2F-3

定点観測による不正アクセス分析システム
－概要－

榊原裕之† 大野一広† 北澤繁樹† 藤井誠司† 平井規郎† 鹿島理華†
三菱電機株式会社 情報技術総合研究所†

1. はじめに

筆者らは未知の不正アクセスを早期に検知するため，定点観測によるネットワーク監視データの変化を主成分分析により検出する不正アクセス分析システムの開発に取り組んでいる[1]．しかし，当システムの運用に際し 3 つの課題がある．1 つ目は不正アクセスからの被害を抑制するための対策の仕組みの開発であり，2 つ目はリアルタイムな検知を実現するための検知方式の改良であり，3 つ目は検知性能の評価である．本稿ではこれらの課題の解決策について論ずる．

2. 対策機能の開発

2.1. N/W 機器の制御による対策

不正アクセスを検知した後の対策については，各計算機において対処する方式と，ネットワーク（以下 N/W）機器において不正なパケットを遮断する方式がある．前者の例として各計算機にインストールされたセキュリティソフトウェアによるワームの駆除が挙げられる．セキュリティソフトウェアは広く普及しているが，既知の不正アクセスへの対策は可能であっても未知の不正アクセスへ対応できない場合がある．

そこで，当システムでは N/W 機器の制御による不正パケットの遮断により早期に被害を抑止する方式を採用した．なお，不正アクセスが既知になればセキュリティソフトウェアで対応が可能となるため一度設定した N/W 機器の制御を解除することが可能となる．

2.2. 機能の概要

N/W 機器の制御による不正パケットの遮断に基づく対策では，正常な通信への影響を抑えるため不正アクセスに関わるパケットのみ遮断することが要求される．一方，不正アクセスの種類によりアクセスのパターンが異なるため，種類に応じて遮断の方法を変える必要がある．

An Intrusion Detection System by fixed-point observation of network security data – overview -, † Hiroyuki Sakakibara Kazuhiro Ohno, Shigeki Kitazawa, Seiji Fujii, Norio Hirai , Rika Kashima, MITSUBISHI ELECTRIC CORPORATION, INFORMATION TECHNOLOGY R&D CENTER

そこで，不正アクセスの種類を判別する機能と N/W 機器の制御情報（ACL :Access Control List)を生成する機能を開発した.図 1は時系列データの変化を検知した後，不正アクセスの種類を判別・生成した ACL をルータに設定することにより不正アクセス元の端末からの通信パケットを遮断する適用例である．

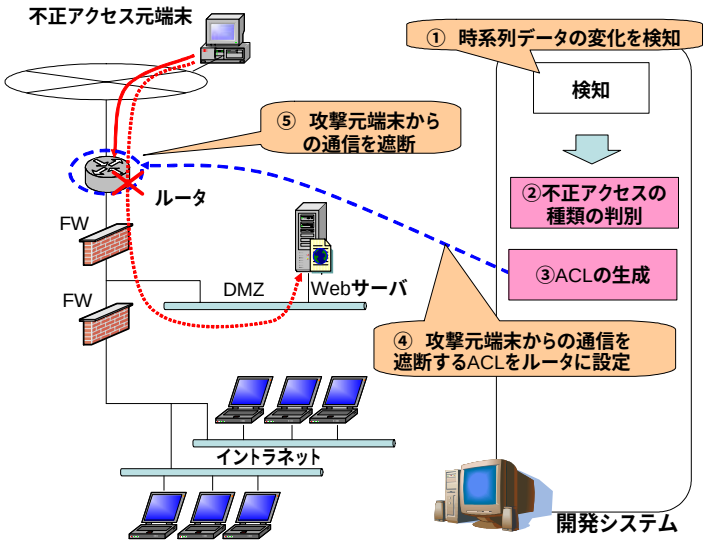

図 1 対策機能の適用例

(1) 不正アクセスの種類の判別

検知した不正アクセスに対し適切な対策を実施するためには，ワームやスキャン等の不正アクセスの種類を判別する必要がある．しかし，検知方式は特定ポートへのアクセス数や特定地域からのアクセス数の時系列変化を捉える方式のため種類を判別することはできない．そこで，通信パターンから不正アクセスの種類を判別する方式を採用した．

例えば，典型的なワームでは，感染時に感染に利用するポートが開いているホストを探す．これは 1 つのホストから複数ホストの該当ポートへのアクセスとして観測される．ポートスキャンでは 1 つのスキャン元ホストから 1 つのスキャン先ホストの複数ポートへのアクセスが観測される．ホストスイープでは 1 つのスイープ元ホストから複数のスキャン先ホストの複数ポ

ートへのアクセスが観測される[1]．DoS では大量の１対１通信が観測される（図 2）．

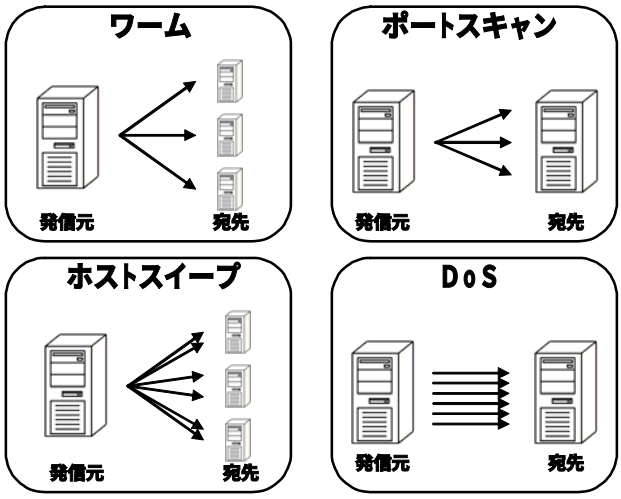

図 2　不正アクセスと通信パターンの例

このように不正アクセスの種類ごとに観測される通信パターンが異なることを利用し，不正アクセスが検知されたタイミングでの通信のパターンを調査することで種類を判別する．

(2)　N/W 機器の制御用情報の生成

当機能では，被害の拡大を抑止することを目的とした対策用の情報生成を行う．不正アクセス判別機能により不正アクセスの種類が特定された場合，種類ごとに ACL を生成する．ACL は遮断すべき IP アドレス/ポートなどの情報で構成される情報である．

ACL の記述方法として[2]を例に挙げると，IP = x.x.x.x のホストから，任意のホストのポート 445(TCP)にアクセスが発生していた場合に，これを遮断する場合は以下の様に記述する．

deny tcp host x.x.x.x any eq 445

生成された ACL を元に，N/W 管理者は N/W 機器の制御を行い被害の拡大を抑止することが可能となる．

3.　検知のリアルタイム化

本システムでは主成分分析(PCA:Principal Component Analysis)を時系列データに含まれるパターンの変化の検知に利用している[1]．PCA の計算において SVD(Singular Value Decomposition)を利用しているが，従来の SVD の実装では処理が遅く，さらに分析対象の時系列データが増加・減少する場合に再計算が必要となりリアルタイムな検知に向かない課題があった．

そこで，アルゴリズムを改良しデータの増減に対しても高速処理が可能な SVD の実装を行った．その結果，従来比で最大約 35 倍の高速化に成功しリアルタイムな検知を実現した[3]．

4.　検知性能の評価

システムの運用にあたり，検知における時系列データの集計時間やウィンドウサイズ[1]を調整し検知性能を最適化する必要がある.最適化の方法として，定常状態と不正アクセスが発生した場合の時系列データを用意し，集計時間とウィンドウサイズを組合わせて検知を試み，早期に検知する組合わせを抽出する方法がある[1]．

定常状態の時系列データは実際に適用する N/W 環境から採取する．一方，不正アクセス発生時の時系列データは様々な変動のパターンが想定されるが，N/W 環境においては不正アクセスを受けてもパターンが限定される可能性がある．従って，N/W 環境からは想定される全ての変動のパターンを採取することは困難なため，シュミレーションデータを利用することとした．

筆者らは，不正アクセス時のシュミレーションデータとして，疫学モデルに基づくデータと，不正アクセスの時系列のデータ形状を分類したデータを用意し，これらを利用した評価を行った[4]．

5.　おわりに

主成分分析を利用した不正アクセス分析システムにおける課題であった，対策の仕組みの開発，検知のリアルタイム化，検知性能の評価を行った．

今後は，対策機能を拡張しさらにきめ細かな N/W 機器の制御を行う ACL の生成を目指す．また，実際に監視対象の N/W において運用を予定している．

参考文献

[1] 定点観測による不正アクセス分析システム，榊原他，CSEC 38
[2] IP アクセスリストの設定 http://www.cisco.com/japanese/warp/public/3/jp/service/tac/707/confaccesslists-j.pdf
[3] 定点観測による不正アクセス分析システム－不正アクセス検知のためのネットワークログ分析手法－,鹿島他，IPSJ 69 回全国大会予稿集
[4] 定点観測による不正アクセス分析システム－検知性能の評価－,大野他，IPSJ 69 回全国大会予稿集

[1]複数のポートにアクセスするワームについては，通信パターンはホストスイープと同一とみなす．