ネットワークフォレンジックシステム向け トラフィックデータ保存専用ファイルシステムの開発

井上喬視† 中島 潤†
†北海道情報大学

1 はじめに

ネットワーク上の全トラフィックを収集し、長期間保存することによってセキュリティインシデント等の発生時に調査を行うシステムとして、ネットワークフォレンジックシステム（NWFS）が注目されている。NWFSはセキュリティ対策としてだけでなく，組織の内部統制支援やe-Discovery制度による証拠開示の必要性に備えるシステムとしても期待されている。

NWFSを用いた調査では，保存された膨大な量のトラフィックデータから目的の通信を取り出して行われるが、通信の検索や抽出といった処理には計算コストがかかるため、迅速なインシデントレスポンスが必要な場合において問題となっている．

そこで本稿では技術的課題を解決するため、NWFSでトラフィックを保存することを前提とした，トラフィックデータの保存手法を提案する。本提案手法はファイルシステムの仕組みを用いての通信フローの単一ファイル化や、時間軸での検索インデックス構築により、通信フローの検索・抽出処理に係るコスト軽減を図る。また、トラフィックデータの証拠性確保のための改ざん防止の仕組みや、システムの長期運用を可能にするディスクのローテート機能といった機能により，NWFSに貢献できるものとした．

2 ネットワークフォレンジックシステム

2.1 概要

本研究で対象としたNWFSは，一般的にFig.1に示すような構成で実現される．まずLANトラフィックは，通信経路上にて複製が行われ，NWFSによって収集される．収集されたトラフィックはPCAPフォーマット等の汎用的な保存形式を用いてファイルストレージ等に時間やサイズ単位で分割してファイル保存される．そ

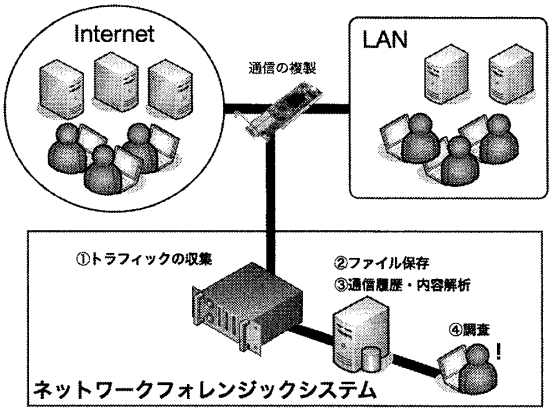

図1: ネットワークフォレンジックシステム

の後．トラフィックデータに含まれる通信フロー情報の解析が行われ，解析結果のデータベースが構築される．調査の際には，このデータベースをもとに通信履歴や内容の検索を行い，検索結果を元にトラフィックデータ内から通信フローの取り出される．

本稿ではこのうち，トラフィックデータの保存と解析処理に関する問題点に着目している．

2.2 トラフィックデータの保存と解析処理に関する技術的課題と要求

NWFSでは，長期間に渡って全LANトラフィックの収集を行うため，膨大な量のトラフィックデータが保存されることになる．このときトラフィックデータはサイズや時間で分割してファイル保存されるが，NWFSにおいては通信フロー単位でインシデント調査が行われる点から，本来は通信フロー単位で分割されて保存されていることが望ましい．しかしながら，通信フロー数はトラフィック量に応じて増加し，作成されるファイル数が膨大となる点や，既存汎用ファイルシステムやOSによる制約条件から，通信フロー毎に分割してのファイル保存は実現が困難である．また，保存されたトラフィックデータに対して証拠能力が求められる

File System for Exclusive Use of Traffic Data for Network Forensic System
Takashi INOUE†, Jun NAKAJIMA†
†Hokkaido Information University
069-8585, Hokkaido, Japan

ため，改ざんが困難であることや，連続的に保存可能な仕組みが要求されている．

3 トラフィックデータ保存専用ファイルシステム

本章では，前章で挙げた技術的課題を解決するアプローチとして，ファイルシステムの仕組みを用いてトラフィックデータの保存手法を提案する．

3.1 概要

提案するファイルシステムでは，トラフィックデータをディスク保存前に解析し，トラフィックデータに含まれる通信フローについて検索用インデックスを作成した後にディスクに対して書き込みを行う，それぞれの通信フローに対して inode 情報を付与することによって通信フローをファイルとしてユーザに提示する．

3.2 ディスクに対する書き込み処理

NWFS において保存すべきデータの発生源は，ネットワークデバイスからのトラフィックデータに限定される．そのため，ディスクに対してファイルシステム内部からのみ書き込みを行うものとし，ユーザ空間からの書き込みを不可能とすることができる．

このようにして収集されたトラフィックデータは，ある一定サイズまでバッファリングし，トラフィックデータ内のパケットを IP アドレスとポート番号によって通信フローごとに分類をおこなう．この分類された通信フローに対してそれぞれ inode 情報の付与を行い，通信フローのファイル化を実現する．さらに，このとき分類に用いた通信フロー情報を用いて索引インデックスを作成することによって，通信フローの検索にも同時に対応する．このようにして分類処理が行われたトラフィックデータは，inode 情報や通信フローインデックスとともに，まとめてディスクに書き出される．

このとき，nilfs[2] に代表されるログ構造化ファイルシステムと同様に，ディスクの先頭位置からシーケンシャルに書き込み行うことにより，ディスクシークを最小限に押さえることが出来るため，読み書き両方の速度向上が期待できる．

3.3 通信フローインデックス

時間軸によるページ検索の為のインデックスと，ページ内の通信フローを検索するためのインデックスの 2 つを作成する．これらインデックス作成の為のアルゴリズムは文献 [2] を踏まえ，B-Tree とした．

3.4 ディスクレイアウト

本提案ファイルシステムの大まかなディスクレイアウト構造を Fig.2 に示す．本提案では，ディスクを固定長ページに分割し使用する．先頭のスーパーブロックにはファイルシステム全体の設定情報や，最後に書き出したページの位置などが記録される．ページ内にはトラフィックデータが通信フロー分類された状態で格納され，ページの最後には通信フローの管理情報が配置される．通信フローの管理情報は，inode 情報や，IP アドレスやポート番号といった通信フローの検索に用いる情報が含まれる．

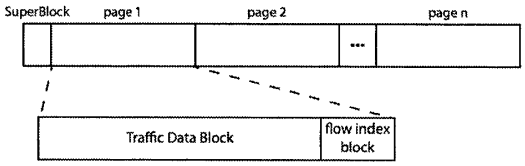

図 2: ディスクレイアウト

3.5 実装

本研究では実装の容易さを考慮し，FUSE を用いてファイルシステムを実装した．この実装により通信フロー単位でファイルとして提示可能である事を確認した．

4 まとめ

本稿では NWFS におけるトラフィックデータの保存・解析処理に関する技術的課題を示し，またそれを解決するためにトラフィックデータ保存専用ファイルシステムの提案し，試作システムの開発を行った．

今後は開発した試作システムを用いて性能評価を行う予定である．

参考文献

[1] 井上喬視，中島潤: トラフィックデータの保存に特化したファイルシステムの提案，情報処理北海道シンポジウム 2009 予稿集，2009

[2] 天海ほか: Linux 用ログ構造化ファイルシステム nilfs の設計と実装，情報処理学会研究報告．[システムソフトウェアとオペレーティング・システム]，2005