近畿大学工学部研究報告 No. 37, 2003年, pp. 121-126
Research Reports of the School of Engineering,
Kinki University No. 37, 2003, pp. 121-126

ＴＣＰ／ＩＰパケット解析による不正アクセス検知とセキュリティ対策

坂本　昭彦*，村上　学**，河口　和範**

Detecting Illegal Access by analyzing TCP/IP Packet and Security Guideline

Akihiko SAKAMOTO*, Manabu MURAKAMI**, Kazunori KAWAGUCHI**

Synopsis

Illegal access to the computer network is one of the serious issues in the present society. Interpolation and deletion of the web files opend on the Internet server are common cases. There are some measures toward those problems. However, they are not perfect because of defects in themselves. And that precautions against illegal access are not enough diffused yet. Alternate measures are desired. Here are some keys to the issues.

In order to make the meansures firm, administrators have to investigate log files thoroughly. However, it forces them to continue hard and complivated work. Because the work must be done with the information given only by the character string. The purpose of our reserch is to lighten the hard and complicated word imposed on administrators by visualizing the log files and automating the investigation. Alternate measures against illegal access and interpolation of the web files, such as, detecting the root of illegal access and restoring the web files automatically are introduced in this paper.

１．はじめに

コンピュータネットワークの通信技術が発展し，今日では ADSL 等のブロードバンド技術が本格化することにより、高速な常時接続環境が極めて身近になっている．ネットワークが一般化するまでは，外部からの攻撃もそれほど重要視されていなかった．しかし，インターネットへ常時接続するとなれば，外部から攻撃される危険性は想像以上に高く，今まで不正アクセス行為の被害とは無縁と考えられていた一個人ユーザ自身のパソコンでも，最低限のセキュリティ対策を行

*近畿大学工学部電子情報工学科　Department of Electronic Engineering and Computer Science, School of Engineering, Kinki University

**近畿大学大学院工業技術研究科　Graduate School of Industrial Technology, Kinki University

う必要があると考えられる．それ以上にインターネットに接続する時間とユーザの数が増えるということは，インターネットサーバはセキュリティの意識を高める必要があるといえる．

本研究では，不正アクセスの手口を解析することにより，サーバセキュリティを向上させることの出来るシステム構築を目的とした．さらに検知作業が困難であるとされるサービス不能攻撃に対し，トラフィックパターンを用いる検知方法を提案した．また，サーバで公開されるコンテンツについても，以前とは違い社会的に大きな影響力を持っていることより，Web サーバで公開されるホームページが改竄された場合の自動修復システムを構築した．

2．不正アクセスの現状

2002 年度，情報処理振興事業協会セキュリティセンター（IPA/ISEC）が発表した不正アクセス届出件数は 619 件である．これは過去最多の件数である．2000 年に不正アクセス禁止法が施行され，セキュリティ管理者や組織のセキュリティに対する関心が高まったにも関わらず，不正アクセスによる被害の届出は増加の一途をたどっている．不正アクセス届出の詳細を表 1 に示す．2002 年は 2001 年と比べて，ワーム感染・形跡の届出が大幅に減少した一方，不正アクセス形跡や DoS（サービス妨害）の届出が大幅に増加している．

3．TCP／IP パケット解析

本研究では，実際に攻撃用に用いられているパケットを解析することにより，攻撃ツールの持つ独自のパケット特性を検出する．攻撃用ホストから攻撃ツールを使いターゲットとするターゲットサーバへの攻撃を試みる．ターゲットであるサーバへのアクセスは必ずパケット解析サーバを通過する設定を行う．ネットワークを流れる攻撃パケットはパケット解析サーバにより取得する．パケット解析サーバを用い同じネットワーク上に流れるデータを観測する．攻撃パケットの解析には TCP ダンプとトラフィック量を用い検証する．

4．不正アクセスの検知

不正アクセス検知とは，様々な情報から不正アクセスと思われる事象を検出し，それをシステム管理者に迅速に通知することである．一般的なログファイルを用いた不正アクセス検知方法と本研究で行った TCP／IP パケット解析により検出することができた攻撃ツールの特性を用いた検知方法について検証する．

表1 不正アクセス届出の詳細（IPA/ISEC）

届出種別	2001年	2002年
不正アクセス	97	106
不正アクセス形跡（未遂）	96	356
ワーム感染	184	6
ワーム形跡	71	34
アドレス詐称	39	49
SPAM	5	3
メール不正中継	25	16
DoS	5	16
その他	28	33
合計（件）	550	619

4．1 ログファイルを用いた検知

不正アクセス検知には，サーバに残るログファイルを定期的に閲覧する作業が必要である．ログを元に様々な情報から不正侵入と思われる事象を検出するのであるが，閲覧すべき量が膨大で、そのうえテキストのみの情報である．ログを全て読み，意味のある情報として解釈することは極めて困難である．また、ログファイルは散在しているため，不正侵入検知を行うためには複数のログを個々に閲覧し，得られた情報を総合して判断を行う必要がある．ログファイル間の関連付けも，閲覧者が行わなければならないならない．さらに，サービスに対して完全に接続が終了していないイベントはログファイルには記録されないことより，DoS 攻撃等は検知できないという問題点がある．

４．２　パケット解析による検知

不正アクセスに用いられる攻撃の多くは，特別に加工されたパケットを使用する．パケット解析による不正アクセスの検知に，ネットワークに存在しないはずの加工されたパケットを検出することにより行う．本研究では以下のパケット解析方法により検知を行う．

（１）ストリングマッチ検知

ストリングマッチ検知は，データベースに登録されている不正アクセス手法のパターンと，ネットワークを流れるパケットのデータ部分に格納されている文字列データのパターンが一致するかどうかを調査し，一致したものを攻撃の疑いがあるとする．

（２）特定コネクション検知

特定コネクション検知は，ポートスキャンやバックドアへの接続の試み，提供していないサービスおよびホストへの接続を検知することにより不正アクセスを検知する．実際の攻撃に使われるポートを登録し，監視ことにより攻撃の判定を行う．

（３）トラフィックパターン検知

サーバのリソース枯渇を目的とした攻撃であるSYN Flood や Smurf 攻撃を受けた場合，サーバへのアクセスは正規の方法を用いるため，従来の不正アクセス検知方法では非常に困難である．不正アクセス者が DoS 攻撃を行うには特定のツールを用いる．通常，トラフィック量にはパターンは現れないが，攻撃のツール等を使用した場合，サーバに対して流れるパケット量の波形に特徴がみられる．このトラフィックパターンを比較することにより不正アクセス検知を行う．トラフィック量の一定時間の波形を切り出し，トラフィックの特徴パターン比較することでトラフィックが攻撃かどうか判断の基準とする．

図１のようにトラフィック量波形の類似性を用いて比較することにより，サービス不能攻撃に対して，トラフィックパターン検知による対策が可能となる．

トラフィック量の類似性の判断基準として相関係数を用いる．相関係数は１に近いほど相関性が強いと判断する．相関係数を用いることにより，アクセス数が１に近い値でない場合も，その形状が類似していれば２つのデータは強い関連があると判断できる．

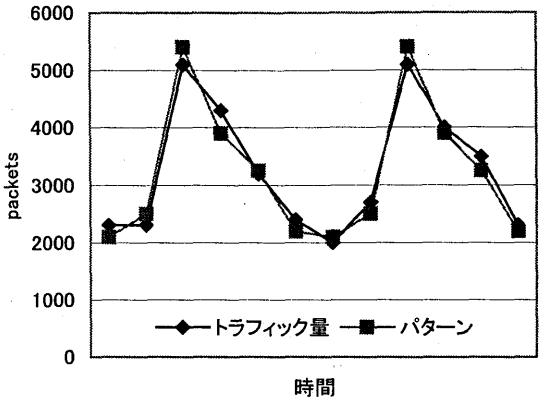

図１　トラフィック量の類似性

２つの変数をX，Yとし，ｎ個のデータ（X1，Y1）（X2，Y2）…（Xn，Yn）とすると，相関係数は

$$r=\frac{\sum\left(Xn-\overline{X}\right)\left(Yn-\overline{Y}\right)}{\sqrt{\sum\left(Xn-\overline{X}\right)^2}\sqrt{\sum\left(Yn-\overline{Y}\right)^2}}$$

で求められる．相関係数ｒを用いてトラフィック量の相関性を評価する．

５．セキュリティ管理サーバ

セキュリティ管理サーバは，不正アクセスの検知と不正アクセスが行なわれた際の事後対策を目的とする．不正アクセスの検知は，セキュリティ管理サーバを通過するパケットを解析することにより行う．同時にシステム管理者のサーバ監視作業の軽減を目的としたサーバアクセス量を視覚化したグラフの表示も行えるようにしている．また事前対策である不正アクセス検知に加え，Web サーバに不正アクセスが行なわれ，ホームページを改竄されたことを想定し，セキュリティ監視サーバにより Web ファイルの監視，自動修復を行う．

構築を行ったシステムを図２に示す．インターネットからのアクセスはセキュリティ管理サーバにより一

般ユーザ，公開サーバのネットワークに分割する．公開を目的としたサーバのみを外部からアクセス可能なDMZ（非武装地帯）とし，一般ユーザのネットワークから切り離す．ユーザのネットワークは外部から侵入できないようにセキュリティ管理サーバを構築する．パケット解析点は図２に示している外部ネットワークのパケットを用いる．不正アクセスを検知した場合はセキュリティ管理サーバでパケットフィルタリングを行い公開サーバにも不正パケットの到達を防ぐ．

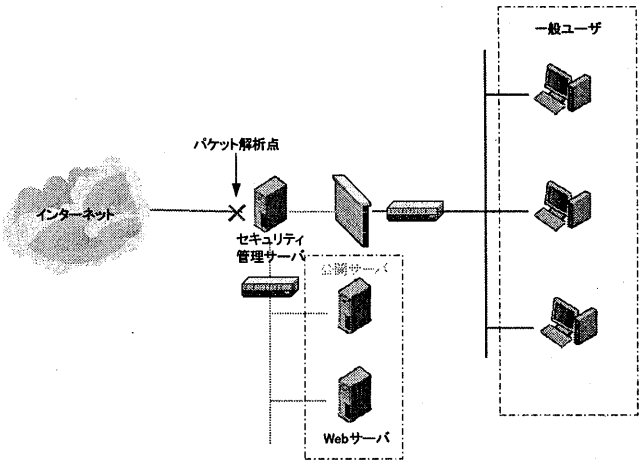

図２　システム構成

（１）アクセス量の視覚化

管理対象サーバへのアクセス量をアクセス元ネットワーク別に視覚化を行う．図３のグラフのようにアクセス量をグループ別に視覚化することで管理者のネットワーク状態認識作業の軽減ができる．

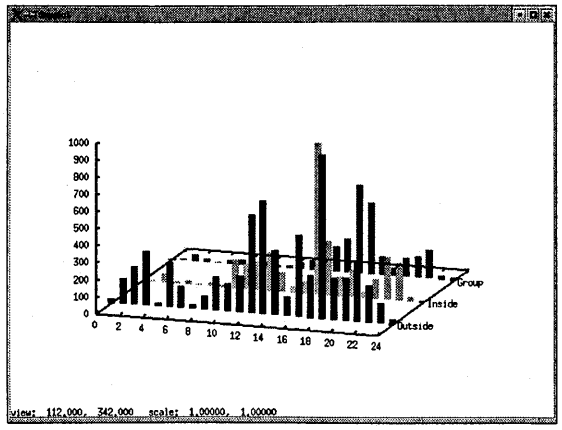

図３　グループ別アクセス量

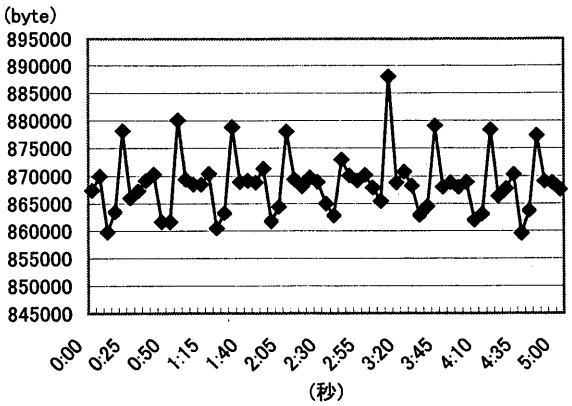

図４　トラフィック量パターン

（２）不正アクセスの検知

セキュリティ監視サーバによりネットワークを流れる攻撃用の不正パケットをストリングマッチ検知，特定コネクション検知，トラフィックパターン検知を行う．トラフィックパターン検知には，パケット解析により得た図４のようなパターンをあらかじめ登録することにより行う．これによりログファイルを用いては検知不可能であるアクセスを認識できる．

不正アクセスを検知した場合は，管理者画面またはメールにより警告する．

（３）Web サーバの監視と自動修復

セキュリティ管理サーバはオリジナルのＷｅｂファイルを保管し，Web サーバ上のファイルと比較することにより改竄の検知を行う．ファイルの改竄を検知した場合，セキュリティ管理サーバに保管されているオリジナルファイルを FTP によるファイル転送を行い自動的に Web ファイルの修復を行う．

本研究では，実際に攻撃に用いられている攻撃ツールを使い，セキュリティ管理システムの有効性の検証を行った．

６．考察

１．アクセス量の視覚化表示

アクセス量を図３のように視覚化することで管理者がネットワークの状態認識作業の軽減ができる．アク

セス量グラフは直接的には不正アクセス検知には結びつかないが，管理者が通常時のネットワークを把握している場合には有効な情報となる．サーバに対するアクセス量は，サーバコンテンツの変更等により変化するが，通常は前日，または１週間前の時間帯アクセス量と大幅には変化が見られることはない．集中アクセスを用い，ネットワークリソースの枯渇を目的とする攻撃に対して，管理者が直感的な検知作業が可能である．本研究では，アクセス量をネットワーク別にグループ化することにより，アクセス元のネットワーク特定に利用できる．

２．不正アクセスの検知

（１）ストリングマッチ検知

ネットワークを流れるパケットの中から，不正アクセスに用いられるキーワードである文字列を検出する方法である．文字列の照合を用いることにより誤報が少ない正確な検知が可能であった．攻撃用のパケットに含まれる文字列をルールとして登録する必要があるため，インターネットやセキュリティのコミュニティで告知されている情報を集めるか，管理者がパケット解析を元にキーワードを作成する必要がある．

（２）特定コネクション検知

通常時のサーバが行っているサービスポートまたは攻撃に用いられる特定のポートへのアクセスを検知することにより警告を行った．サービスに対してアクセスを監視することで，攻撃だけでなく攻撃を行う上での事前調査にあたるアクセスの検出も可能といえる．特定コネクション検知は，監視対象サーバのサービス状況を把握し，管理者により不正アクセス検出ルールを常に変更する必要がある．ルールはセキュリティポリシーや管理者の能力に大きく依存する．

（３）大量コネクション検知

一定時間のサーバに対するコネクション量を監視することにより異常アクセスの検知を行った．大量にコネクションが行なわれたとしても，正常のサービス利用によるアクセスの可能性がある．大量コネクション検知の結果だけでアクセスが不正なものかどうかの断定はできないが，不正アクセス検知と判断する要素になりえる．

（４）トラフィックパターン検知

セキュリティ管理サーバを通過するパケット量の波形を，相関係数を用い攻撃用ツールの波形と比較することにより攻撃と判断する．DoS 系の攻撃はログファイルを用いた不正アクセス検知が不可能であるうえ，パケットに特定の文字列がふくまれていないため，他の不正アクセス検知方法は有効ではない．トラフィックパターン検知を用いることでコネクションの確立されない攻撃に対して検知が可能であった．相関係数を用いることにより波形の類似性を用いた検出であるため，DoS 攻撃の検知はできるが正常アクセスに対しても誤報として警告を出す可能性がある．そのため誤認が最も少なくなる相関係数の検討が課題である．

セキュリティ管理サーバによりトラフィックパターン検知を行う方法は，トラフィック量を用いる方法は SMNP によるサーバ環境変数を取得できるネットワークであれば，監視対象サーバから遠隔にある場所での不正アクセス検知を可能とする．

トラフィックパターンは，トラフィック量の波形パターンを自動的に取得することができれば未知の攻撃に対し検出が有効である．

３．Web ファイルの自動修復

CRC を用いたファイル比較により Web ファイルに変更が加えられた場合，自動で修復を行うことができる．ファイルの比較タイミングをタイマーにより行うため，ファイルの改竄が行なわれてから最大３０分修復に必要な時間がかかる．比較を行う時間を縮める事も可能ではあるが，Web サーバの負荷とネットワーク帯域の消耗を考慮することが今後の課題である．

7．おわりに

現在の不正アクセス検知システムにはさまざまな問題点がある．特に誤検知とそれを防ぐためのルールのチューニング問題は非常に重要である．侵入検知システムを熟知した管理者のいるところでは，ルールの最適化と細かなメンテナンスが可能かもしれない．しかし，それ以外ではルール最適化は事実上不可能で，またこうした熟練管理者の数は絶対的に不足している．不正アクセスの手口が多様化している現代ではこうした管理者の支援を行うシステムが必要である．

TCP／IP パケットの解析により不正アクセスを目的とした攻撃の検知，改竄されたWebファイルの自動修復システムにより管理者を支援できるシステム構築が達成された．主にDoS攻撃のようなログファイルに記録されない攻撃に対しパケット解析による判定が可能である．特に，本研究で用いたトラフックパターン検知方法は，トラフィック量を用いることにより検出に要する負荷が軽く，高速ネットワークへの対応が容易である．さらに，リモート監視に適用できることは，今後の不正アクセス検知システムの構築で非常に有効な手段である．

参考文献

[1]Stephen Northcut, Mark Cooper, Matthew Fearnow, Karen Frederick: "Intrusion Signitures and Analysis", Jan, 01, 2001, New Riders Publishing

[2] Stephen Northcut, Judy Novak :
"Network Intrusion Detection"
Jun, 01, 1999, New Riders Publishing