L-015

通信の証拠保全を目的とする高速通信に対応可能な 汎用 LAN 向けセッションレコーダの開発

Development of Session Recorder for Digital Forensic on high-speed universal LAN

中島 潤† 居内寛貴† 岸本 裕之‡
Jun Nakajima Hiroki Iuchi Hiroyuki Kishimoto

1. はじめに

通信ネットワークを介した相次ぐ不正アクセスや機密情報の漏洩により，コンピュータネットワークを利用する各企業はその対応に迫られている。当然のことながら，ファイアウォールの設置やコンピュータウィルス対策，あるいは IDS/IPS の設置は常識化されてきているところであり，企業によってはネットワークフォレンジックシステムの導入により，通信の証拠保全や組織内部における不正利用の抑止対策を行っているところも多い。

一般的に，ネットワークフォレンジックシステムは，アクセスログの収集や電子メールのアーカイブに絞った製品を指す場合もあるが，ネットワーク上を流れる通信は多種多様であり，全てのアプリケーション・トラフィックを対象として通信の証拠保全を行おうとする場合，イーサネット LAN であれば，イーサネット上を流れる全てのフレームを，中長期にわたってストレージ内に保存し，将来発覚する可能性のある何らかのインシデントのために備えておく，ということが望まれる。しかしながら，昨今の高速 LAN 環境では，記録保存すべき通信内容が膨大なものとなり，機密情報の漏洩に備えて全ての通信内容を長期間に渡り記録保存するということは，大規模ストレージの導入コスト，記録保存した情報の解析負荷を考えると，現実的ではなくなってきている。

そこで本研究では，メールサーバや Web サーバに代表される既存の各種ネットワークサービスサーバや，ルータや F/W 等の既存のネットワーク接続装置と連携させることにより，必要な通信セッションのみを抽出して記録保存出来る，ネットワークフォレンジックシステムとして活用可能な高速汎用 LAN 向けセッションレコーダの開発について研究を行ったので報告する。

2. ネットワークフォレンジックシステム

通信の証拠保全を目的とするネットワークフォレンジックシステムでは，キャプチャした膨大なパケットの中から目的の情報を迅速に見つけ出し効果的に解析が行えること，インシデント発生前後のパケットデータをエビデンスとして確実に保全できることが要求される。すなわち，後々の検索やプレイバックの必要に備え，パケットキャプチャ後にある程度の解析処理を行う必要があるため，必然的に内部の処理フローは図 1 のようになる。

筆者らの過去の研究開発等により[1][2]，通常の GbE 程度の LAN 速度であれば，フレームの取りこぼしもなく全

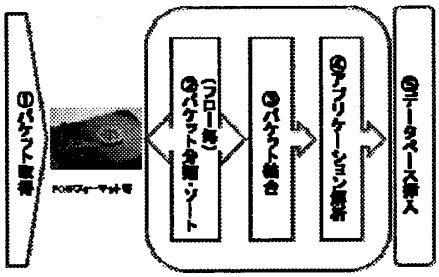

図 1 フォレンジックシステムの内部処理フロー

てのトラフィックを記録保存可能であることが判明しているが，パケットキャプチャ後の事後処理負荷が膨大なものとなり，これをリアルタイムで行おうとすると，汎用的なサーバ程度の処理能力では実用的なシステム構築が困難となる。

また，最近のネットワークトラフィックの特徴として，音声や映像などストリーミング系の通信や，SSL や VPN 等の暗号化通信の割合が増加し，記録保存したとしても結果として利用できない通信も同様に記録されなければならない構造となっている。

以上のことから本研究では，①企業等における既存のネットワーク環境に容易に導入可能で，②必要なセッションのみを選択的に記録保存可能であり，③キャプチャ後の事後処理負荷を必要最小限とする，構造としたセッションレコーダの開発を目指した。

3. 事後処理プロセスの負荷軽減の方策

先に述べたように，本研究ではキャプチャ後の事後処理負荷，すなわち図 1 における②から④の処理負荷軽減の課題を図ることを目的とする。これらの処理は，少なくとも，①キャプチャしたパケットを通信フローごとに区分し，②パケットをシーケンス順にソート，③パケットを結合し，④さらに上位のアプリケーション・プロトコルごとの解析処理を行った上で，データベースなどに通信の概要情報を記録し，検索を可能とする，といった流れとなる。その結果として，最終的にデータベースなどの記録される情報は，4W1H,すなわち，いつ，どのクライントマシンが，どのサーバに，どのような通信を行ったのかというような，時間情報やアドレス情報，URL 等のみということとなり，これらの情報の取得を他の手段で代替可能であれば，パケットキャプチャ後の処理を大幅に軽減可能であろうと考えた。

ここで，多くの企業におけるネットワーク環境を考えると，ほとんどの場合，企業内部ではローカルアドレスで運用されているため，NAT 対応のルータやファイアウォールが導入されている。またメールサーバ，プロキシサーバ等

† 北海道情報大学 Hokkaido Information Univ.
‡ (株)コムワース Comworth Corp.

の各種サーバ類も一元的に集中管理されている場合が多い。また IDS/IPS が導入されているケースも増えてきている。

ルータやファイアウォール，IDS/IPS の基本機能として，ACL(Access List)やポリシルール，シグネチャに合致した通信を通過・不許可とするフィルタリング機能がある。さらに，ACL 等に合致した場合，それを SNMP trap や syslog を通じて，他の外部システムへ通知・保存する機能を持っている。また，メールサーバやプロキシサーバの場合においても，メールや Web アクセスの度に，メールアドレスや URL 等の情報を syslog 等を通じて外部システムへ通知可能となっている。

そこで，これらの既存のネットワーク機器やサーバ類と連携することにより，パケットキャプチャ後の解析処理の負荷軽減を行うことが可能であると考えた。

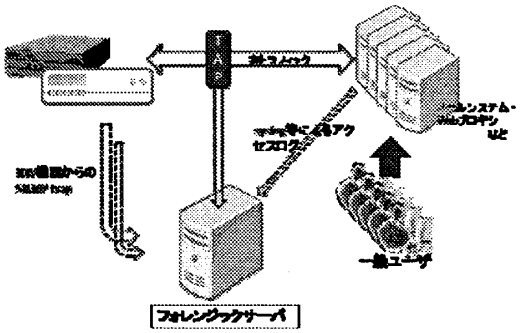

図 2　外部システムとの連携

4. 試作システムの開発

本提案を検証するために，試作システムの開発を行った。試作システムは，Linux OS マシン上で，汎用キャプチャプログラム tcpdump によりパケットキャプチャを行い，
それを外部システムからの通知情報により，保存対象とするパケットのみをフィルタリングしファイルへ保存すると共に，外部システムからの通知情報から得られたメールアドレス，URL 等の情報を用いて，データベースへ通信の概要を書き出す構造（図 3）とした。

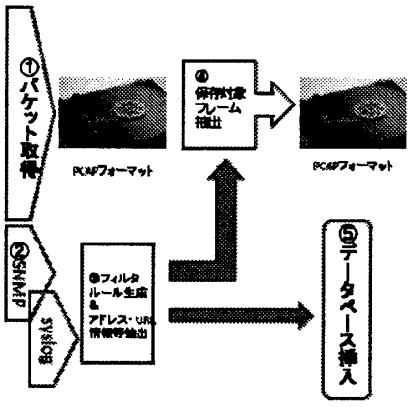

図 3　提案システムの処理フロー

外部システムとしては，Cisco 社製ブロードバンドルータ，メールサーバとして postfix，プロキシサーバとして Squid を想定し，それから排出される SNMP trap と syslog を，NetSNMP や syslogd で受信し，本システムで必要な情報を抽出し利用可能な変換プログラムをそれぞれ開発した。

Web アクセスの場合におけるシステムにおける処理フローの例をあげると，①プロキシサーバを通過した Web アクセスのトラフィックは，フォレンジックサーバでパケットキャプチャされ，PCAP 形式で一度ファイルへ一時保存される。②これと同時にプロキシサーバから syslog によりアクセスログが通知され，これに含まれるアクセス時刻・クライントの IP アドレス，URL・メソッド（GET または PUT）の情報を抽出し，あらかじめ管理者によって設定した記録ルールに基づいた，次のパケットフィルタリング処理のためのルールファイルを生成する。それと同時に，後の検索のために必要な情報をデータベースに登録する。③①で一時保存しておいた PCAP ファイルを②で生成したフィルタリングルールに基づきフィルタリングし，ファイル保存する，という流れとなる。

これにより，例えば，外部のサーバへアクセスした際に，Web ページの閲覧や画像ファイルの受信は記録保存の対象としないが，誰かが掲示板へ記事を投稿した場合はその通信を記録する，IDS/IPS が検知した不正アクセスの可能性があるセッションのみの記録保存を行うなど，アクセス対象のサイトやコンテンツの種類,あるいは不正アクセスの種類・プライオリティに応じた記録対象の選別が，処理負荷の大きい事後解析を軽減させた上で可能とした。ただし，アクセスログ情報等から得られる情報項目は限定されるため，フォレンジックシステムとしての利用を考えた場合，個々のアプリケーションレイヤの解析処理を全く不要とすることは出来ないが，はじめからアプリケーションレイヤの解析を必要としないセッションの選別のために利用可能であると考えている。

また本システムの導入に際しては，既存ネットワーク設備における SNMP trap 送信先の設定や syslog 送信先のコンフィグ変更のみであり，既存ネットワークの変更は必要最小限にとどめることが可能である。

5. おわりに

本研究では，通信の証拠保全を目的とする高速通信に対応可能な汎用 LAN 向けセッションレコーダの開発に際して必要な，事後解析処理の軽減をはかるために，既存のネットワーク機器類との連携を行うことにより，現実的なネットワークワークフォレンジックシステムを構築可能であることを示した。

現段階では，まだ試作システムを構築したのみであるため，今後は筆者らが開発済の製品へ組み込み，実ネットワークに導入の上，検証を行う予定である。

参考文献

[1]中島 潤,居内寛貴, “高性能 F/W 向け通信履歴記録装置の開発”, 電子情報通信学会 2008 年総合大会(2008).

[2]居内寛貴,中島 潤, “Gigabit Ethernet 全二重ワイヤレートに対応したネットワークフォレンジックシステムの開発”, 情報処理学会第 69 回全国大会(2007).