パケット逆探知システム PAFFI™

PAFFI™ IP Traceback System

梅 澤 昭 生*1
UMEZAWA Akio

1. はじめに

近年のネットワーク回線の大容量化に伴い，DoS(サービス不能攻撃)やワームなどによるネットワーク攻撃が急増している。攻撃による対外サービス停止や内部ネットワーク麻痺，あるいは踏み台としての他者攻撃は，直接・間接的に大きな損失となりうる。さらに，検知後の素早い対策が求められてきている。2003年1月のSQL Slammer騒動以来，UDPパケットを使ったソースアドレス詐称タイプの不正アクセスが流行する可能性が高まったと言われている。

当社では，ソースアドレスが偽装されたパケットでも，実際にパケットが通過してきた経路を追跡することができるパケット逆探知システムPAFFI(パフィー)を開発した。また，PAFFIの簡易版としてIPトレースバック技術を実環境で確認していただくために，Petit PAFFI(プチパフィー)を開発した。後述のサイトからダウンロードして，無償で使うことができる。本稿ではPAFFIとPetit PAFFI，およびその手法であるIPトレースバック技術を紹介する。

2. IPトレースバック手法の種類と特長

「IPトレースバック」は，IPアドレスが詐称されているか否かにかかわらず，発信元と経路を素早く簡単に特定することを目的とした技術である。この手法には，追跡パケット方式，パケットマーキング方式，パケット記録方式，パケットハッシュ記録(Hash-Based)方式といったさまざまな手法が提案されている。ここでは，PAFFIが採用しているパケットハッシュ記録方式について，簡単に解説する。

本方式は，ネットワーク中の各所で監視記録したパケット情報を基に，問題のパケットの通過経路を調べる方式であり，以下の特長がある。

・1つのパケットだけでも追跡が可能である。
・記録したパケットハッシュ値から元のパケットを復元することが不可能なため，パケットの内容に関する直接的なプライバシーの問題は回避される。
・記録をハッシュ化することで，ストレージをそれほど必要としない。

本方式では，同じパケットがネットワーク中の各所で記録された場合，そのハッシュ値が全て同一になるようにする必要がある。そこで，IPパケットがネットワーク中を伝播する間にルータによって書き換えられてしまうTTL(Time To Live：パケット生存可能時間)などのフィールドをマスクした上で，ハッシュ値を算出している。

3. PAFFIの特長

PAFFIはネットワークにおいて，従来困難だったソースIPアドレス詐称型DoS攻撃等の流入口や，内部の不正アクセス発生(侵入したワーム等)元を素早く突き止め，事態収拾を強力にサポートし，以下の特長を持つ。

・ソースアドレスが偽装されたIPパケットの追跡
・効率的でレスポンスの早い追跡
・使用しているネットワークに影響を与えないパケット監視
・専用プロセッサの採用による高いパケットキャプチャ性能(ソフト版もあり)
・プライバシーの保護

4. PAFFIのシステム構成

PAFFIシステムは，**図1**に示すように単一組織内部に導入することを想定し，次のFootmarker，Manager，Gateの3つのサブシステムから構成される。

・Footmarkerは，ネットワーク各所に設置され，通過するパケットの特徴情報である“Footmark”と通過時刻を記録蓄積する。
・Managerは，Footmarkerに蓄積されたパケットの追跡と，Footmarkerの管理およびこれらを容易にするユーザインタフェースの提供を行う。
・Gateは，IDS等のさまざまなセキュリティ機器とManagerをつなぐゲートウェイの役割をする。

外部組織との接続をしている境界ルータや，各フロアおよびサーバセグメントのレイヤ2スイッチのアップリンクなどの要所にFootmarkerを配置する。Footmarkerは，Ethernetケーブルから直接ケーブルタップ装置で分岐して接続するか，あるいはミラーポートに接続する。

*1 技術開発本部 セキュリティプロジェクトセンター

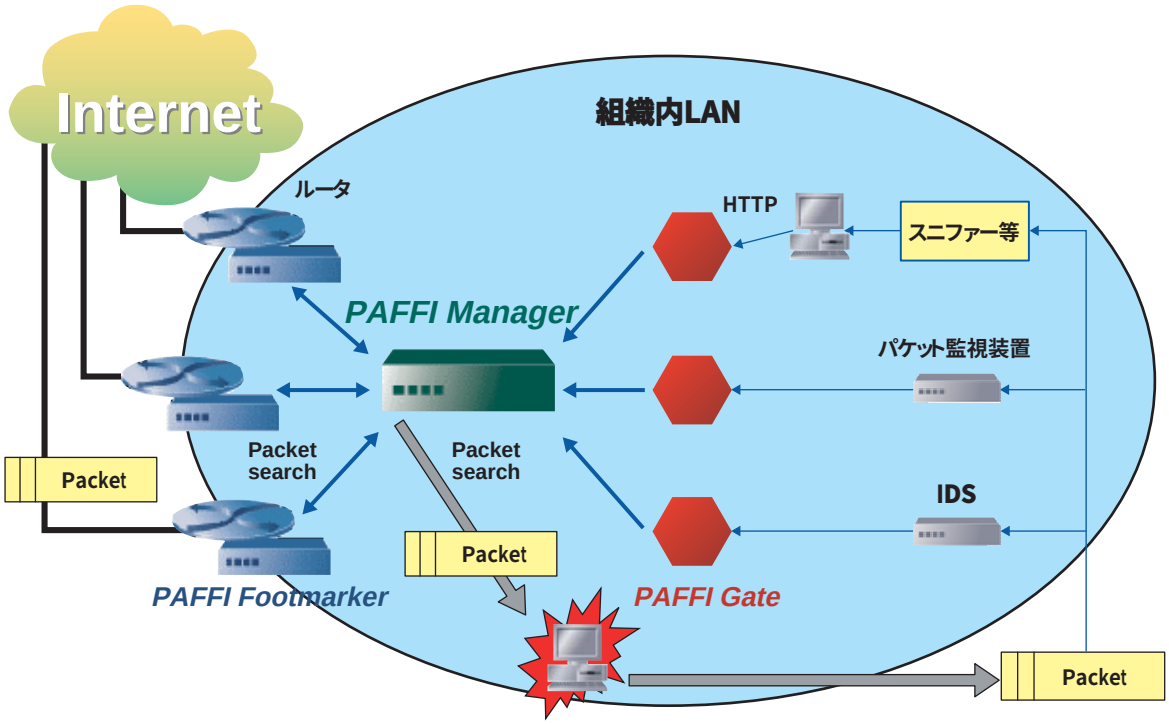

図1　PAFFIシステム

インターネットおよび外部組織との境界に設置されたIDSにより，不正アクセスが行われたことを検知する。IDSで検知したDoSやワームのトラフィックによるアラートを基に，PAFFI GateからPAFFI Managerを経由してFootmarkerへ問い合わせ，パケットの追跡を行うことで，組織内部のどのセグメントで問題が発生しているかを素早く突き止め，そのセグメントの隔離などの対策が可能である。

5.　Petit PAFFI とは

Petit PAFFIは，PAFFIをユーザの皆様にいち早く手軽に体験していただくために，無償で配布する簡易IPトレースバックシステムである。

本ソフトウェアは

http://www.paffi.net/

からダウンロードできる。

Petit PAFFIは，パケット検索ユーザインタフェースを提供するPetit Packetraceと，PAFFI Footmarkerと同様なパケット記録機能を持つPetit Footmarkerとで構成される。PAFFIと比べた場合，Petit PAFFIはFootmarkerを管理統合する機能，検索のレスポンス性能，Footmarkerの記録保持時間やネットワークインタフェースの数などが限定されている。

Petit Footmarkerをユーザが監視したいポイントに設置すれば，不正なパケットや疑わしいパケットの流入経路や攻撃元を逆探知することができる。本ソフトウェアは，今後リリース予定の有償版PAFFIとも接続が可能である。

6.　お わ り に

当社では，増大しつつあるネットワークの脅威に対する「社会への貢献」の一環としてPetit PAFFIを無償提供し，そのフィードバックをPAFFIの開発に活かしていきたい。

将来は組織内だけでなく，ISP，データセンタなど，広域ネットワークの脅威に対しても有効な手段を提供することを目指している。

問い合わせ先：セキュリティプロジェクトセンター
TEL：0422-52-6419
FAX：0422-52-5204
E-Mail：paffi@csv.yokogawa.co.jp