社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (29)
2009－CSEC－ 44 (29)
2009／3／6

ネットワーク異常検知システムにおける攻撃種別判定法

北澤 繁樹† 河内 清人† 榊原 裕之† 藤井誠司†

†三菱電機株式会社 情報技術総合研究所
247-8501 神奈川県鎌倉市大船 5-1-1

あらまし 本論文では，異常検知に基づくワーム検知方式によって異常が検出された場合に，検知内容の真偽を確認した上で，対策が必要かどうかを判断するまでの一連の分析作業の効率化を図る手法について述べる．

本論文では，検知内容の分析を行うための分析モデルを，検知される事象を特徴付ける3つの分析パラメータで定義する．分析を行う際には，分析対象となるFirewallログを集計して，各分析パラメータの値を導出し，通常時に観測される実データから決定した閾値によって評価して，分析モデルに当てはめることによって検知内容を判断する．これにより，対応が必要な検知アラートに対して即座に対策をとることが可能となる．

Means for Attack Decision in Anomaly-Based Network Intrusion Detection System

Shigeki KITAZAWA† Kiyoto KAWAUCHI† Hiroyuki SAKAKIBARA† Seiji FUJII†

†Mitsubishi Electric Corporation, Information Technology R&D Center
5-1-1, Ohfuna, Kamakura, Kanagawa 247-8501, Japan

Abstract In this paper, we describe means for improving an efficiency of a flow of a firewall log analysis when a network anomaly-based intrusion detection system detected an unknown network anomaly is occurred. We define an analysis model based on experience of a system operation. And we also formalize the means for analysis. As a result, immediately taking measures based on the detection alert became possible achieving the reduction in an unnecessary detection alert notification.

1 はじめに

近年，マルウェアによる被害が増加の一途をたどっている．最近の傾向としては，正規のプログラムを装ってユーザに実行させるトロイの木馬型のマルウェアが主流となっている [12]．また，2008年末からネットワーク感染型のワームであるConfickerが発生し，インターネット上で猛威を振るっている [10]．

このような背景の下，異常検知に基づくワーム検知方式の研究が広く進められており [4, 5, 7, 9, 11]，我々も，インターネット上で新規に発生したワームやDoS/DDoS攻撃を早期に検知して，いち早く対策をとることを目的として，未知ワーム検知システム（以降，予兆分析システムと呼ぶ）を開発している [2]．

予兆分析システムでは，トラフィックの異常な変化を主成分分析によって捉えることで未知のワームの発生を検知する．これにより，ワームの発生から既設のセキュリティ対策によって，検知・対策できるようになるまでの無防備な期間を短縮し，被害を最小限に抑えることができる．

我々は，開発した予兆分析システムを実際にインターネットに接続されているWebサイトの監視へ導入し，運用を行った．

運用を進めるなかで，実際のトラフィック変動はワームなどの攻撃に起因するものの他に，偶発的な要因やWebサーバの利用状況によっ

ても発生するため，それらを全て異常として検知することがわかってきた．このような状況下においては，それぞれのアラートに対して検知内容の分析を行う作業が，管理者にとって高負荷となることが，日々の運用上課題となった．

そこで，本論文では，異常検知に基づくワーム検知方式によって，異常が検出された場合に，検知内容の真偽を確認した上で，対策が必要かどうかを判断するまでの一連の分析作業の効率化を図る手法について述べる．

本論文の構成は次の通りである．2 節では，実運用されている Web サイトに我々が開発した，“予兆分析システム” を導入して実際に運用を行った際に課題となった，異常検知後のログ分析の負荷について述べる．3 節および 4 節で，2 節であげた課題を解決するための検討内容について述べる．さらに，5 節にて，検討結果に関する評価手順と評価結果について説明し，6 節にて評価結果に関する考察を行う．最後に，7 節で関連研究に触れた後，8 節で本論文をまとめる．

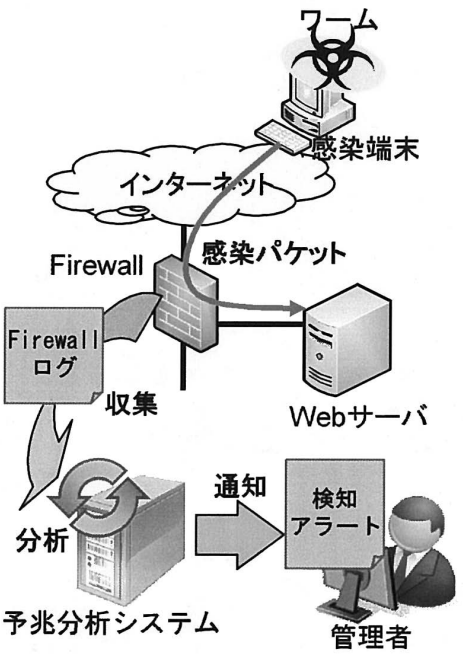

図 1: Web サイト監視システム概要

2 Web サイト監視システム

2.1 システム構成

予兆分析システムを用いた Web サイト監視システムの概要を，図 1 に示す．

予兆分析システムでは，インターネットに接続された Firewall で記録されたログをリアルタイムで収集して分析する．

分析では，Firewall の通過ログを集計して得られるトラフィックの時系列データを主成分分析によって分析し，Web サーバへのトラフィックの特徴量の変化を検出する．Firewall の通過ログを分析対象としたのは，Firewall を通過した通信は直接 Web サーバに到達するため，攻撃を検知した場合，緊急の対応が求められるためである．分析の結果，異常を検知した場合に，検知アラートを管理者へ通知する．

検知アラート受けた管理者は，検知内容を特定し，対策が必要であるかどうかを判断する．

2.2 システム運用上の課題

システムの運用では，管理者は，検知アラートが通知された後，対策が必要かどうか判断するため，予兆分析システムによって異常が検知された原因について分析する．分析では，観測されたトラフィックの時系列データを見ながら，異常が検知された時刻付近の Firewall ログを抽出し，不審なログ（普段発生しないようなログ）が記録されているかどうかを調査する．

ログの調査において，管理者は，普段 Web サーバに対してどのようなアクセスがあり，それが Firewall ログにどのように記録されるのか，熟知している必要がある．また，特に，予兆分析システムの検知アラートが誤検知の場合には，不審なログが記録されていないことを確認する必要があり，この作業には数時間かかることも，しばしばある．

しかしながら，実際のトラフィック変動はワームなどの攻撃に起因するものの他に，偶発的な要因や Web サーバの利用状況によっても発生する場合がある．Web サイト監視システムの運用開始後，平均 1 件/日程度の検知アラートが発生し，また，その全てが分析の結果として対策が必要のない検知アラートであると判断された．

このような状況下においては，それぞれのアラートに対して手動で分析を行う作業が日々の運用上，管理者にとって大きな負担になることが課題となった．

そこで，検知アラート発生後に管理者が行うログ分析手順の整理および効率化について検討

し，最終的には，分析処理の自動化を目指すこととした．

3 ログ分析手順の効率化検討

3.1 ログ分析手順の整理

我々はまず，管理者が予兆分析システムから検知アラートを通知された後のログ分析手順について整理した．整理した分析作業の流れは，以下の通りである．

1. 検知アラートがあがった付近のトラフィック変動（時系列グラフ）の調査
2. Firewall ログを集計し，発信元 IP アドレス別の Web サイトへのアクセス数一覧を作成
3. 作成した発信元 IP アドレス別のアクセス数一覧を元に以下の点を確認
   (a) 他と突出してアクセス数の多い発信元 IP アドレスがあるかどうか（Dos/DDoS 攻撃の可能性）
   (b) アクセスしてきている発信元 IP アドレスの数が普段と比べて多いかどうか（ワーム，もしくは，アクセスユーザ数の増加の可能性）
   (c) それぞれの発信元 IP アドレスからのアクセス数が普段の Web アクセスの状況から推測して，極端に少ないアクセスと通常観測されうるアクセス数との比率に乖離がないかどうか（ワームとアクセスユーザ数の増加による一時的なトラフィックの増加の切り分け）

基本的には，分析は上記の手順に沿って行われるが，各確認項目において，明確な判断ができない場合もあり，その際には，様々な状況の発生を想定し，分析の範囲を広げて分析を行っていた．このため，最終的な判断ができるまでに数時間かかることもあった．

3.2 検知事象のモデル化

管理者が行うログ分析では，3.1 節で示した手順にしたがって，予兆分析システムで検知アラートが通知される検知事象として，攻撃にあたる事象である，“ネットワークワーム”，“DoS 攻撃/DDoS 攻撃” と，通常のアクセスにあたる事象である “アクセスユーザ数の増加による一時的なトラフィックの増加” について，切り分けを行っている．

そこで，これらの事象に関してトラフィックに現れる特徴に基づいて検知事象をモデル化することにより，特定すべき検知事象を定義し，特定すべき事象の判断基準を明確化する．それぞれの事象について，ネットワーク上で観測される特徴は以下の通りである．

ワーム

- インターネット上でワームが発生した場合，ワームが感染先を探すためのスキャンパケットが発生する．
- 総感染端末数が増えるにつれ，スキャンパケットを受信する確率が高くなる（アクセスしてくる発信元 IP アドレスの数も増える）．
- 1IP アドレスからのアクセス数としては，1 宛先 IP に対して，アクセス数が少数の通信が観測される．

DoS 攻撃/DDoS 攻撃

- Firewall を通過する可能性がある，SYN フラッド，コネクションフラッド，リロード攻撃（F5 攻撃）とも，特定 IP アドレス宛のアクセス数の高い通信が観測される（DoS によりサーバ負荷を上げることが目的であれば宛先を分散することに攻撃者のメリットはないため）．
- SYN フラッド，コネクションフラッドともに，アクセス頻度以外に通過ログとしては，通常アクセスとの差はない．
- DDoS 攻撃の場合は，観測される発信元 IP アドレスの数が増加する．

アクセスユーザ数の増加

- Web サイトのコンテンツ更新や Web サイト固有の事由によって，通常の Web アクセスが多数の発信元 IP アドレスから発生する．

予兆分析システムが検知する事象について，その特徴を，それぞれ，単位時間あたりの “発信元 IP アドレスの数”，“1IP アドレスあたりのアクセス数”，“少数アクセスの通信の数” をパラメータとして着目すると，表 1 のようにモデル化できる．

表 1 で定義したモデルに対して，予兆分析システムが異常を検知した際に観測された事象を

表 1: トラフィックに観測される検知事象の特徴

検知事象	発信元 IP アドレスの数	1 発信元 IP アドレス当りのアクセス数	少数アクセスの通信の数
ネットワークワーム	多数	—	多数
DoS 攻撃	—	多い発信元少数	—
DDoS 攻撃	—	多い発信元多数	—
アクセスユーザ数の増加	多数	—	—

当てはめることによって，発生した事象の特定を行う．なお，観測されている事象がどのモデルにも当てはまらない場合は，普段偶発的に発生しうる事象を誤って検知したものと判断する．

4 ログ分析手順の自動化

3 節では，運用で行ってきた分析手順を整理し，予兆分析システムからの検知アラートが通知された場合に特定すべき検知事象についてのモデル化を行った．本節では，3 節での検討結果を踏まえて，分析手順の自動化について述べる．

3 節での検討結果を元にログ分析手順をフロー化したものを，図 2 に示す．ログ分析手順

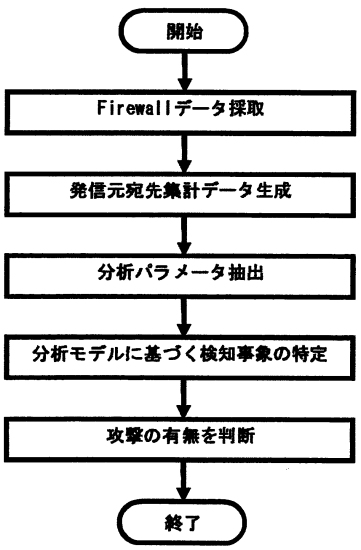

図 2: 分析フロー

の大まかな流れは，まず，分析の元となる Firewall ログを集計し，分析モデルへ当てはめるための分析パラメータ抽出し，評価することによって，発生した事象を特定する．

図 2 における各処理の詳細について，次節以降で説明する．

4.1 発信元宛先集計データの生成

予兆分析システムで異常が発生されたときに観測された事象を，表 1 の定義に当てはめるにあたって，パラメータとして “発信元 IP アドレスの数”，“1IP アドレスあたりのアクセス数”，“少数アクセスの通信の数” を導出する．

各パラメータを導出するために，発信元 IP アドレスから宛先 IP アドレスへのアクセス数に着目して，Firewall のログを集計する．

Firewall ログの集計では，観測された Firewall ログを，発信元ＩＰアドレス，宛先ＩＰアドレス，宛先ポート番号が同じログを，観測された Firewall 別に集計する．集計によって得られたデータを，“発信元宛先集計データ” と呼ぶ．

発信元宛先集計データには，発信元ＩＰアドレス，宛先ＩＰアドレス，宛先ポート番号，集計値が含まれる．

4.2 分析パラメータの抽出

4.1 節で生成した発信元宛先集計データから分析パラーメータを抽出する．まず，“発信元 IP アドレスの数” は，発信元宛先集計データに含まれる発信元 IP アドレスの種類を算出する．

次に，“1IP アドレスあたりのアクセス数” については，生成された発信元宛先集計データの中で集計値が上位のデータから抽出される．

“少数アクセスの通信の数” については、生成された発信元宛先集計データのうち，集計値が n 以下の通信を抽出する．

4.3 分析モデルに基づく検知事象の特定

4.2 節で抽出された分析パラメータを，表 1 に当てはめて分析を行う．各分析パラメータの評価では，パラメータ別に定められた閾値を元に，ログ集計機能で算出された各分析パラメー

タの値が閾値を超えているかどうかを判断する．

分析パラメータの評価で用いる閾値は，あらかじめ設定しておく．閾値は，一定の学習期間を設け，その間に収集されたFirewallログから，それぞれの分析パラメータを導出し，最大値のk倍を設定する．kの値はチューニングパラメータであり，運用を継続行しながら最適値に設定する．なお，運用の初期段階では，$k=2$に設定した．

5 評価

5.1 評価手順

3節，および，4節で検討した内容を元に実際の手順に従って分析を実施するための分析ツールを開発して，分析手順の効率化，ならびに，分析結果の正しさの観点から評価する．

評価では，まず，過去3ヶ月に渡って予兆分析システムで異常を検知（106件発生）した際の検知事象について分析ツールによって検知事象の特定処理を行い，分析にかかる時間を測定して従来かかっていた時間と比較することによって，効率化の観点での評価を行う．

また，分析結果の正しさの観点では，分析ツールによって得られた分析結果を，実際に管理者が分析した結果と比較することによって，差異がないかどうかを確認する．

5.2 評価結果

5.1節の評価手順に従って評価を実施した．

結果として，まず，分析にかかる時間に関しては，手動で分析した場合には，1件につき2〜3時間かかっていた分析作業が，分析の自動化によって1分程度まで短縮された．

一方，分析結果の正しさの観点においては，発生した106件の検知アラートのうち，定期メンテナンスによるトラフィックを検知したアラートが1件DoS攻撃と判定されたが，残りの105件では，ネットワークワーム，DoS/DDoS攻撃といった攻撃と判断された事象はなく，全ての検知アラームに対して，通常偶発的に発生しうる通信と判断された．この結果は，手動によるログ分析の結果と一致している．

6 考察

5.2節で述べた評価結果から，3節ならびに4節での検討した結果に関して，目的であった予兆分析システムで検知した事象の特定のためのログ分析作業が効率化といえる．

分析結果の正しさの観点において，定期メンテナンスによるトラフィックの変動を検知したアラームに関して，DoS/DDoS攻撃と判定されている．これは，作業端末からWebサイトに対するアクセス数が，設定した閾値を超えたため，DoS攻撃の特徴と一致したためである．

定期メンテナンスに関しては，作業実施日，時間帯などの情報を事前に入手可能であるため，運用上は，定期メンテナンス中の検知アラートに関しては，対応不要とすることによって解決可能である．また，システムによる解決の方法としては，ホワイトリストへメンテナンスや管理通信で用いられる発信元IPアドレスを登録しておき，検知アラートから除外するといった解決策が考えられる．

なお，評価した3ヶ月間では，攻撃自体が発生していないため，False Negative（攻撃が通常発生しうる事象として判定されること）が発生しているかどうかについては十分な評価はできていない．仮に，False Negativeが発生していた場合には，各分析パラメータを評価するために設定する閾値を調整する必要がある．

また，開発した分析ツールを予兆分析システムで異常を検知した後に自動実行させ，攻撃が発生していた場合のみ，検知アラートとして管理者へ通知することが可能となった．これにより，対応不要な検知アラートの通知を管理者が受け取ることがなくなった．したがって，検知アラートを通知された管理者は，ログの分析作業を行うことなく，検知アラートの結果に基づいて即座に対策をとることが可能となった．

本論文で検討した分析モデルによる検知内容の分析手法では，さらに運用の効率をあげるために，今後，閾値のチューニング手順が運用上の課題となる．閾値の設定は，分析結果の精度に直接影響を及ぼすことから，常に適切な値が設定されている必要があるため，閾値のチューニング方法については，引き続き，検討を深める必要がある．

7 関連研究

現在一般的に利用されているシグネチャ方式の侵入検知システムにおいても誤検知（False Positive）が多く発生することが運用上の課題としてあがっており，誤検知削減を目的とした研究が進められている[6, 8]．また，SIEM（Security Information and Event Management）製品[1]

などに実装されたイベント相関分析機能などによっても不要アラート削減の取り組みがなされている．

ただし，これらの試みでは，シグネチャ方式の侵入検知システムでは，攻撃を検知した際に得られる詳細情報（攻撃が影響するOSや，脆弱なアプリケーションのバージョンなど）に基づいて，攻撃成功の有無を確認するものである．したがって，ネットワーク異常検知システムのように，攻撃による異常が検知された時点では攻撃に関する詳細情報が得られない場合には対応できない．

一方，本論文と同様，ネットワーク異常検知システムで検知された異常に関する研究もなされている．自己組織化マップを用いた方式 [3] では，分析結果を視覚化し，異常を検知した際のグラフのパターンを管理者が視覚的に発生事象を判断する．しかしながら，視覚化による発生事象の判断では，管理者の主観によって判断結果が異なることも考えられる．本論文の方式によれば，検知事象のなかから管理者の主観によらず，攻撃に関するものを明確に判断できる．

8 おわりに

本論文では，異常検知に基づくワーム検知方式によって，異常が検出された場合に，検知内容の真偽を確認した上で，対策が必要かどうかを判断するまでの一連の分析作業の効率化を図る手法について述べた．

本論文では，検知内容の分析を行うための分析モデルを，検知される事象を特徴付ける3つの分析パラメータ（“発信元IPアドレスの数”，“1IPアドレスあたりのアクセス数”，“少数アクセスの発信元IPアドレス数”）で定義した．分析を行う際には，分析対象となるFirewallログを集計して，各分析パラメータの値を導出し，通常時に観測される実データから決定した閾値によって評価して，分析モデルに当てはめることによって検知内容を判断する．

また，定義した分析モデル，ならびに，分析フローを実装した分析ツールを開発し，予兆分析システムで異常を検知した後に自動実行させることにより，攻撃が発生していた場合のみ，アラートとして管理者へ通知することが可能となった．これにより，不要な検知アラート通知の削減を実現した．したがって，検知アラートを通知された管理者は，ログの分析作業を行うことなく，検知アラートの結果に基づいて即座に対策をとることが可能となった．

今後の課題としては，False Negativeが発生しているかどうかについては運用を継続しながら通常時のトラフィックを観測し，擬似的な攻撃トラフィックと混合させた評価を実施する．

また，現在はあらかじめ定義しておく必要がある閾値についての最適値の決定方式について，さらに検討を進める．

参考文献

[1] ArcSight: ArcSight SIEM Platform. http://www.arcsight.com/.

[2] 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，情報処理学会研究報告 (2006). CSEC-35-13.

[3] 大河内一弥，力武健次，中尾康二：自己組織化マップを用いたネットワークインシデント分析の研究，暗号と情報セキュリティシンポジウム (2006). SCIS2006-2e-2-3.

[4] 北澤繁樹，河内清人，榊原裕之，藤井誠司，平井規郎：時系列分析による未知ワーム検知システムの実装と評価，マルチメディア・分散・協調シンポジウム (2005). DICOMO 2005.

[5] 北澤繁樹，河内清人，榊原裕之，大越丈弘，藤井誠司，平井規郎：ワーム検知システムの検討，情報処理学会 第67回全国大会 (2005).

[6] Kruegel, C., Robertson, W. and Vigna, G.: Using Alert Verification to Identify Successful Intrusion Attempts, *Practice in Information Processing and Communication*, Vol. 27, No. 4, pp. 219–227 (2004).

[7] Qin, X., Dagon, D., Gu, G. and Lee, W.: Worm detection using local networks, Technical report, College of Computing, Georgia Tech. (2004).

[8] 北野雄大，嶋村 誠，河野健二：パッケージマネージャと連携したNDISの誤検知削減，情報処理学会研究報告 (2008). CSEC-43-6.

[9] 山西健司，竹内純一，丸山祐子：統計的異常検出3手法，情報処理，Vol. 46, No. 1, pp. 34–40 (2005).

[10] ZDNet Japan: 世界で350万のホストがConficker ワームに感染. http://japan.zdnet.com/sp/feature/07zeroday/story/0,3800083088,20386578,00.htm.

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

[12] 独立行政法人情報処理推進機構（IPA）：情報セキュリティ白書 2008 第II部 10大脅威ますます進む『見えない化』. http://www.ipa.go.jp/security/vuln/documents/10threats2008.pdf.