault らは，送信元 IP 別に送信先ポートの分布に対して距離を定義することで，送信元に対するクラスタリングを行い，クラスタ構成の変化により異常を検知する方法[17] を提案している．能動観測データを用いたものには，TCP コネクション確立の有無を観測することで，ワーム感染の尤度を求める方法[18] や，送信元 IP アドレスごとに SYN パケットと FIN パケットの数を計測し，その SYN パケットと FIN パケットの差から攻撃を検知する方法[19] が提案されて

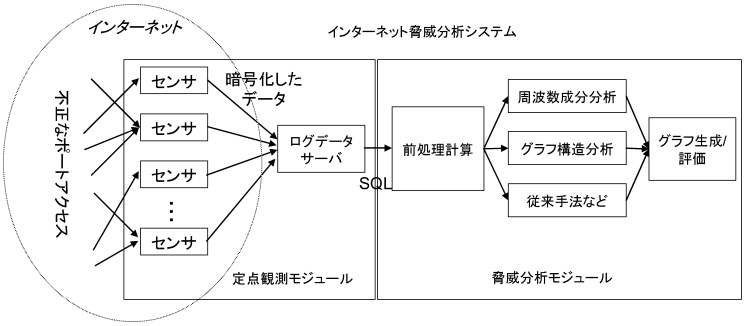


図 1 インターネット脅威分析システムの構成
Fig. 1 Structure of the Internet threat analysis system.

いる．一方，振舞い分析型で，時系列特徴量分析型には，送信元 IP アドレスごとに，送信元ポート番号と送信先 IP アドレスの関係を時間を追ってグラフ表示することにより，個々の送信元のパケット送信パターンを視覚的にとらえる研究[20] がある．

本研究では，集団特徴分析のうち特徴量自体に時系列情報を持つウェーブレット解析法と，空間特徴量分析で，集団特徴分析と振舞い分析の両方の性質を持つ不正パケットのグラフ構造分析に基づく手法について提案する．

3. インターネット脅威分析システムの構成

本研究で提案するインターネット脅威分析システムの構成を**図 1** に示す．

本システムは，不正パケットの観測および観測データを管理する定点観測モジュールと観測データに対して脅威分析を行うモジュールから構成される．インターネット上に配置した複数のセンサで観測された不正パケットはログデータサーバで管理され，脅威分析モジュールで必要となるデータは，SQL を用いて定点観測モジュールから取得し，グラフ構造分析，周波数成分分析や，従来手法であるベイズ推定法など複数の手法で分析した結果を出力する．

センサは，アクセスに対してはいっさい応答を返さない受動型の観測を行い，観測された各パケットについて**表 1** に示すデータを記録する．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 アドレスに到達するパケットを観測することで，本来，送信されるはずのないパケットを観測することができる．このようなパケットには，ワームが感染のために送信したパケット，送信元を改竄した DDoS 攻撃の応答パケット（Back Scatter），ネットワーク設定の不備により送信されるパケット，ポートスキャンなどが含まれる．各センサは，一定の時間間隔で，ログデータサーバに観測データを送信する．

表 1 観測されるデータの属性
Table 1 Target data.

パケットのアクセス時刻（年月日，時間）
プロトコル種別（TCP，ICMP，UDP）
送信元 IP アドレス
送信元ポート番号
送信先 IP アドレス
送信先ポート番号

グラフ構造分析では，送信元アドレスと送信先ポートの関係によって構成されるグラフからのインターネット上の脅威を評価する．周波数成分分析は，ウェーブレット解析を用いて，ワーム感染活動の周期性に関する変化を検知し，時系列グラフ表示を行う．これらの複数の手法による多面的な分析により，未知のワームなどインターネット上の脅威を分析する環境を提供する．

4. 脅威分析手法

本章では，インターネット上で発生する未知の脅威を多角的に分析するための方法として，以下に示す 2 つの異なる分析手法を示す．

(1) 周波数成分変化に基づく手法
(2) グラフ構造分析に基づく手法

これら 2 つの手法は，時間と空間に関する特徴量に基づく新しい手法で，従来の手法を補完することを目的としている．

4.1 周波数成分変化に基づく異常検知手法

ウェーブレット変換を用いて，時系列データに含まれる局所的な振動成分（周波数成分）の変化を時間軸上で検出することができる．離散ウェーブレット変換は，**図 2** に示すとおり，元データに対して，低い周波数を通すフィルタ（スケーリングフィルタ）と高い周波数を通すフィルタ（ウェーブレットフィルタ）を繰

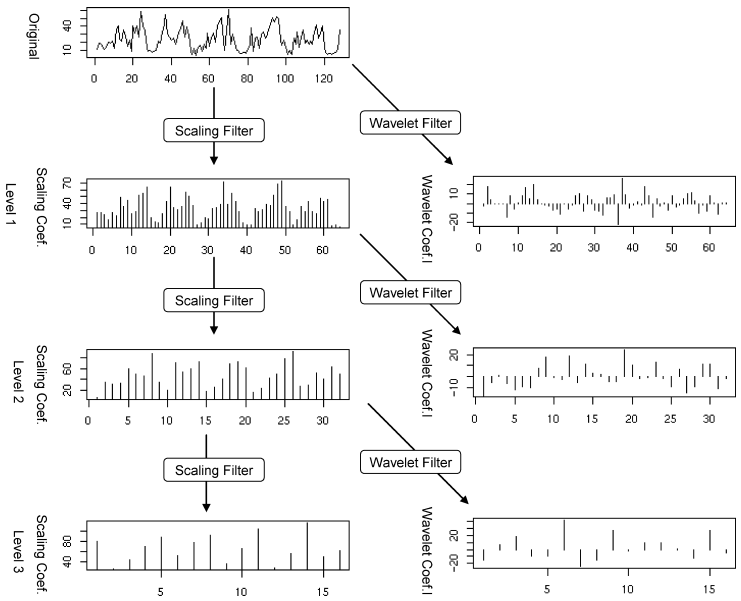


図 2 離散ウェーブレット変換の流れ
Fig. 2 Process of discrete wavelet transformation.

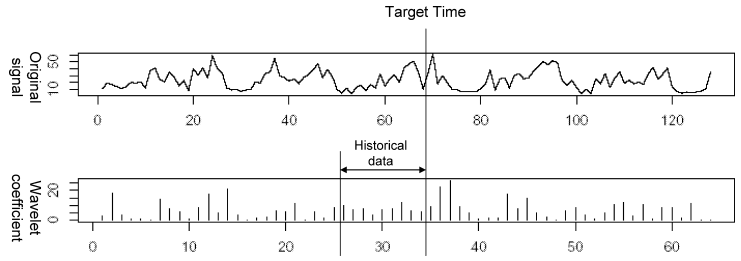


図 3 異常検出におけるウェーブレット係数
Fig. 3 Wavelet coefficients used for the anomaly detection.

り返し適用することにより時間周波数成分を求める．図 2 左上のグラフは，元データを示す．これに対して，スケーリングフィルタ，ウェーブレットフィルタを適用することにより，レベル 1 の 2 段目に示すスケーリング係数およびウェーブレット係数を求める．得られたスケーリング係数は，元データの 1/2 の時間解像度のトレンドを示し，ウェーブレット係数は，スケーリング係数からの変動を示す．以下同様にして，レベル i のスケーリング係数に対して，スケーリングフィルタおよびウェーブレットフィルタを適用することにより，単位時間に対して 2^{i+1} のスケールのトレンド成分および周波数成分の強度を求めることができる．レベルの値 i が大きいほど，低い周波数に対応する．

ワームの感染活動は時間帯，曜日など周期性を持つものが多い．このため，不正パケット数の時系列データには，さまざまな周期の振動成分（周波数成分）が観測される．このような周波数成分の変化をとらえることで，インターネット上のワームの構成比率や振舞いの変化など，不正パケット数の増減からでは検出が難しい変化を検知することができる．

ウェーブレット係数の絶対値は，局所的な周波数成分の強度を示している．本手法では，標準的なドビッシーウェーブレット（長さ 8）を用いたウェーブレット変換を行う．また，位相のずれにともなうウェーブレット係数の変動はノイズとなるため，ウェーブレット係数を被う包絡線を求め，ウェーブレット係数の変動を抑えた補正済みウェーブレット係数を求める．この係数を用いて評価対象時刻から過去一定期間の局所的なウェーブレット係数の平均値および標準偏差を用いて，評価時刻のウェーブレット係数が近い過去の分布における偏差（Z スコア）を求めることができる．**図 3** は，異常検出の対象時刻と，元データに対して得られた特定のレベルのウェーブレット係数のうち，異常検出に用いられる過去のデータの関係を示している．

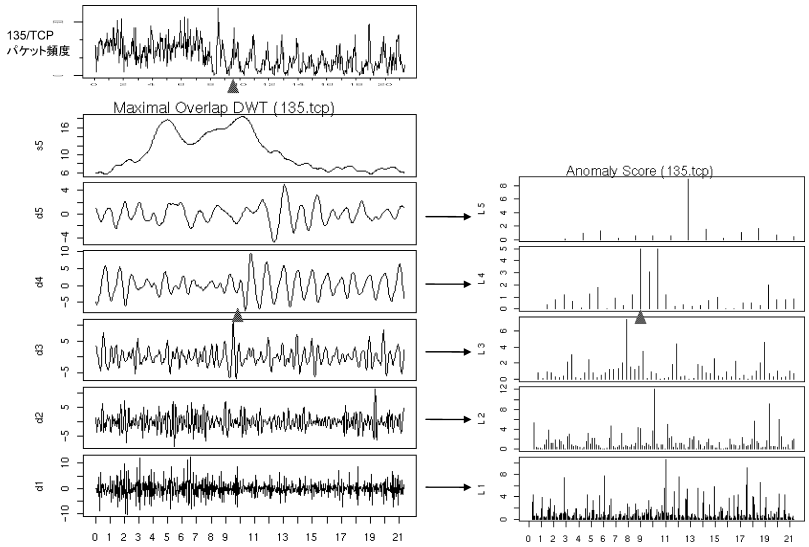


図 4 周波数成分異常検知手法の適用結果（135/TCP）
Fig. 4 Application result of the anomaly detection method based on frequency-component analysis (135/TCP).

レベル i の離散ウェーブレット変換によって得られるウェーブレット係数☆の系列を $\mathbf{w}_i = \{w_{i,1}, \cdots, w_{i,t}\}$ とする．分析対象時刻 t_0 に対して，近い過去の平均値を $M_i(\mathbf{w}_i)$ とする．ここで，レベル i の平均は，時刻 $t_0 - 1$ から過去 N_i 個の系列の平均として求めるものとする．

$$M_i(\mathbf{w}_i) = \sum_{t=t_0-1}^{t_0-N_i} |w_{i,t}|/N_i \qquad (1)$$

また，レベル i における近い過去の標準偏差（不遍推定量）を $SD_i(\mathbf{w}_i)$ とする．レベル i の標準偏差は，N_i 個の系列から求めるものとする．

$$SD_i(\mathbf{w}_i) = \sqrt{\sum_{t=t_0-1}^{t_0-N_i} (|w_{i,t}| - M_i(\mathbf{w}_i))^2/(N_i - 1)} \qquad (2)$$

レベル i のウェーブレット係数に対して，対象時刻における周波数成分の強度に関する，近い過去の周波数強度の分布における偏差（Z スコア）は以下のとおり定義することができる．

$$v_{i,t_0} = \frac{|w_{i,t_0}| - M_i(\mathbf{w}_i)}{SD_i(\mathbf{w}_i)} \qquad (3)$$

ワームなどの感染活動は多様であるため，特定の周波数に限定せず複数の周波数の Z スコアを用いて異常を検出する．ただし，高周波成分には，ノイズによる変動が多く含まれるため，最も周波数の高いレベル 1（2 時間解像度）の成分は除外し，レベル 2（4 時間），レベル 3（8 時間），レベル 4（16 時間），レベル 5（32 時間）の成分を対象として，いずれかの成分に大きな偏差が見られるときに異常と判断する．1 つの判定法は，時刻 t_0 における各周波数成分から求めた Z スコアの組 $\{v_{2,t_0}, v_{3,t_0}, v_{4,t_0}, v_{5,t_0}\}$ が，各レベル $2, \cdots, 5$ に指定した対応する閾値 $\{T_2, T_3, T_4, T_5\}$ のいずれかを超える場合に，異常と判定する．閾値は，発生頻度が稀であることを示す目安として 6.0 などを基準に，必要とする検知の感度から実験的に設定する．また，またもう 1 つの簡易な判定法として，Z スコアの組のうち最大値が指定した閾値 T を超えるときに異常と判断する方法を用いる．

4.1.1 事 例 実 験

本項では，具体的な観測データに対して本手法を適用した結果を示し，その特徴を示す．

図 4 は，2005 年 4 月 8 日から 4 月 30 日までの 135/TCP ポートの 1 時間単位の不正パケット数の時系列データに対して，本手法を適用した結果である．横軸は，経過日数を示す．左上のグラフは元の不正パケット頻度を表し，その下には，トレンド（s5），32 時間（d5），16 時間（d4），8 時間（d3），4 時間（d2），2 時間（d1）の周波数成分を抽出した時系列データを示す．右側のグラフは各成分に対応する異常検知結果を示す．

元の不正パケットは開始日から 9 日目ごろから典型

☆ 包絡線により補正したウェーブレット係数

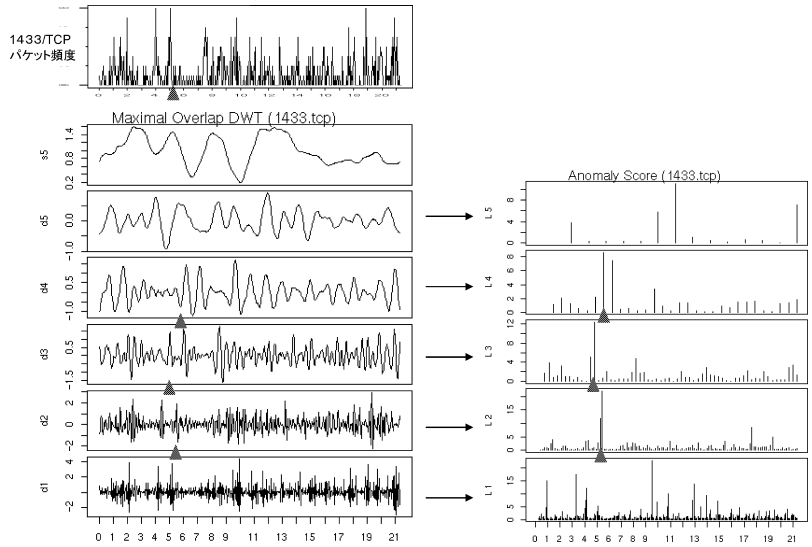


図 5 周波数成分異常検知手法の適用結果（1433/TCP）
Fig. 5 Application result of the anomaly detection method based on frequency-component analysis (1433/TCP).

的な 24 時間周期の振動が見られ，それより前の時期は不規則な頻度が確認される（グラフ中の三角形の印で示される位置）．

図 4 左側 d4 のグラフでは，16 時間（d4）周波数成分のグラフで，9 日目以降強い振動成分が確認でき，対応する右側のグラフでは，9 日目ごろに周波数成分の変化を検知したピークが確認され 16 時間周期成分の変化を示している．また，右側の周波数成分 2 時間（L1）のグラフを除く，各周波数成分のグラフからそれぞれ乖離度が最大のものを抽出すると，L2 グラフから 10 日目，L3 グラフから 8 日目，L5 グラフから 12 日が異常として検知される．これらはそれぞれ異なる要因の周波数成分変化と考えられるため，それぞれ異常と判断する．

図 5 は，2005 年 4 月 8 日から 4 月 30 日までの 1433/TCP ポートの 1 時間単位の不正パケット数の時系列データに対して，本手法を適用した結果である．

元の不正パケットの時系列データは全体的に不規則であるが，6 日目前後に変化が見られる．周波数成分を示す右のグラフでは，16 時間（L4），8 時間（L3），4 時間（L2）成分に強いピークが見られる．これらからは異なる周期性に関する変化が複数同時に起こっている可能性が推測される．しかし，正確な原因を特定するためには，パケットデータなどの詳細な分析が必要となる．

4.1.2 評価実験

本手法の性能を評価するために，実際の観測データを用いて False-Positive Ratio（FPR）および False-Negative Ratio（FNR）を求める．FPR は，誤検知率を表し，FNR は検知漏れ率を表す．FPR と FNR はトレードオフの関係にあり，双方の値が同時に小さいほど高い性能を示す．

不正パケットに基づく異常検知では，観測されるものはすべて不正なパケットであり，その中から脅威の高いものを検出することを目的とする．そのため，IDS やスパムメール検出のように真の正解を確認することは一般的に困難である．そのため，現実的に行える評価方法として，従来手法の不正パケットの増減により検知される異常を基準として，その前の一定期間あるいはその前後の一定期間で検知できるかによって評価する．

図 6 は，検知性能の評価法について示している（図は，2006 年 8 月の Windows サーバーサービス（ポート 139 番）のインシデント（MS06-040）が発生した時期を例としている）．横軸は，8 月 10 日からの経過日数を示している．グラフは，下から順に，不正パケット数，不正パケット数の各時刻の Z スコア（従来手法），本手法の検知スコアを示している．

正解として，インシデントの発生している期間と，インシデントのない期間を定め，各期間で本手法の検知結果と比較する．まず，不正パケット数の時系列データから Z スコア（「不正パケット数」の Z スコアのことであり，「周波数成分」の Z スコアではない）により急激な増加を検知し，「インシデント観測開始

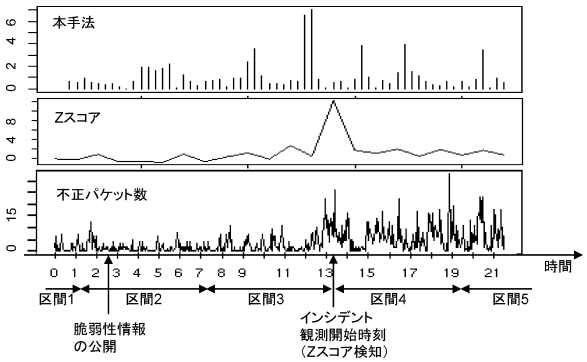


図 6 性能評価方法（Windows サーバーサービスのインシデントの例）
Fig. 6 Performance evaluation method (An example incident of Windows server service).

時刻」とする．図 6 に示すインシデントの例では，横軸の経過日数 2 日目あたりに脆弱性情報が公開され，経過日数 13 日目あたりからパケット数の増加によるインシデントが検知されている．インシデントの正確な発生時期は特定できないが，図の例では，脆弱性情報が公開された経過日 2 日目から，パケット数の増加により検知された経過日 13 日目の間に，異常を検知されることが期待される．

本評価では，(a) 早期検知の性能と (b) 遅い検知を含む緩い性能評価の 2 通りの評価を行う．脆弱性情報の公開から従来手法によるインシデントの検知までの期間のずれ（図の例では約 10 日間）を考慮し，インシデント観測開始時刻前の 7 日間を，早期検知の評価においてインシデントを検知すべき期間（図中「区間 3」に該当）と定める．また，時間軸を 7 日単位の区間に分け，インシデントを検知すべき期間以外の期間を，危険なインシデントのない期間と仮定する．このようにして正解を決めた各区間において，本手法の検知結果をもとに評価する．一方，(b) 緩い性能評価では，インシデント観測開始時刻の前後 7 日間を検知すべき期間（図中「区間 3」と「区間 4」に該当）とし，それ以外を「インシデントなし」とした場合について評価する．

センサにより不正パケットの増加が確認されない場合や，不正パケットの増加からの検知が難しいインシデントが存在するため，一般には，正解となるインシデントの発生期間を特定することは難しいが，本評価では，統計的な傾向性を確認することを目的として，不正パケットの増加が見られない時期を，「インシデントなし」と見なす．

評価実験は，2006 年 8 月から 12 月までの期間で，5 つのセンサ別に，パケット数が上位 7 つのポートに対して行った．本手法を，42 日単位の時系列データに対して適用し，周波数成分が 4 時間，8 時間，16 時間，32 時間のそれぞれについて，この期間で補正済みウェーブレット係数が最大の値を示すものを異常と判定した．**表 2** は，センサ全体のインシデント有無と警報有無の事例数を示している．**表 3** は，センサ全体

表 2 異常検知事例数（センサ全体）
Table 2 The number of samples of anomaly detection evaluation.

(a) インシデント観測開始前 7 日間

		インシデント		
		あり	なし	計
警報	あり	25	43	68
	なし	4	66	70
	計	29	109	138

(b) インシデント観測開始前後 7 日間

		インシデント		
		あり	なし	計
警報	あり	27	27	54
	なし	3	81	84
	計	30	108	138

表 3 異常検知性能
Table 3 The performance of the anomaly detection method.

(a) インシデント観測開始前 7 日間

センサ	FPR	FNR
全体	39%	14%
センサ A	41%	18%
センサ B	42%	20%
センサ C	47%	0%
センサ D	33%	17%
センサ E	33%	0%

(b) インシデント観測開始前後 7 日間

センサ	FPR	FNR
全体	25%	10%
センサ A	31%	8%
センサ B	21%	20%
センサ C	27%	0%
センサ D	17%	17%
センサ E	20%	0%

および各センサの FPR および FNR を示している．

表 3「(a) インシデント観測開始前 7 日間」の結果は，不正パケットの増加によって特定できるインシデント観測開始時刻よりも早期に検知する場合の評価を行っているため，FPR は 39%，FNR は 14%と検知性能はあまり高くはない．表 3「(b) インシデント観測開始前後 7 日間」の結果は，検知評価を前後 7 日間の期間に条件を緩めているため，(a) よりも良い結果を示している．

本手法は，不正パケットの増加からでは検知が困難なものを周波数成分の変化という従来とは異なるアプローチで早期に検知することを目的としたもので，不正パケットの増減による検知手法と比べて，検知できるインシデントの性質が異なる．したがって，本手法を補完的に利用することで，不正パケットの増加による手法で検知できないインシデントを検知するために利用することが考えられる．

4.2 グラフ構造分析に基づく脅威評価手法

本節では，定点観測システムによって観測される不正パケットの送信元および送信先の関係によって構成されるグラフの構造からインターネット上の脅威を分析する方法について示す．ワーム感染ホストの増大は，送信元 IP アドレスの増加によってとらえることができる．さらにそれを拡張し，脆弱性の高いポートへのワーム感染の効率性の観点を考慮した脅威分析法を示す．

定点観測システムによって観測される不正パケットの主な原因はワームからの感染パケットと考えられる[21]．ワームによるインターネット上の脅威は，(1) 感染自体の脅威と，(2) 感染後にワームから受ける被害に分けられる．感染後にワームから受ける被害は，ファイルの削除，個人情報の送信など定性的な要素が大きく，数理的に評価することは困難である．また，感染の脅威と感染後の被害の関係は独立性が高く，定点観測システムで観測されるワームの感染活動から感染後の被害を推論することは原理的に困難である．したがって，本研究では，ワームの感染力の強弱によるインターネット上の脅威を評価の対象とする．

通常，感染の脅威の評価においては，観測される不正パケット数自体よりも，不正パケットの送信元の数が重要である．なぜなら，不正パケットの送信元の数が多ければ，実際に多くのホストにワームが感染したことを示しているが，観測されるパケット数自体が多いだけでは，感染力の弱い少数のワームが多くのパケットを送信している場合があるためである．

図 7 は，一定時間の観測パケットを，送信元 IP アドレスと送信先ポート番号の間のアクセス関係によりグラフ表示したものである．図の左側（図中 “Source IP Addresses（Renumbered）”）には送信元 IP に対応するインデックスを並べ，右側（“Destination Port Numbers”）には，送信先ポート番号を並べたものである．この例では，ポート 1433（MS SQL サービス），21（ftp），80（http）は，多くの異なる送信元 IP アドレスからのアクセスを受けていることが分かる．この事例は，ポート 1433 番への感染攻撃を行う spida ワームの感染が活発化し，インターネット上の脅威が高い時期を示している．

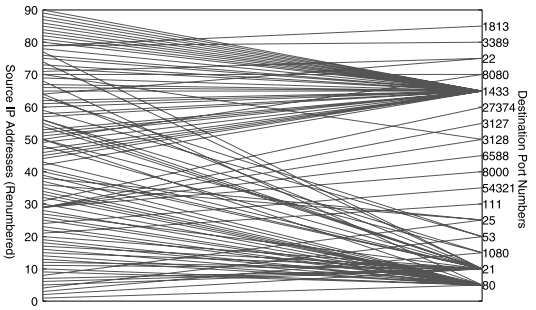


図 7 送信元と送信先ポートのアクセスグラフの構造
Fig. 7 Access graph between sources and destinations.

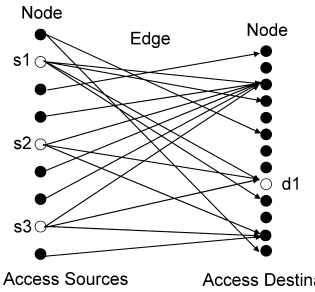


図 8 送信先 d1 と送信元ノードの関係
Fig. 8 Relation between destination d1 and several sources.

このようにあるポートへの不正パケットの送信元の数から脅威を評価することができる．さらにこれを拡張し，仮に送信元ごとにワームの感染力によって決まる脅威の高さ（脅威値と呼ぶ）が分かっていると仮定すれば，送信先が受ける脅威は，送信元の脅威値の総和で評価することができる．**図 8** は不正パケットの送受信の関係をグラフで示したものとする．送信先ノード d1 が受ける脅威は，送信元 s1，s2，s3 の脅威値の和によって評価できる．

一方，特定のポートに重大な脆弱性が存在すれば，そのポートを狙うワームの感染数が増大する傾向があることから，脆弱性の高いポートほど，ワームから

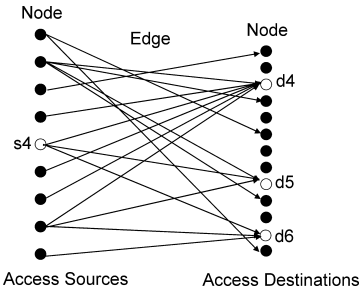


図 9 送信元 s4 と送信先ノードの関係
Fig. 9 Relation between source s4 and several destinations.

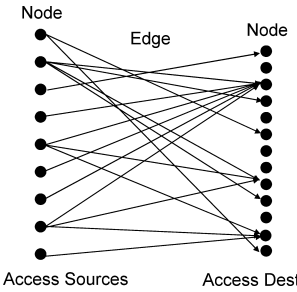


図 10 ポートアクセスのネットワーク上のグラフ
Fig. 10 Graph of port accesses on a network.

脅威を受ける傾向が高い．ワームの感染力は，脆弱なポートを攻撃する方が高くなるため，仮に送信先のポートの脆弱性が分かっていれば，送信元のワームの脅威は，送信先が受ける脅威（脆弱性）の和によって評価することができる．**図 9** のグラフでいえば，送信元 s4 の脅威は，送信先 d4，d5，d6 が受ける脅威の和として評価することができる．

以上の 2 つの関係のうち，一方は，送信元の脅威値を仮定して，送信先が受ける脅威値を評価し，もう一方は，送信先が受ける脅威値を仮定して，送信元の脅威値を評価する．この関係をまとめると以下のようになる．

送信元の脅威と送信先が受ける脅威の関係：

関係 1 送信先（のポート）が受ける脅威は，送信元の（ワームの）脅威の総和で評価できる．

関係 2 送信元の（ワームの）脅威は，送信先（のポート）が受ける脅威（脆弱性）の総和で評価できる．

送信元と送信先に対して任意の脅威値を初期値として設定し，上記の関係 1，2 を交互に繰り返し適用することで脅威値が収束した場合，不正パケットのグラフの構造から評価される脅威値を示している．このようにして求めた脅威は，感染ホスト数の増加とワームによる脆弱なポートへの効率的な攻撃という観点から，ワームの感染力に基づく脅威を評価していると考えることができる．また，以上のようにして評価される脅威値は，インターネット上の一種の脅威の高さを定義していると考えることができる．

次項では，漸化式の関係を固有値問題に変換することにより初期値を与えずに脅威値を計算する方法を示す．

4.2.1 脅威の計算法

不正パケットのネットワーク上でのグラフの構造を**図 10** のようなグラフによって表現する．送信元はイ

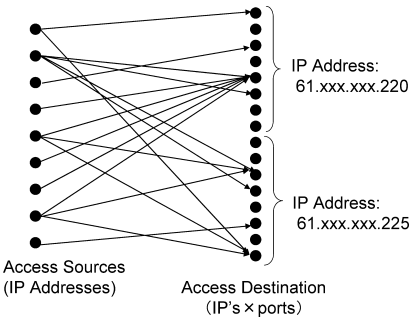


図 11 ポートアクセスのグラフ（送信先が複数 IP アドレス）
Fig. 11 Graph of port accesses on a network (Multiple destination IP addresses).

ンターネット上の IP アドレスによって決まるノードである（図 10 中の “Access Sources”）．送信先は定点観測システムのポート番号によって決まるノードである（図 10 中の “Access Destination”）．また，送信元から送信先へのアクセスの有無をグラフのエッジ（“Edge”）として表現する．このとき，観測されるアクセスは，センサ外の IP アドレスからセンサのポートへのアクセスのみである．また，送信元と送信先のノードの集合には重複はない．これらのことからアクセスグラフは 2 部グラフとなる．定点観測システムのセンサの IP アドレスが複数ある場合は，**図 11** で示すようにセンサの IP アドレスごとにポート番号を区別したものを送信先ノードとすることで，自然に拡張できる．

これらの関係を一般化して定義する．送信元のノード i の脅威レベル t_i を組にしたベクトル，および送信先のノード j がさらされる脅威レベル v_j を組にしたベクトルを考え，それぞれ $\mathbf{t}$，$\mathbf{v}$ と定義する（以下，送信元脅威ベクトル，送信先脅威ベクトルと呼ぶ）．

$$\mathbf{t} = (t_1, t_2, \cdots, t_n) \quad (4)$$

$$\mathbf{v} = (v_1, v_2, \cdots, v_m) \quad (5)$$

このとき，前述の関係 1 から，送信先 j がさらされる脅威 v_j は，送信元 i の脅威 t_i に，送信元 i から

送信先 j へのアクセスのエッジの重み $w_{i,j}$ によって重み付けした総和として式 (6) のように定義できる．

$$\begin{cases} v_1 = c_1(w_{1,1}t_1 + w_{2,1}t_2 + \cdots w_{n,1}t_n) \\ \quad \cdots \\ v_m = c_1(w_{1,m}t_1 + w_{2,m}t_2 + \cdots w_{n,m}t_n) \end{cases} \tag{6}$$

ただし，c_1 は，本項で後述する固有方程式を解くことにより決まる係数である．

エッジの重み $w_{i,j}$ は，送信元 i からのアクセスが，送信先 j に与える脅威にどの程度影響するかをもとに定義する．ここでは，ワームからのアクセスの性質を考慮し以下のように定義する．ワームからのアクセスは，同一の送信元から慢性的に送信されるものよりも，感染力の強いワームの感染拡大により新たな送信元から来るアクセスの方が脅威が高い．そのため，連続する 2 つの観測期間を前期と後期とし，前期にはアクセスはなく，後期にアクセスが発生した場合は，新たに感染したワームからの攻撃と見なして 1 とし，それ以外の場合は 0 とする．それ以外の場合とは，前期，後期の両方からのアクセスがあるような慢性的なアクセスがある場合，前期にアクセスがあり，後期にアクセスが止む場合，前期も後期もアクセスがない場合の 3 通りである．

次に，前述の関係 2 に基づき，送信元のノード j の脅威 t_j について考える．脅威 t_j は，送信先 i がさらされる脅威 v_i に，上記で定義したエッジの重み $w_{j,i}$ をかけたものの総和をとり，係数 c_2 を用いて，式 (7) のように定義できる．

$$\begin{cases} t_1 = c_2(w_{1,1}v_1 + w_{1,2}v_2 + \cdots w_{1,m}v_m) \\ \quad \cdots \\ t_n = c_2(w_{n,1}v_1 + w_{n,2}v_2 + \cdots w_{n,m}v_m) \end{cases} \tag{7}$$

係数 c_2 は，c_1 と同様に，後述する固有方程式を解くことにより決まる．

関係式 (6) は，送信元脅威ベクトルから送信先脅威ベクトルを求める漸化式を表し，関係式 (7) は，送信先脅威ベクトルから，送信元脅威ベクトルを求める漸化式を表している．送信先脅威ベクトルおよび送信元脅威ベクトルの初期値として任意のベクトルを選び，関係式 (6) および (7) を漸化式として交互に用いて計算を繰り返す．その結果収束したベクトルが送信先脅威ベクトルおよび送信元脅威ベクトルである．

この繰返し計算を無限回行った結果得られる収束解は，以下のように固有値ベクトルの計算により求められる．上記で定義した送信元から送信先へのアクセスの重みを，行列 (8)（アクセス行列と呼ぶ）として定義する．

$$W = \begin{pmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,m} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,m} \\ \vdots & & & \vdots \\ w_{n,1} & w_{n,2} & \cdots & w_{n,m} \end{pmatrix} \tag{8}$$

関係式 (6)，および関係式 (7) を，行列 W を用いて表現すると以下のとおりである．

$$\mathbf{v} = c_1 \underset{m\times n}{{}^tW}\ \mathbf{t} \tag{9}$$

$$\mathbf{t} = c_2 \underset{n\times m}{W}\ \mathbf{v} \tag{10}$$

ただし，行列 ${}^tW$ は，行列 W の転置行列で，各行列の下に記した $m \times n$ などは，行列の行数と列数を示している．

これらの関係式を変形すると以下の固有方程式が得られる．

$$\mathbf{v} = c_1c_2 \underset{m\times m}{{}^tWW}\ \mathbf{v} \tag{11}$$

$$\mathbf{t} = c_1c_2 \underset{n\times n}{W{}^tW}\ \mathbf{t} \tag{12}$$

この固有方程式より，送信先脅威ベクトル $\mathbf{v}$ は，サイズ m の正方行列（$\underset{m\times m}{{}^tWW}$）に関する固有値 $\frac{1}{c_1c_2}$ の固有ベクトルとなり，送信元脅威ベクトル $\mathbf{t}$ は，サイズ n の正方行列（$\underset{n\times n}{W{}^tW}$）に関する固有値 $\frac{1}{c_1c_2}$ の固有ベクトルとして求めることができる．特に，$\underset{m\times m}{{}^tWW}$，$\underset{n\times n}{W{}^tW}$ は，その要素がすべて正であれば，Perron-Frobenius の定理[22] から最大固有値の固有ベクトルはすべて正となる．よって，送信先の脅威ベクトル $\mathbf{v}$ と送信元の脅威ベクトル $\mathbf{t}$ の解が一意に求まる．したがって，上記の漸化式による脅威値の算出は，固有値問題に変換されるため，漸化式の脅威値に対する初期値の設定は必要なくなる．

インターネット上のワームによる不正パケットは，送信先を確率的に選択するため，すべての送信元から送信先に対してランダムな少数の不正パケットが存在すると仮定できる．これらの不正パケットに対応して，アクセス行列 W のすべての要素に微少量 δ（$\ll 1$）を加えれば，すべての要素が正のアクセス行列を定義できる．これにより，式 (11) を解いた送信先脅威ベクトルの要素はすべて正となる．固有ベクトルとして，単位ベクトルを選べば，送信先脅威ベクトルの要素は 0〜1 の間の値となる．

4.2.2 実　　験

アクセスグラフに基づく脅威の評価法を，実際のイ

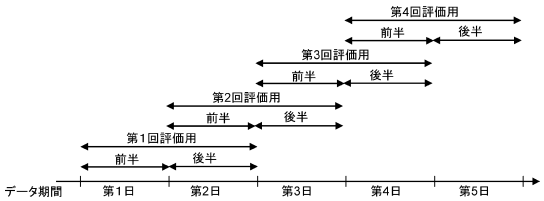


図 12 脅威評価におけるデータ期間の使い方
Fig. 12 Data usage for evaluating threats.

ンシデントの発生期の観測データに対して適用し，本手法の実用性，有効性を検証する．

本研究では，インターネット上の脅威を，感染力の強いワームによってホストがさらされる脅威として定義した．ワームの感染力は，攻撃対象となる脆弱性を持つホストのインターネット上での分布や，ワームの感染先探索戦略によって決まる．インターネット上のこれらの情報全体を知ることは困難である．そこで，本実験では，JPCERT/CC などによって公表された注意勧告から深刻なインシデントが発生した時期をインターネット上の脅威が高いものと仮定し，本手法によって求めた脅威レベルと比較する．

過去のデータからの機械学習を用いた評価手法の場合，学習に用いた訓練データと評価用のテストデータを分けて性能評価を行う必要がある．本手法では，機械学習を用いておらず，評価結果が過去のデータに依存しないため，訓練データとテストデータを分けた評価実験は必要ではない．

(1) MS SQL に関するインシデント

ここで評価対象とするデータは，JPCERT/CC から MS SQL の脆弱性を狙ったポート 1433 番への攻撃に対する注意勧告（JPCERT-AT-2005-0006）が出された 2005 年 7 月 9 日から 7 月 13 日までの 5 日間の TCP アクセスである．

5 日間の観測データを，**図 12** に示すように，2 日間のデータを 1 組として，1 日ずつずらした 4 回分のデータとして本手法を 4 回適用する．各 1 回の適用（図中 “第 1 回評価用”，“第 2 回評価用”，...，“第 4 回評価用” の各回）においては，前期 1 日（図中 “前半”）と後期 1 日（図中 “後半”）を用いて前項で定義したとおりアクセス行列を求める．つまり，7 月 10 日の適用結果は，7 月 9 日と 7 月 10 日の 2 日のデータを用いてアクセス行列を求め，7 月 11 日の適用結果は，7 月 10 日と 7 月 11 日の 2 日のデータを用いてアクセス行列を求めるというように順に 4 回適用する．

表 4 は，本手法を 4 回適用した結果得られた脅威レベルのうち上位 10 位を示している．表 4 中の “port” は，ポート番号，“count” は，ポートへのアクセスパケット数（当日のパケット数から，送信元，送信先が同じ前日のパケット数を差し引いたもの），“threat” は本手法で求めたポートがさらされる脅威のレベルを示している．

表 4 ポート 1433 インシデント時の脅威計算結果の上位 10 件
Table 4 Top 10 list of threat levels for the port 1433 incident.

July 10			July 11			July 12			July 13		
port	count	threat	port	count	threat	port	count	threat	port	count	threat
135	1031	0.627	135	1038	0.789	135	885	0.792	135	1057	0.636
445	1121	0.472	445	822	0.378	445	820	0.432	1433	346	0.331
12345	10	0.163	139	208	0.160	1433	222	0.233	445	739	0.305
139	232	0.159	1433	159	0.130	139	219	0.195	2745	6	0.148
1433	115	0.132	12345	13	0.109	9898	7	0.089	139	204	0.135
3410	8	0.123	901	14	0.109	1024	2	0.085	2100	3	0.111
901	9	0.123	3410	11	0.087	4899	64	0.078	8080	3	0.111
22	12	0.112	3389	6	0.087	3306	19	0.064	8535	3	0.111
3090	7	0.112	3306	18	0.087	2100	1	0.064	25	6	0.111

表 4 では，発生したインシデントに対応するポート 1433 番の脅威のレベルは，7 月 10 日から 7 月 13 日の順に，0.132，0.130，0.233，0.331 と増加している．また，他のポートと比較した脅威のランクは，7 月 10 日から 7 月 13 日にかけて，5 位，4 位，3 位，2 位へと上昇している．

本実験では，ポート 1433 番に関するインシデントの存在が確認されている時期を対象としているため，定常的に不正パケットの多い 445 番，135 番ポートよりも，1433 番ポートの脅威が高くなることが期待される．表 4 の 7 月 13 日の結果では，不正パケット数については，ポート 445 番よりポート 1433 番が少ないにもかかわらず，脅威レベルではポート 1433 番の方がポート 445 番より高いため，不正パケット数の増加よりも，本手法の脅威レベルの方がポート 1433 番の脅威をよくとらえている☆．一方，135 番ポートに関しては，1433 番ポートよりも高い評価値となっている．これは，本手法では，グラフの構造以外に，不正パケット数自体も脅威値に影響を与えるためであると考えられる．アクセスグラフのウェイトを最適化することで，不正パケット数よりもグラフ構造を重視した評価を行うことで改善できる可能性がある．

表 4 では，7 月 10 日のポート 12345 番（Amitis.B バックドア），7 月 12 日のポート 9898 番（Win32.Dabber.B ワーム），7 月 13 日のポート 2745 番（Bagle ワームのバックドアを利用する Agobot ボットネットワーム）は，不正パケット数が少ないにもにもかかわらず脅威レベルは上位に位置している．これらの事例についても，従来の不正パケット数によるも

☆ 実際には，インターネット上の真の脅威の有無（正解）は，完全には知りえないため，あくまでも脅威の高いインシデントが確認された時期の観測データに対する比較結果のみ示すことができる．

表 5 ポート 139 インシデント時の脅威推定結果の上位 10 件
Table 5 Top 10 list of threat levels on port 139 incident.

June 9			June 10			June 11			June 12		
port	count	threat	port	count	threat	port	count	threat	port	count	threat
135	2551	0.954	135	2174	0.883	135	2834	0.879	135	1906	0.846
445	751	0.209	445	1008	0.227	445	1308	0.244	445	989	0.249
1433	140	0.078	1080	4	0.104	12345	11	0.085	139	242	0.106
4899	43	0.052	44599	8	0.099	139	257	0.081	42857	2	0.102
1521	1	0.052	10589	4	0.099	21	4	0.077	4899	46	0.076
8535	1	0.052	8080	2	0.070	1433	142	0.065	143	1	0.076
8536	1	0.052	4899	47	0.070	44599	3	0.064	3306	9	0.076
2100	3	0.052	22	23	0.070	10589	3	0.064	1256	3	0.076
22	10	0.052	25	10	0.070	11524	2	0.064	2419	1	0.076
143	1	0.052	3306	4	0.070	42857	2	0.064	6346	3	0.076

のよりも本手法の脅威値の方がポート 12345 番，ポート 9898 番の脅威を高く評価している．

(2) Windows ファイル共有に関するインシデント

ここで評価対象とするデータは，IPA によって公開された注意情報[23] で，Windows ファイル共有で利用されるポート TCP/139 番に対してボットネットによる攻撃に関するインシデントで，2005 年 6 月 8 日から 6 月 12 日までの 5 日間である．本実験でも，(1) の実験と同様に，2 日間のデータを 1 組として本手法を 4 回適用した．**表 5** は，本手法を適用した結果で，脅威の高いポートを順に上位 10 位を示したものである．表中の “port”，“count”，“threat” は，(1) に示したものと同様である．

本結果では，インシデントの Windows ファイル共有に該当するポート 139 番は，最初の 2 日の脅威レベルは，順に 0.029（ランク 20 位），0.055（ランク 33 位）で，値が小さいため，表 5 の上位 10 位には現れない．しかし，6 月 11 日，6 月 12 日の適用結果では，脅威レベルは，0.081，0.106 と上昇し，脅威ランクは 4 位，3 位へと上昇している．

表 5 では，6 月 11 日から 6 月 12 日にかけて不正パケット数は減少しているにもかかわらず，脅威値は上昇している．脅威の高いインシデントが発生した時期を対象としているため，本実験においても不正パケット数によるものよりも本手法の脅威値の方が良い結果を示している．

5. 提案手法の関係と利用法

インターネット上には，性質や振舞いの異なるさまざまなワームによる脅威が存在する．これら特徴の異なる多様な脅威に対応するためには，複数の手法を組み合わせて，多角的に分析することが必要である．

本論文では，従来の不正パケットの増減による手法[13] などでは検知が難しい変化をとらえるための 2 つの手法を示した．提案手法は，従来の検知手法を補完し，脅威検知の範囲を広げるために利用できるが，これらだけであらゆる種類の脅威に対して十分に対応できるとはいえない．しかし，提案した 2 つの手法は，それぞれ時間と空間に関する対称的な特徴量に基づく新しい検知方法を提供し，それぞれの手法に応じて，検出された脅威の特徴を分析するために役立つ．

提案した 2 つの手法は，以下のような特徴と問題点を持ち，検知できる脅威の範囲に違いがある．

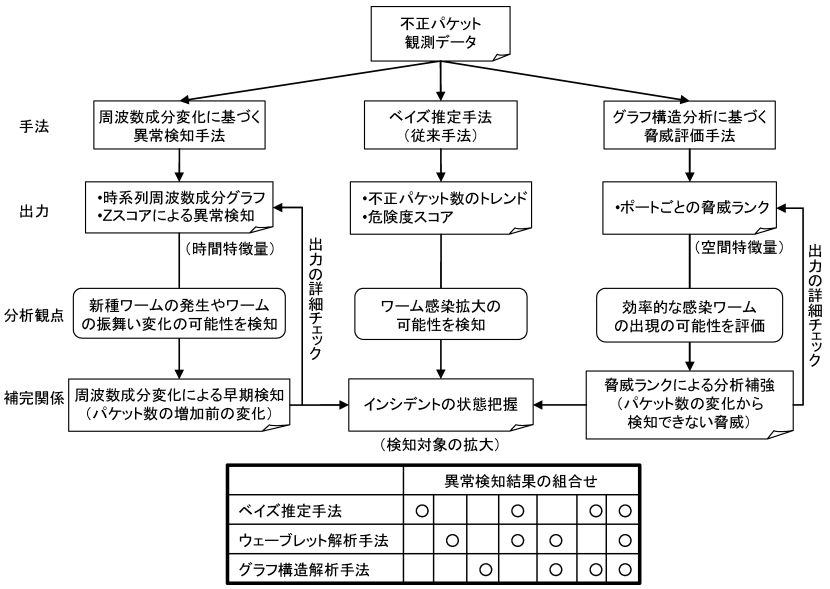
(1) 周波数成分変化に基づく異常検知手法（周波数成分分析法）
不正パケットの増加では検知が難しい，ワームなどの活動の周期性の変化を検知する．これによりインターネット上のワームの構成比率の変化や振舞いの変化を検出する．不正パケットが増加する場合でも，周波数成分に変化が少なければ検知しにくい場合がある．また，不正パケットの確率的変動により，高い周波数成分において脅威とはならない変化に反応することがある．

(2) グラフ構造分析に基づく脅威評価手法（グラフ構造分析手法）
感染ホスト数の増加と脆弱なポートへの攻撃の効率性に基づき，不正パケット数の増加ではとらえにくい，ワームの感染力に基づく脅威を評価する．1 つの攻撃元から複数の脆弱性の高いポートに同時に攻撃するパケットデータの影響度が大きいため，グラフの構成に用いるデータ量全体が少ない場合，評価結果の変動が大きくなるという問題がある．

このような特徴を考慮して，提案手法と従来の不正パケットの増減による検知手法[13] を組み合わせた利用法について**図 13** に示す．

不正パケットの観測データは，提案手法である周波数成分分析法とグラフ構造分析手法および従来手法であるベイズ推定法を用いて異常検知を行う．周波数成分分析法では，周波数成分の Z スコアが，一定の閾値を超える場合に異常と判断する．グラフ構造分析手法では，ポートの脅威ランクが一定の閾値以上に上昇した場合に，異常と判断することができる．

それぞれの手法は，異常検知結果と特徴量を視覚的に表示したグラフを出力する．これらの手法の 1 つでも異常検知があれば，総合的に異常と判断する．一方，各手法の出力は，インターネット上で発生している脅威の性質や種類の分析の参考情報として利用できる．周波数成分分析法の出力からは，新種のワームの発生やワームの振舞い変化の可能性などを推測することができる．グラフ構造分析手法の出力からは，効率的に感染する脅威の高いワームの出現の可能性を評価することができる．また，ベイズ推定手法からは，ワーム



	異常検知結果の組合せ						
ベイズ推定手法	○			○		○	○
ウェーブレット解析手法		○		○	○		○
グラフ構造解析手法			○		○	○	○

図 13 脅威検知手法の関係と利用法
Fig. 13 Relationship and usage of threat detection methods.

の感染拡大によるインシデントの活発化を推測することができる．

複数の手法で同時に異常検知があった場合には，その組合せに応じてインシデントの状態を推測するための参考とすることができる．たとえば，周波数成分分析法とベイズ推定法の両方から検知があった場合，インターネット上のワームの振舞い（構成比率など）の変化があり，しかも，すでにインシデントが拡大していることなどが推測される．

このような複数の手法を組み合わせることで，インターネット上のインシデントの状態を深く把握することが可能となり，脅威の性質や原因の分析に役立てることができる．

6. 考　　察

グラフ構造分析手法の特徴は，グラフ全体の構造から脅威値が定量的に計算され，一見関係のないようなグラフ上の離れたノードに関する不正パケットのアクセス関係もグラフ全体のノードの脅威値に波及する点である．不正アクセスの送信元送信先のペア解析[24]では，グラフ全体の構造から定量的な評価が行われていない点が異なる．本手法は，ワームの感染力に関する脅威とポートの脆弱性の関係に基づき，不正パケットが構成するグラフの構造から求められるインターネット上の脅威について 1 つの定義を提示している．本手法は，送信先のポートに対する脅威をベクトル値として計算することに対して，エントロピー手法[16]では，不正パケットの送信先に対するランダム性や偏りによる評価値をスカラー値として与えているが，グラフの空間的な構造の違いは反映されていない点が本手法と異なる．

実験では，実験期間（2005 年 6 月から 7 月）において，JPCERT/CC の注意喚起などにより深刻なインシデントと考えられるものを対象とすることで，実験的に本手法の効果を示した．

評価実験では，2 日を 1 組として 1 日単位のデータに対して本手法を適用している．これは，送信元 IP アドレスが，DHCP などにより動的に変化する影響を抑えるためである．1 日単位のパケット観測の場合，DHCP による送信元 IP アドレスの変化による誤差が比較的小さく抑えられる[25]ことから，本実験では，1 日を単位とした実験を行った．送信元ソース IP アドレスの変化による誤差の影響を低減させる方法としては，IP アドレスの論理的な距離が近い/24 のネットワークブロック内のアクセス元のノードを同一のグループと見なして，送信元ノードをグループ化したものに本手法を適用することで，確率的な変動を抑える方法などがある．これは，IP アドレスの近いネットワークには，設定の似たホストが多数存在すると考えられることが理由である．本手法は，ワームの感染力に基づく脅威を [0,1] の区間で標準化して示しているため，過去の履歴に基づく分布からの偏差を用いずに脅威値から直接比較している．

周波数分析に基づく提案手法では，ウェーブレット

解析を用いている．これは，不正パケット数の時系列データは，周波数成分が時間とともに変化する非定常的な性質を持つため，分析区間全体で同一の周波数成分を仮定するフーリエ変換よりもウェーブレット解析が適していると考えられることによる．短時間フーリエ変換を用いれば，時間的に局在する周波数成分を分析できるが，窓の区間を手動で与えることが難しく，また，解析区間全体を通じて，窓の区間が固定であるため，時間帯によって分析したい周波数と時間解像度を適応させることが難しい．ウェーブレット変換であれば，時間帯ごとに適切な時間解像度と周波数の分析に適している．

7. まとめ

本研究では，インターネット上で観測される不正パケットから，ワームなどの脅威を分析するための手法を提案した．周波数成分分析により，不正パケットの増減からでは検知が難しいワームの活動の周期性に関する変化を検知する手法を提案した．また，グラフ構造分析では，感染ホスト数の増加とワームによる脆弱なポートへの効率的な感染に基づく脅威の評価法を示した．これらの手法は，時間および空間に関する特徴量に基づく新しい分析方法を提供し，従来の異常検知手法を補完する役割を果たす．従来の手法と本提案手法を組み合わせて多角的にインターネット上の脅威を評価することにより，検出の範囲を広げるとともに，検出した手法の特徴に応じて，脅威の性質を分析するために利用することができる．

参考文献

1) Moore, D., Shannon, C., Voelker, G.M. and Savage, S.: Network Telescopes: Technical Report, Technical report, CAIDA (2004).
2) SANS Institute: Internet Storm Center. http://isc.sans.org/
3) DShield.org: Distributed Intrusion Detection System. http://www.dshield.org/index.html
4) Shinoda, Y., et al.: Vulnerabilities of Passive Internet Threat Monitors, *14th USENIX Security Symposium* (2005).
5) 鈴木裕信，石黒正揮，村瀬一郎，大野浩之：インターネット早期広域攻撃警戒システム WCLSCAN，ソフトウェアシンポジウム 2004 予稿集 (2004). http://www.clscan.org
6) JPCERT/CC：インターネット定点観測システム Internet Scan Data Acquisition System (ISDAS). http://www.jpcert.or.jp/isdas/
7) University of Michigan: Internet Motion Sensor (IMS). http://ims.eecs.umich.edu/index.html
8) Pang, R., Yegneswaran, V., Barford, P., Paxson, V. and Peterson, L.: Characteristics of Internet Background Radiation, *Proc. ACM Internet Measurement Conference* (2004).
9) The Distributed Honeypot Project: Tools for Honeynets. http://www.lucidic.net/
10) Rajab, M.A., Monrose, F. and Terzis, A.: On the Effectiveness of Distributed Worm Monitoring, *14th USENIX Security Symposium*, pp.225–237 (2005).
11) Zou, C.C., Gao, L., Gong, W. and Towsley, D.: Monitoring and early warning for Internet worms, *The 10th ACM conference on Computer and communications security*, pp.190–199 (2003).
12) Lakhina, A., Crovella, M. and Diot, C.: Characterization of Network-Wide Anomalies in Traffic Flows, *Proc. Internet Measurement Conference* (2004).
13) Ishiguro, M., Suzuki, H., Murase, I. and Ohno, H.: Internet Threat Detection System Using Bayesian Estimation, *16th Annual FIRST Conference on Computer Security Incident Handling* (2004).
14) Yamanishi, K. and Takeuchi, J.: A Unifying Approach to Detecting Outliers and Change-Points from Non Stationary Data, *8th ACM SIGKDD International Conference on Data Mining and Knowledge Discovery*, pp.676–681 (2002).
15) 竹内純一，佐藤靖士，力武健次，中尾康二：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，*SCIS2006* (2006).
16) Wagner, A. and Plattner, B.: Entropy Based Worm and Anomaly Detection in Fast IP Networks, *14th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises* (2005).
17) Theriault, K., Vukelich, D., Farrell, W., Kong, D. and Lowry, J.: Network Traffic Analysis Using Behavior-Based Clustering, BBN Technologies Technical Paper.
18) Schechter, S., Jung, J. and Berger, A.W.: Fast Detection of Scanning Worm Infections, *7th International Symposium on Recent Advances in Intrusion* (2004).
19) Kompella, R.R., Singh, S. and Varghese, G.: On scalable attack detection in the network, *4th ACM SIGCOMM conference on Internet measurement*, pp.187–200 (2004).
20) 中尾康二，松本文子，井上大介，馬場俊輔，鈴木和也，衛藤将史，吉岡克成，力武健次，堀 良彰：インシデント分析センタ nicter の可視化技術，

情報処理学会研究報告，Vol.2006, No.81, 2006-CSEC-034, pp.313–319 (2006).
21) @police：インターネット定点観測. http://www.cyberpolice.go.jp/detect/observation.html
22) 日本数学会：数学辞典，岩波書店 (1985).
23) IPA：インターネット定点観測での観測状況について (2005). http://www.ipa.go.jp/security/txt/2005/documents/TALOT2-0507.pdf
24) 久保田和己，鳥居　悟，小谷野修：不正アクセスシナリオの導出に向けた検知ログ解析，情報処理学会第 64 回全国大会，pp.379–380 (2002).
25) Moore, D., Shannon, C. and Brown, J.: Code-Red: A Case Study on the Spread and Victims of an Internet Worm, *Internet Measurement Workshop*, pp.273–284 (2001).

(平成 18 年 11 月 27 日受付)
(平成 19 年 6 月 5 日採録)

石黒　正揮（正会員）

1994 年東京大学大学院理学系研究科情報科学専攻修士課程修了．同年株式会社三菱総合研究所入社．形式仕様検証システムの研究開発，画像認識に関する研究開発，情報セキュリティリスク定量化分析に関する研究，インターネット脅威分析システムの研究開発等に従事する．

鈴木　裕信

1985 年（株）SRA 入社．1990 年同社ソフトウェア工学研究所．1997 年鈴木裕信事務所有限会社設立．OpenPGP 公開鍵サーバ OpenPKSD.ORG，早期広域攻撃警戒システム WCLSCAN の研究等を実施する．早稲田大学理工学術院理工学術センター客員研究員，専修大学ネットワーク情報学部兼任講師，学校法人実践女子大学人間社会学部非常勤講師．特定非営利活動法人フリーソフトウェアイニシアティブ副理事長．

村瀬　一郎（正会員）

1986 年名古屋大学理学部卒業，同年株式会社三菱総合研究所入社．以来，情報技術の研究開発および調査に従事する．現在は，情報セキュリティ研究グループ・グループリーダー・主席研究員．専門は情報セキュリティであり，ネットワークセキュリティ，重要インフラにおける情報セキュリティ等に興味を持つ．2006 年以降早稲田大学理工学術院客員研究員を務める．

篠田　陽一（正会員）

1989 年東京工業大学大学院博士課程修了．北陸先端科学技術大学院大学情報科学センター教授．(独) 情報通信研究機構情報通信セキュリティ研究センター長（兼務）(2006/4)．内閣官房情報セキュリティ補佐官（兼務）(2007/3)．ネットワーク分散システム，次世代ネットワークアーキテクチャ，情報環境等の研究を行う．ソフトウエア科学会企画委員（1992〜1993 年）．