6Q-04

不正アクセス発信源追跡システムのモデル検討

小久保 勝敏　渡辺 英俊　松田 栄之
(株) NTT データ　情報科学研究所
e-mail: {kokubo, hidetosi, matu}@rd.nttdata.co.jp

寺西 俊晴　巻田 政好　加藤 幹一郎
東日本電信電話株式会社　法人営業本部マルチメディア推進部
e-mail: {teranisi, makita, kan}@mm.bch.east.ntt.co.jp

1. はじめに

インターネットは、ビジネスや社会のインフラとして、重要な役割を担っている。しかし、インターネットを経由した不正侵入やサービス妨害等の悪質な行為が年々目立ってきており、その防止策が求められている。

本稿では、インターネットを利用した不正アクセスの発信源を追跡するシステムについて検討し、追跡を実現するための構成要素とその課題について述べる。

2. 発信源追跡に対する問題点と要件条件

インターネットにおける不正アクセスの対策として、Firewall によるアクセスコントロールや、IDS (Intrusion Detection System) による不正アクセスの検知等の防御技術が普及してきている。その一方で、不正アクセスの発信源を特定することが、対策の一つとして効果が大きいと考えられる。

発信源を特定するには、通常、IP パケットに格納されている送信元 IP アドレスを元に、nslookup や whois 等のコマンドを使用して情報を収集するのが一般的である[1]。また、不正アクセスの場合には、特定したホスト等が踏み台となっているケースも想定されるため、これに対応する追跡技術の研究が行われている[2]。しかし、送信元 IP アドレスは容易に偽造でき、送信元 IP アドレスが偽られていた場合は発信源の追跡は困難となる。不正アクセスの中でも、Flood 系攻撃や OOB(Out of Band)攻撃などは、送信元 IP アドレスを偽った場合でも効果があり、その場合には、追跡が困難で、効果的な防御も難しい。

A study of unauthorized access tracing system

Katsutoshi KOKUBO, Hidetoshi WATANABE and
Shigeyuki MATSUDA,
Laboratory for Information Technology, NTT DATA CORPORATION
Toshiharu TERANISHI,Masayoshi MAKITA and Kanichiroh KATO,
Multimedia Business Department,
NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION

また、未知の手法による不正アクセスに迅速に対応することは、不正アクセスの防止策として重要である。現在の多くの IDS では、既知の不正アクセスの特徴をデータとして保持し、その特徴とネットワーク上のパケットの内容とを比較して不正アクセスを検知する。また、その他の手法として、実際のアクセスの統計により得られた通常時のアクセスパターンと比較することにより、異常なアクセスを検知する研究もある[3]。しかし、この手法では不正アクセスを行う者が故意に統計データを変化させる事が可能であり、検知結果の正当性の判断が困難である。

さらに、発信源追跡システムに対する不正行為からシステムを防御することも必要となる。

以上をまとめると、インターネットにおける発信源追跡のための要求条件は以下のようになる。

- 送信元 IP アドレスが偽られた場合を想定し、IP アドレスのみによらずに追跡が行えること。
- 未知の手法も含めた不正アクセスが検知できること。
- 追跡システム自体に対する不正行為からシステムを防御できること。

3. 発信源追跡システム

3.1. 追跡範囲と対象不正アクセス

提案するシステムの追跡範囲は以下の通りとする。

- TCP/IP ネットワークを対象とする。
- 不正アクセス発信源ホストの真の IP アドレス、または所属するネットワークのアドレスの特定を目標とする。
- ただし、踏み台を介して不正アクセスされている場合には、その踏み台にされているホストまでを追跡の対象とする。
- WWW サーバ等のインターネットサーバを対象とした不正アクセス、特にアドレス偽造されても効果がある不正アクセスを対象とする。

3.2. 基本的な追跡の仕組み

2 章で示した要求条件を踏まえて、インターネットサーバへの不正アクセス発信源追跡システムを提案する。

送信元 IP アドレスが偽造されたパケットは、その偽った先の送信元IPアドレスを持つホストから中継される経路とは異なる経路で到達すると考えられる。したがって提案するシステムでは、中継機器にパケットが通過した記録を残し、その記録をもとにパケットの到達点から順に発信源に向かって辿っていく。また、中継機器が本来の「中継機能」を著しく妨げることが無いよう、追跡全体を制御する機器を別に設け、中継機器には一定量の記録だけを残す形態をとる。

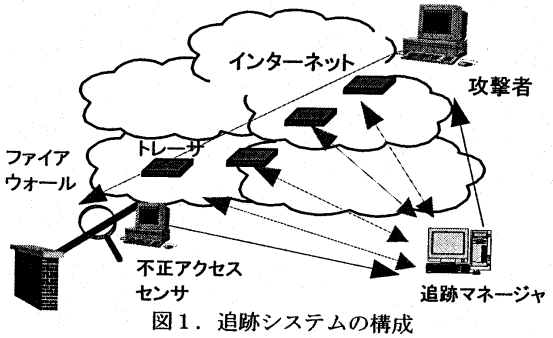

図１．追跡システムの構成

3.3. 発信源追跡システムの構成

提案する不正アクセス発信源追跡システムの構成を図１に示す。

システムは、主に、トレーサ、追跡マネージャ、不正アクセスセンサから構成される。各構成要素の機能を以下に示す。

（1）不正アクセスセンサ

未知の不正アクセスを含め、不正アクセスを検知し、追跡マネージャに追跡依頼を出す機能を有する。

（2） 追跡マネージャ

不正アクセスセンサからの追跡依頼をもとに、複数のトレーサを制御することによって、追跡全体を管理する機能を有する。

（3）トレーサ

中継する IP パケットの情報を保持する機能と、追跡指示に対して、追跡指示に含まれる追跡対象のパケット情報と保持した情報の比較から、追跡方向を検出し、その結果を返す機能を有する。トレーサは、ルータ等の中継機器に実装される。

また、システム全体、及び、各構成要素の不正利用防止のための認証、暗号通信等の仕組みを有する。

4. システム実現上の課題

不正アクセス発信源追跡システムを実現する際の課題を以下に述べる。

- トレーサと追跡マネージャの連携方式及び通信プロトコル等、追跡全体のアーキテクチャの確立[4]
- アクセスパターンの統計だけによらない、未知の手法も含めて不正アクセスを検知する技術の実現[5]
- 追跡システム自体に対する不正行為からシステムを防御する技術の実現[6]

5. おわりに

インターネットにおける不正アクセスを防止するために、不正アクセスの発信源を追跡するシステムを提案した。すでに、4 章で述べたシステムを構築する上での課題に対する検討を進めており、今後は、プロトタイプシステムの開発とその評価を行う予定である。

6. 謝辞

本研究は、通信・放送機構（TAO）の委託研究テーマ「不正アクセス発信源追跡技術に関する研究開発」の一環として行われているものである。

参考文献

[1] E. Amoroso, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response", Intrusion.Net Books, Sparta, New Jersey, 1999.

[2] M. Asaka, "Information-Gathering with Mobile Agents for an Intrusion Detection System", *Systems and Computers in Japan*, Vol.30 No.2, pp.31-37, 1999.

[3] P.A. Porras and P.G. Neumann. "EMERALD: Event monitoring enabling responses to anomalous live disturbances". In *Proceedings of the 20th National Information Systems Security Conference*, pp. 353-365, October 1997.

[4] 竹爪他, “不正アクセス発信源追跡アーキテクチャの一検討”, 情処 60 全大, 6Q-06, Mar 2000

[5] 馬場他, “プロトコル仕様及びポリシー情報を利用した不正アクセス検知方式の検討”, 情処 60 全大, 6Q-05, March 2000

[6] 巻田他, “不正アクセス発信源追跡システムの不正利用防止アーキテクチャの検討”, 情処 60 全大, 6Q-08, March 2000