不正アクセスシナリオの導出に向けた検知ログ解析

3H－01

久保田　和己　鳥居　悟　小谷野　修
富士通株式会社

1　はじめに

分散型サービス不能攻撃（DDoS）攻撃に代表されるネットワーク上の不正アクセス攻撃に対して、実被害を回避するためのセキュリティ機構が必要である。従来の侵入検知ツールで広く採用されている検知手法では、攻撃を構成する断片的な振舞いの検知やシステムの状態変化だけを監視しているため、誤った警報を挙げてしまったり、実際の攻撃が発生した時点でしか攻撃検知を行うことができないといった問題が存在している。特にDDoS攻撃の場合、一般的なアクセスと明確な区別がつけにくく、実際に攻撃が開始されてしまってからでは対処が間に合わないため、これらの検知手法だけでは不十分である。

そこで、我々は不正アクセス攻撃のモデルを元に、単独事象だけではなく複数の事象発生を時間的、空間的に関連付けて不正アクセス攻撃の予兆もしくは予兆の候補となる事象を導くための解析手法の研究を行っている。このためには、複数の侵入検知ツールで検知された不正アクセスイベントの中から発生した順序や対応関係を見つけ出し、関連する事象を一連の攻撃の手順（シナリオ）として導き出す必要がある。

本稿では最終的な目標であるDDoS攻撃における実被害を回避する機構の実現に向け、その第一歩として、不正アクセスシナリオの導出を目的として行った検知ログの解析実験について報告する。

Sequential pattern analysis on IDS event logs for deriving intrusion scenarios.
Kazumi Kubota, Satoru Torii, Osamu Koyano
Fujitsu LTD.

2　解析対象ログデータの概要

本解析実験で対象としたデータは、複数の侵入検知ツール（IDSツール）の検知ログであり、発生時刻、検出した不正アクセスイベントの種類、発信元、送信先のIPアドレスとポート番号などが記録されている。これらの情報は、IDSツールが不正なアクセスとして検知を行うごとに1レコードが出力される。不正アクセスイベントの種類の項目にはIPHarfScan、Smurf等のシグネチャの粒度のレベルで記録される。

分析に使用したデータの概要を次に示す。

- 記録期間　約12週間
- レコード数　約246万レコード
- 発信元IP数　約2万5千種類
- 送信先IP数　約57万6千種類
- 検知イベント　126種類

なお、本実験に用いたログは、独立した18個のクラスCまたはクラスBのネットワークを監視するIDSツールが出力したものである。また、発信元IPについてはspoofされたものである可能性があるが、ここではログに記録されたものをそのまま採用した。

3　イベントシーケンスの抽出

関連する事象を一連の攻撃の手順として導き出すためにログに含まれるイベントデータを発生時刻に沿って時系列に解析し、イベントシーケンスの切り出しを行った。

イベントシーケンスとは、ある発信元IPからある送信先IPに対して連続して行われた不正アクセスイベントの時系列の並びである。例えば

IPHalfScan->TraceRoute は長さが 2 のシーケンスである。組合せ的にはイベントシーケンスのパターン数は「イベントの種類」のべき乗となり、長さが長くなるにつれてパターン数は膨大となるが、実際のログから抽出されたシーケンスでは次第に頭打ちとなった。今回の実験ではログ上に記録されている長さ 2 から 12 までのすべてのシーケンス約 51 万種類を抽出し解析に用いた。

4　解析実験により得られた知見

上記のシーケンス情報から以下の知見が得られた。

(1) 発生イベント間の前後関係

上記のシーケンスの中から、長さ 3 のシーケンス 5393 個を選択し、あるイベントの前後でどのようなイベントが発生しているかを各シーケンスパターンが発生した件数を数え上げて分析した。長さ 3 のシーケンスにはその順列により 6 通りの並びがありえる。これらの間で発生数に統計的な差があるかどうかを判定した。その結果、一部のイベントシーケンスには発生する順序が固定的なものと、順不同であるものが存在することがわかった。

(2)　発信元と送信先の分布

発生したイベントの発信元と送信先を軸にとり、イベントの発生回数を 2 次元にプロットした(図 1)。ここでは全体的な傾向を見るため IP アドレスの 1 オクテット目を用いた。その結果 y=x の直線を軸として大部分のイベントが対称な分布をしていることがわかった。分布が対称になるということは、発信元と送信先が逆転したイベントが IDS により検知されている可能性を意味する。

(3) 発生イベント間の呼応関係

上記の分布で対称となるイベントの呼応関係をみるために、あるイベントが発生した後 5 秒以内に発信元と送信先が逆転したイベントが記録されている部分を抽出し、どのイベント同士が対応関係をもっているかを解析した。その結果 58 種類のイベントの呼応関係が抽出できた。この呼応関係のあるイベントに関して前述の発信元と送信先の分布との比較を行った結果、対称となった分布はイベントの対応関係によるものであることがわかった。

5　今後の課題

今後は解析実験で得られた知見をもとにして、不正アクセスの攻撃モデルの構築につなげていきたいと考えている。

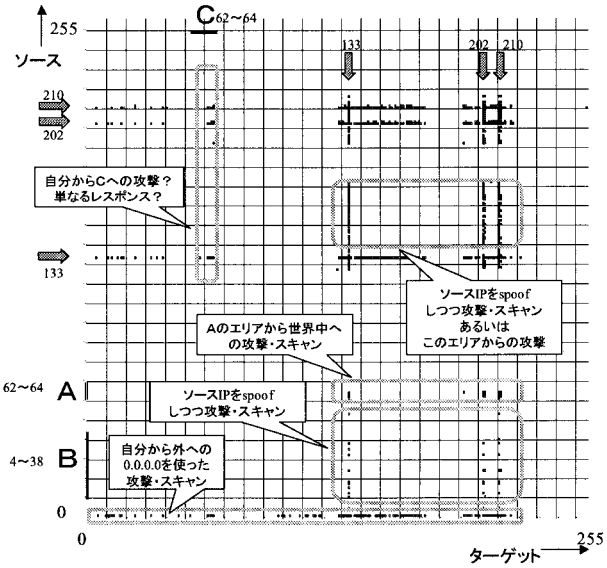

図 1　発信元と送信先の分布

謝辞

本研究は，通信・放送機構の委託研究テーマ「サービス不能化(DDoS)攻撃に対する防御技術に関する研究開発」の一環として行なわれているものである。

参考文献

[1] K.J.Houle, G.M.Weaver, *"Trends in Denial of Service Attack Technology,"* CERT/CC, Oct. 2001

[2] 鳥居 他, 不正アクセス予知回避機構の提案, 情報処理学会　第 62 回全国大会　特別セッション 6F-05, 2001 年 5 月

[3] 久保田 他, 認証エラーの傾向分析による不正ホストの絞込み情報処理学会　第 62 回全国大会　特別セッション 6F-04, 2001 年 5 月