4X-6

侵入検知機能を用いたフロークラスタ診断システム

青木滋† 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情報工学専攻†‡

1. はじめに

現在，ネットワークを経由した不正侵入が，社会的に大きな問題となっている．組織内のネットワークの安全性を確保するために，ファイアウォールとともに侵入検知システムの利用が進んでいる．侵入検知システムは不正侵入を検知して，管理者にアラートを発するもので，これにより不正侵入による被害の早期発見が可能になる．しかし，従来の侵入検知システムでは誤検知により通常の通信に対しても多数のアラートを発することが大きな問題となっている[1]．侵入検知システムでは，大量に発生するアラートログの把握が困難であり，効果的なシステムの運用を行うことは容易ではない．

本稿では，上記問題を解決するため，侵入検知機能が発するアラートから，不正アクセスの可能性があるフロー集合（フロークラスタ）を求めて可視化するフロークラスタ診断支援システムを提案する．このシステムの特徴を以下に示す．

特徴 1 アラートの発生元となったパケットから，不正アクセスの可能性が高いパケットフロー集合（フロークラスタ）のパターンを求める機能を実現する．

特徴 2 求めたフロークラスタパターンが，実際のトラヒック内に存在するかどうか検査し，存在した場合ユーザに知らせる機能を実現する．

これらの機能により，ユーザが大量のアラートログの中から不正アクセスの可能性が高いアラートを判別するための支援を行う．

2. 提案システムの概要

2.1 フロークラスタ

フロークラスタとは，フローの「共起性」に着目して関連性のあるフローをまとめたものである．フローの共起性とは，2つのフローが同じホストや同じネットワークに同時に存在していることを意味して，フローの関連性の強さを表す．注目するフローの出現場所と出現時刻に基づいてフローの共起性を指定して，関連性の強いフローの集合を求めたものがフロークラスタである．

フロークラスタの特徴をパターンとして記述したものをフロークラスタパターンと呼ぶ．図1に不正アクセスの例として，MSBlastワームの感染プロセスを示す．

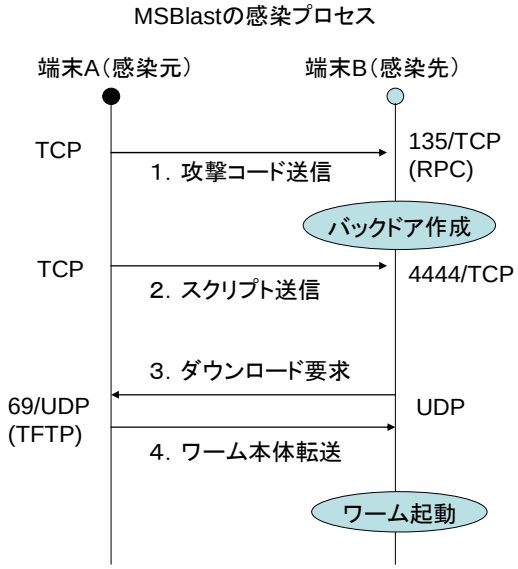
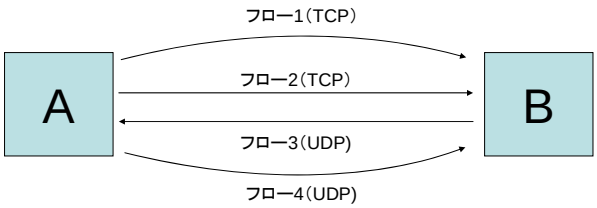


図 1: 不正アクセスの例

図 1 の通信で発生したパケットに対して，それぞれパケットヘッダ情報を用いて表現できるフローを作成し，フロークラスタパターンを構成すると図 2 のようになる．sip は送信元 IP アドレス，spt は送信元ポート番号，dip は送信先 IP アドレス，dpt は送信先ポート番号，prot はプロトコルの種類を表す．



(a) 図式表現

Flow Cluster Diagnosis System using Intrusion Detection Function

†Shigeru Aoki, ‡Yuichiro Tateiwa, ‡Yoshiaki Katayama, ‡Naohisa Takahashi
†‡Dept of Computer Science and Engineering, Nagoya Institute of Technology

```
1. sip==A, dip==B, dpt==155, prot==tcp
2. sip==A, dip==B, dpt==4444, prot==tcp
3. sip==B, dip==A, dpt==69, prot==udp
4. sip==A, spt==69, dip==B, prot==udp
```

(b) フロークラスタ記述言語[2]による表現

図 2　フロークラスタパターンの例

2.2　提案システムの構成

提案システムは図２に示すように，アラート解析機能，フロークラスタルール生成機能，フロークラスタ検出・可視化機能，フロークラスタ分析機能からなる．以下に各機能の概要を示す．

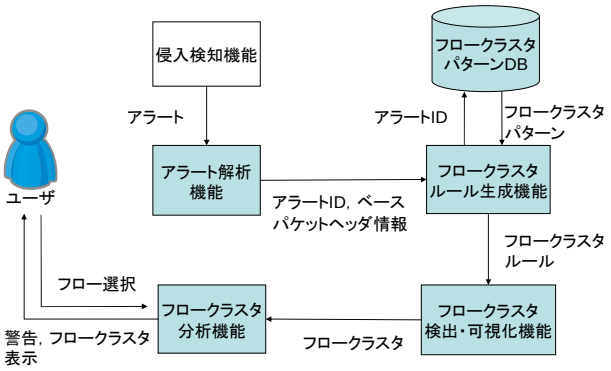


図 3:　システムの構成図

（1） アラート解析機能

侵入検知機能の発するアラートから，アラート ID とアラートの発生原因となったパケット（ベースパケットと呼ぶ）のヘッダ情報を求める．これにより，アラートと関連パケットを結びつけることが可能になる．

（2） フロークラスタルール生成機能

あらかじめ作成したフロークラスタパターンデータベースから，アラート ID に対応するフロークラスタパターンを検索する．さらに，パケットヘッダ情報を用いて，フロークラスタパターンを具体化してフロークラスタルールを生成する．これにより，アラートに関連したフロークラスタを抽出することが可能になる．

（3） フロークラスタ検出・可視化機能

ネットワークを監視しパケットをキャプチャすることにより得られるフローDB から，（2）で生成されたフロークラスタルールによりフロークラスタを抽出し可視化する．これにより，アラートに関連するフローを辺とし，各フローの送受信ホストを頂点とするフロークラスタグラフが得られる．

（4） フロークラスタ分析機能

フロークラスタ検出機能で得られたフロークラスタがフロークラスタパターンと一致するかどうか判定を行う．また，フロークラスタグラフを観察し，関連フローの詳細を分析する．これにより，関連フローの一覧表示や，フローの詳細情報を得て，アラートの発生原因を探求することが可能になる．

3.　システムの実現法

提案システムの主要機能の実現法を述べる．

3.1　フロークラスタルール生成機能

STEP1 アラート ID をキーとして，フロークラスタ DB を検索する．

STEP2 DB 内に一致するアラート ID が見つかった場合，アラート ID に対応するフロークラスタパターンを返す．

STEP3 STEP2 で得られたフロークラスタパターンに，ベースパケットヘッダ情報から得られる実際の IP アドレスやポート番号を当てはめ，フロークラスタルールを生成する．

3.2　フロークラスタ検出・可視化機能.

STEP1 フローDB からフロークラスタルールに一致するフロークラスタを検出する．

STEP2 STEP1 で得られたフロークラスタを，辺をフロー，頂点を各フローの送受信ホストとしたグラフとして可視化する．

3.3　フロークラスタ分析機能

STEP1 フロークラスタが，フロークラスタパターンと一致するかどうか判定する．一致した場合は STEP2 へ進み，一致しなかった場合はアラート解析機能へ戻る．

STEP2 アラート解析機能で入力されたアラートと，アラートに関連するフローの一覧をユーザに表示する．

STEP3 ユーザがフロー一覧から選択したフローについての詳細情報を表示する．

4.　おわりに

本稿では，侵入検知機能が発するアラートを元にしたフロークラスタ診断システムを提案した．アラートの発生源となったパケットに関連するフローを調べることで，誤検知の判別と原因究明の支援を行う．

参考文献

[1]藤田直行：侵入検知に関する誤検知低減の研究動向，電子情報通信学会論文誌．B, Vol. J89-B, No. 4, pp. 402-411, 2006.

[2]大見浩明，立岩佑一郎，片山喜章，高橋直久：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，第 74 回情報処理学会全国大会 4X-5, 2012.