6Q-06　不正アクセス発信源追跡アーキテクチャの一検討

竹爪 慎治† 松田 栄之‡ 渡辺 英俊‡ 柳田 正博‡ 小久保 勝敏‡
(株)NTT データ †公共地域ビジネス事業本部 ‡情報科学研究所
e-mail: †taketsumes@noanet.nttdata.co.jp, ‡{matu, hidetosi, yanagida, kokubo}@rd.nttdata.co.jp

1. はじめに

インターネットを経由した不正アクセスを検知し、その発信源を特定する不正アクセス発信源追跡システムの研究を行っている[1]。本稿では、パケットの送信元 IP アドレスが偽造された不正アクセスであっても、その発信源を特定できる不正アクセス発信源追跡アーキテクチャ(以下、追跡アーキテクチャ)を検討する。

2. 追跡アーキテクチャの要求条件

追跡アーキテクチャの要求条件を以下にまとめる。

① 不正アクセスの発信源情報として、発信源ホストの IP アドレスあるいは発信源ホストが接続しているネットワークのネットワークアドレスが特定できること。

② パケットの送信元 IP アドレスが偽造された不正アクセスであっても、発信源情報が特定できること。

3. 不正アクセス発信源追跡アーキテクチャ

3.1. 発信源追跡の基本方式

提案する追跡アーキテクチャでは、上記の要求条件を満たすために、発信源追跡の基本方式として Ethernet における MAC アドレス等の下位層フレームあるいはセルの識別子(以下、データリンク層識別子)を活用する。

一般に、パケットの送信元 IP アドレスは、発信源側で容易に偽造することができる[2]。一方、データリンク層識別子は、ルータ等の中継装置によって、フレームあるいはセル転送時に順次中継装置のインタフェースの識別子に書き換えられるため、発信源側で転送時にこれらを偽造することは困難である。したがって、各中継装置では、隣接する中継装置(以下、隣接ノード)のデータリンク層識別子とパケットに対応するデータリンク層識別子から、該当パケットが送信されてきた隣接ノードを確実に特定することができる。

提案する方式では、各中継装置において、転送したパケットとそれに対応するデータリンク層識別子を保存しておき、不正アクセスパケットと一致する転送パケットを検索することで隣接ノードを特定する(これらの機能を実装した中継機器をトレーサと呼ぶ)。隣接ノードの特定をターゲットサイトに接続しているトレーサから順番に各トレーサで行っていくことにより、送信元 IP アドレスが偽造された不正アクセスパケットであっても、最終的にその発信源を特定することが可能となる(図 1 参照)。

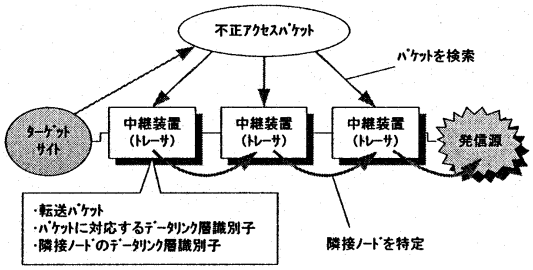

図 1 発信源追跡の基本方式

3.2. 追跡アーキテクチャの基本方針

追跡アーキテクチャの基本方針を以下にまとめる。

(1) 追跡管理範囲の導入

インターネットは大規模なネットワークであるため、追跡の制御や追跡に必要な情報の管理を一元的に行うことは不可能である。また、管理方針等の異なるネットワーク間で無制限に他のネットワークからの追跡を継続させることは困難である。そこで、追跡の管理範囲として、自律管理ネットワーク(以下、AMN: Autonomous Management Network)の概念を導入し、追跡の制御や情報の管理を AMN 毎に分散して行う。

(2) AMN 内の追跡制御

AMN 内における統一的な方針に基づく追跡および効率的な追跡関連情報の管理を実現するために、AMN 毎に追跡の制御や追跡関連情報の管理を集中的に行う追跡マネージャを導入する。

(3) AMN 間の追跡制御

追跡が AMN を超える場合、AMN 間の追跡状態の把握、追跡継続の判断等の全体的な追跡状態の管理は、追跡を開始した AMN の追跡マネージャが行う。

A study of architecture for unauthorized access tracing system
Shinji TAKETSUME†, Shigeyuki MATSUDA‡,
Hidetoshi WATANABE‡, Masahiro YANAGIDA‡,
Katsutoshi KOKUBO‡,
†Public Administration Community Business Sector,
‡Laboratory for Information Technology,
NTT DATA CORPORATION

3.3. 発信源追跡の流れ

追跡アーキテクチャにおける不正アクセス検知から、発信源特定までの流れを以下にまとめる(括弧内の数字は図2中の番号に対応する)。

① ターゲットサイトには、不正アクセスを検知する不正アクセスセンサが設置されている[1]。不正アクセスセンサは、不正アクセスを検知すると不正アクセスパケットの特徴情報を生成し、自分が所属するAMN の追跡マネージャに追跡を依頼する(1～2)。

② 追跡マネージャは、AMN 内のトレーサに追跡を指示する。トレーサは隣接ノードを特定して、追跡マネージャに追跡結果を返す(3～4)。

③ 追跡結果に従って、②を発信源が特定されるまで繰り返す(5～6、9～12、16～19)

④ 追跡がAMNを超える場合には、該当AMNを管理する追跡マネージャ(以下、依頼先マネージャ)に追跡を依頼する(7～8、14～15)。

⑤ 各AMNの追跡マネージャは、管理するAMN内で追跡を行い、追跡結果を統合して、追跡が開始されたAMNの追跡マネージャ(以下、依頼元マネージャ)に送信する(13、20)。

⑥ 依頼元マネージャは、最終的な追跡結果を不正アクセスセンサに送信する(21)。

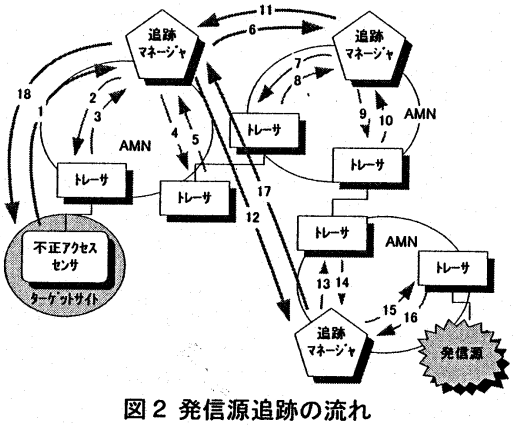

図2 発信源追跡の流れ

3.4. 通信メッセージと主なパラメータ

追跡アーキテクチャにおいて実際にやり取りされる通信メッセージを表1にまとめる。また、各メッセージにおける重要なパラメータを以下にまとめる。

(1) パケットフィーチャ

パケットを識別するのに必要な情報を抽出したパケットの特徴情報をパケットフィーチャと呼ぶ。トレーサは、転送パケットのパケットフィーチャと対応するデータリンク層識別子を保存し、不正アクセスパケットのパケットフィーチャから隣接ノードを特定する。パケットフィーチャのデータサイズは、実パケットと較べて小さいため、CPU、記憶装置、ネットワーク帯域等の追跡に必要なリソースをより効率的に使用することが可能となる[3]。

(2) 追跡判断結果

追跡マネージャは、不正アクセスセンサや他の追跡マネージャからの追跡依頼に対して、管理するAMN 内で追跡を行うかを判断し、必要に応じて拒否することが可能である。これにより、管理方針等に基づいて追跡を制限することや過負荷による追跡マネージャのサービス停止を防ぐことが可能となる。

表1 通信メッセージ一覧

メッセージ名 (重要パラメータ)	概要
追跡依頼 (パケットフィーチャ)	不正アクセスセンサから追跡マネージャに、発信源追跡を依頼する。
追跡判断結果 (追跡判断結果)	追跡マネージャから不正アクセスセンサに、追跡開始の判断結果を通知する。
統合追跡結果	追跡マネージャから不正アクセスセンサに、最終的な追跡結果を通知する。
AMN 間追跡依頼 (パケットフィーチャ)	依頼元マネージャから依頼先マネージャに、発信源追跡を依頼する。
AMN 間追跡判断結果 (追跡判断結果)	依頼先マネージャから依頼元マネージャに、追跡開始の判断結果を通知する。
AMN 間追跡結果 (パケットフィーチャ)	依頼先マネージャから依頼元マネージャに、AMN 内の追跡結果を通知する。
追跡指示 (パケットフィーチャ)	追跡マネージャからトレーサに、発信源追跡(隣接ノードの特定)を指示する。
追跡結果 (パケットフィーチャ)	トレーサから追跡マネージャに追跡結果を通知する。

4. まとめ

インターネットにおいてパケットの送信元 IP アドレスが偽造された不正アクセスであっても、その発信源を特定できる不正アクセス発信源追跡アーキテクチャを提案した。今後は、提案したアーキテクチャを実装したプロトタイプを開発し、追跡の精度等の評価を行う予定である。

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] 小久保他: 不正アクセス発信源追跡システムのモデル検討, 情処 60 全大, 6Q-04, Mar. 2000.

[2] Edward Amoroso, Intrusion Detection, Intrusion.Net Books, Sparta, NJ, 1999.

[3] 渡辺他: 不正アクセス発信源追跡のためのパケット識別情報の検討,情処 60 全大, 6Q-07, Mar. 2000.