4X-5

フロークラスター記述言語を有する ネットワークトラヒック検査システムの提案

大見浩明† 立岩佑一郎‡ 片山喜章‡ 高橋直久‡

†‡名古屋工業大学大学院工学研究科

１．はじめに

送信元 IP アドレス(SIP)，送信元ポート番号(SPT)，送信先 IP アドレス(DIP)，送信先ポート番号(DPT)，プロトコル(PROT)が同じパケットの集合(フロー)単位でネットワークトラヒックを解析することでアプリケーションごとの通信時間帯や通信量を把握できるようになる[1]．フローを扱った解析手法も提案されている[2]．また，フローの因果関係に注目することで，事象の流れを把握し，異常に対して適切に対処できる場合がある．例として，踏み台ホストを利用した攻撃の場合についてみると次のようになる．攻撃者はまず踏み台ホストに侵入し，エージェントを仕掛ける．その後，攻撃者は踏み台ホストのエージェントに命令を送信（フローＡ）し，エージェントが他のホストへ通信（フローＢ）する。この場合にはフローＡの送信元が原因で，フローＢが発生しており，フローＡとＢに因果関係があるといえる．このフロー間の因果関係を把握するためにはエージェントが設置された踏み台ホストを特定し，そのホストの動作とホストが送受信したフローを調べる必要がある．

しかし，これには以下の問題点がある．

問題点１ フロー単体からフローＢがエージェントの行った通信であることを判別することは困難である．また，過去の動作に関するログも攻撃者に改竄されている可能性が高い．そのため，ホストの動作や通信から踏み台ホストを自動的に特定することは難しい．

問題点２ 攻撃者は複数の踏み台ホストを経由する場合がある．各踏み台ホストのフローを調べるだけでは，複数の踏み台ホストを経由したことを知ることはできない．

本稿では，これらの問題を解決するために，関連性のあるフローをまとめて提示するネットワークトラヒック検査システムを提案する．このシステムにより，ユーザがフロー間の因果関係を分析・検査する一助を提供する．

２．提案システムの概要

踏み台ホストを利用した攻撃の場合に，フローA，B はほぼ同じ時間帯に同じホストに存在している．この例を少し一般化して，同一空間（ホスト，サーバ，ネットワーク）上の近接時間帯に同時に存在する場合，これらのフローは共起性があるとみなす．また，共起性のあるフローの集合を強い関連性を有するとみなし，フロークラスターと呼ぶ．本稿では，フロークラスターに基づき注目すべきフローを提示するネットワークトラヒック検査システムを提案する．提案システムの特徴を以下に示す．

A Proposal of Network Traffic Checking System using Flow Cluster Description Language

Hiroaki Omi†, Yuichiro Tateiwa‡, Yoshiaki Katayama‡, and Naohisa Takahashi‡

Dept. of Computer Science and Engineering, Graduate School of Engineering, Nagoya Institute of Technology

表 1. フローの特徴パラメータ

フローの特徴パラメータ	意味
sip	送信元 IP アドレス
spt	送信元ポート番号
dip	送信先 IP アドレス
dpt	送信先ポート番号
prot	プロトコル
first	フローの発生開始時刻
last	フローの発生終了時刻
packets	フローに含まれる総パケット数
sizes	フローに含まれるパケットの総バイト数
dur	フローの持続時間(last-first)
end	フローの終了条件

表 2. クラスターの特徴パラメータ

フローが共起している時間・空間	フロークラスターの特徴パラメータ
ホスト	sip, dip
サーバ	sip, spt, dip, dpt, prot
ネットワーク	sip, dip
発生時間	first, last, dur

特徴１ フロークラスター記述言語の提供

フロークラスターを指定するルールの系列を記述するフロークラスター記述言語を提供する．この言語では，フローを表１のような特徴パラメータで表し，フロークラスターを表２のような特徴パラメータで表す．

特徴２ フロークラスターの検出と可視化

フロークラスター記述言語で書かれたルールの系列を順番に解釈実行することにより，指定されたフロークラスターの集合を検出し，可視化する．

提案システムは図１に示すように，フローデータ導出機能，中間コード生成機能，フロークラスター検出機能，アクション実行機能から成る．提案システの動作手順を以下に示す．ここでは，あらかじめパケットをキャプチャしてパケット DB に格納してあるとする．

STEP1 フローデータ導出機能は，パケット DB からパケット系列を読み出し，それを要素とするフローを導出し，フローの特徴パラメータをフローDB に格納する．

STEP2 中間コード生成機能は，管理者が事前に記述したパケットクラスター集合のルール系列を中間コードに変換する．

STEP3 フロークラスター検出機能は，中間コードを解釈実行してフロークラスターを検出し，フロークラスターDB に格納する．また，アクション実行機能は検出結果及び各ルールで指定された検出時の動作に基づいて，ログファイルを作成し検出結果を可視化する．

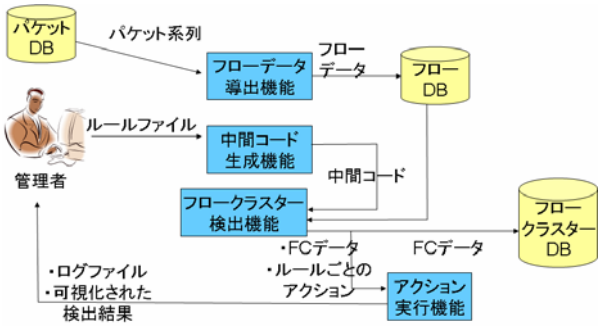

図１．システム構成図

３．提案システムの実現法

本章ではフロークラスター検出機能の実現法について述べる． 本機能における入力はフローの集合とルール，出力はフロークラスターである．クラスターの検出はルールで指定された特徴パラメータの値の持つべき条件(パラメータ条件)を満たすフローを要素とする集合を構成することで行う．

３．１．フロークラスター記述言語

本節ではフロークラスター記述言語におけるパラメータ条件について詳細に述べる．

パラメータ条件はフローのパラメータ名(key)，key と比較する値(value)，key と value を比較する条件(op)により構成される．value では以下の 2 種類の値を用いることができる．

予約値　あらかじめ決めた値

依存値　他のクラスターに属するフロー(参照フロー)のパラメータの値

各値を用いて検出可能なクラスターの例を以下に示す．

例(予約値)．特定のホストを発生元とするフロー

「あらかじめ決めたホストから発生したフロー」を要素とするクラスターを検出する．検出可能なクラスターの具体例を図２に示す．

例(依存値)．あるフローの発生先から発生したフロー

「検出したクラスターに属するフローの発生先を発生元とフロー」を要素とするクラスターを検出する．検出可能なクラスターの具体例を図３に示す．

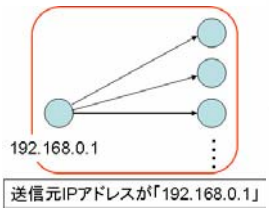

図２．クラスターの例１

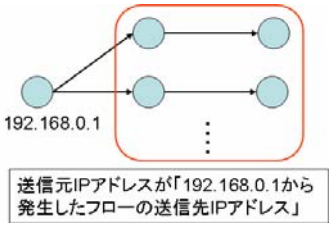

図３．クラスターの例２

３．２．フロークラスター検出機能の実現手順

フロークラスター検出機能は特徴パラメータの value の種別に応じた処理を実行する．それぞれを用いた処理の実現手順を以下に示す．

予約値を用いた場合の処理の実現手順

STEP1 フローの集合からフローを１つ選択する．

STEP2 選択したフローのパラメータがパラメータ条件を満たしているかどうかを判定する．判定は，条件式を選択したフローのパラメータとパラメータから作成し，その条件式の真偽により行う．真ならば選択したフローをクラスターの要素とする．条件式の作成例を図４に示す．

STEP3 集合の全てのフローに対して STEP1-2 を実行する．

依存値を用いた場合の処理の実現手順

STEP1 フローの集合からフローを１つ選択する．

STEP2 クラスターから参照フローを１つ選択し，パラメータの値を読み出す

STEP3 選択したフローのパラメータがパラメータ条件を満たしているかを判定する．判定は，条件式を選択したフローのパラメータ，参照フローのパラメータ及びパラメータから作成し，その条件式の真偽により行う．真ならば選択したフローをクラスターの要素とする．条件式の作成例を図５に示す．

STEP4 クラスター内に参照フローとして用いていないフローがなくなるまで，STEP2-3 を実行

STEP5 集合内の全てのフローに対して STEP1-4 を実行

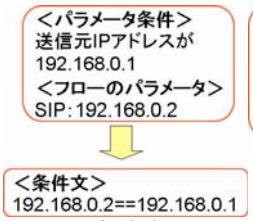

図４．条件式の例１

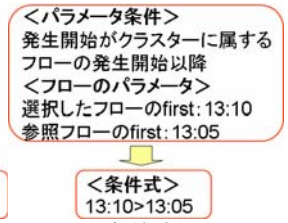

図５．条件式の例２

４．プロトタイプシステム

提案システムのプロトタイプの出力例を図 6，図 7 に示す．図 6 は検出結果を可視化したものである．頂点をホスト，辺をフローとしたグラフ形式で可視化が行われる．ホスト間のフローの数，パケット数，サイズが，辺の太さとして反映される．図 7 は検出結果のログである．各クラスターに属するフローの ID とパラメータが出力される．依存値を用いた場合，真となった条件式の作成に用いた参照フローも出力する．

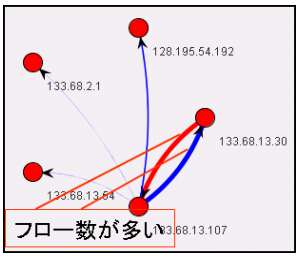

図６．可視化の例

図７．ログの例

５．おわりに

本稿では，パケットクラスター記述言語を用いたネットワークトラヒック検査システムを提案した．パケット系列をフローに再構成し，その中から指定された共起性を持つフローの集合をフロークラスターとして検出することが可能である．

参考文献

(1) Cisco IOS Net Flow: http://www.cisco.com/en/US /products/ps6601/products_ios_protocol_group_home.html

(2) Y.Shomura, Y.Watanabe, and K.Yoshida, "Analyzing the number of variety in frequent found flows," IEICE Trans. Commun., vol.E91-B, no.6, pp.1896-1905,June 2008.