HOKUGA 北海学園学術情報リポジトリ
学校法人北海学園
北海学園大学
北海商科大学

タイトル	次世代電子商取引における証拠保全と高速ネットワークに対応可能なフォレンジックシステムの提案(栃内香次教授退職記念号)
著者	中島，潤
引用	北海学園大学経営論集，7(3)：51-63
発行日	2009-12-25

Hokkai-Gakuen Organization of Knowledge Ubiquitous through Gaining Archives.

次世代電子商取引における証拠保全と高速ネットワークに対応可能なフォレンジックシステムの提案

中　島　　潤

1　はじめに

情報化社会の進展により，商取引の分野でもインターネットを始めとする情報通信技術（ICT）の利用が定着してきた。このような環境変化に伴い，コンピュータウィルスや情報システムへの不正アクセス，また企業や官公庁などにおける情報漏洩事件など，通信ネットワークを経由した情報セキュリティに関連する問題（セキュリティインシデント）が数多く発生しているところである。

一般的に情報セキュリティ対策は，セキュリティインシデントが発生しない様に予防対策を施す「事前対策」と，セキュリティインシデントが発生した後に迅速な事後対応を行うための「事後対策」に分類できる。事前対策の代表的ものとしてはファイアウォールやアンチウィルスソフトウェア，通信暗号化装置などであり，また事後対策の代表的なものとしては，デジタルフォレンジックを挙げることができる[1)]。

現状のセキュリティ対策は，主に事前対策について重点的に行われており，特にアンチウィルスソフトウェアやファイアウォールは企業のみならず個人ユーザーにとっても一般的な防御策として浸透している。しかしながら，多くの企業がこのような予防策を取っているにも関わらず，セキュリティインシデントの減少には至っていない。現状においては，どのような事前対策を施していたとしても，情報セキュリティに対する脅威を完全に回避することは困難であるといえる。

そこで本論文では，セキュリティインシデントに対する事後対策として期待されているネットワークフォレンジックに着目し，現状のネットワークフォレンジックシステムの技術的課題を明らかにし，それを解決するための手法について提案を行う。

2　デジタルフォレンジック

本章ではまず，電子商取引に関わる通信の証拠保全のための方法と技術的課題と，その解決のための最も有力な手法であるデジタルフォレンジック全般に関する近年の動向について述べ，デジタルフォレンジックが社会においてどのような役割を果たすのかを明らかにする。その上で，本研究の対象分野であるネットワークフォレンジックについて，調査の対象となるトラフィックデータの保存について求められる要件，そして技術的課題に関して議論を行う。

2-1　デジタルフォレンジックの動向

今日のように，情報通信ネットワークを通じて商取引に関わる情報を交換することが一般的になった環境下では，情報通信ネットワークにより通信されている内容を記録し保

存することが重要で，セキュリティ管理上の意義が大きい。また，企業内部からWWWやメール，あるいはFTPなどを使って送信された内容をいつでも知ることができるようにしておくことは，企業内の不正なネットワークシステム利用に対して大きな抑止力を持つことが期待され，内部統制の面からもニーズが高まっている。

このような，ネットワークシステムを介して通信されるデジタル情報の記録・保全をデジタルフォレンジックという。フォレンジック（Forensics）とは，証拠を科学的に確定する作業のことを意味し，その基本的な役割とは，事件・事故が起こったあと，証拠を収集し調査を行うことである。ICTにおけるフォレンジックは，不正な情報漏えいや操作を発見するためにコンピュータネットワークで通信された内容を対象とする「ネットワークフォレンジック」（Network Forensics）（以下「NWF」）と，インシデント発生後に対象となるPCのHDD（Hard Disk Drive）等を保全し解析する「コンピュータ・フォレンジック」（Computer Forensics）に分類される[2)]。

NPO法人デジタルフォレンジック研究会では「インシデント・レスポンスや法的紛争・訴訟に対し，電磁的記録の証拠保全及び調査・分析を行うとともに，電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術」とデジタルフォレンジックを定義している。デジタルフォレンジックが日本において注目されるきっかけとなったのは，2006年に発生したライブドアによる証券取引法違反事件である。ライブドアを強制捜査した東京地検特捜部は，データセンターにあったメールサーバや，日常業務で用いられていたパソコンを押収した。特捜部は押収したサーバやパソコンに保存されていた10万通にも及ぶとされるメールを分析し，取り調べや裁判の際に重要な証拠として用いることで，当時社長であった堀江貴文の証券取引法違反容疑立件に結びつけたとされている。このとき特捜部が，サーバやパソコンからデジタルデータを法的に効力のある証拠として取り出すために用いた調査手法がデジタルフォレンジックである。

デジタルフォレンジックの対象となるデジタルデータの特徴として，コピーや消去，改ざんが容易であるという点を挙げることができる。デジタルデータが改ざんされていた場合は真正性が失われるため，そのデータの証拠性が失われてしまうため，デジタルデータの真正性確認には，一般的にハッシュ関数やデジタル署名技術が用いられる。さらに，ファイル転送やコピーなどによって，同一情報が様々な場所に散逸して保存される可能性を持っている。このことから，デジタルデータは元データの保管者や情報を持つ範囲を特定することが困難であるといえる。また，CDやHDDなどの媒体に情報を保存した場合，同様の情報を紙媒体で保存するよりはるかにコンパクトであるため，電子情報は紙媒体の情報に比べて保存される情報量が多いという特徴を持つ。これらの特徴が，デジタルフォレンジックを行うに際して重要ポイントとなる。

コンピュータフォレンジックは，PCのHDDやUSBメモリなどの周辺機器に記録されるデジタルデータを対象としたデジタルフォレンジックの一分野である。コンピュータフォレンジックでは，証拠保全のため，対象となるHDDなどの媒体を物理的に複製することが行われる。これは調査の際，直接PCを操作することによるデータの変更を防ぎ，デジタルデータの証拠性を失わないようにするためである。複製されたデータに対し，専用の調査ツールを用いて，操作記録や，パスワード等の解析，また削除されたデータの復元などを行って調査が行われる。デジタルフォレンジックは事後対策としての情報セ

キュリティツールとして利用する以外にも，内部統制やeディスカバリといった，近年企業に求められているCSRのための情報システムとしても注目を集めている。

2-2　ネットワークフォレンジック

一般の事件においては，フォレンジックの対象になるものとしては，写真やビデオ，指紋，場合によってはDNA検査標本といったものとなるが，NWFの場合は通信内容そのものであり，電子メールやWebページの内容，もしくは電文がそれに当たる。この場合，過去に行われた通信の記録がなければ調査不能であるため，NWFを行うためには，常時，通信内容や通信履歴を取得し記録しておく必要が生じる。NWFはデジタルフォレンジックの一領域であり，NWFは，ネットワークトラフィック，あるいはサーバやネットワーク機器等からのログ情報を主に扱うもので，対象別に，大きく以下の3つに分類することができる。

① パケット収集型　　LANを流れる全てのトラフィックを収集し保全，分析・調査をおこなうシステム
② ログ収集型　　サーバやネットワーク機器等からのログ情報を収集し保全，分析・調査をおこなうシステム
③ ネットワーク監視型　　IDSに代表されるような，ネットワークの監視を目的としたシステム

一般的にNWFシステムといった場合，アクセスログの収集や電子メールのアーカイブのみに絞った製品を指す場合もあり，NWFシステムという言葉に対して正確な定義付けがなされていないのが実情である。

これまでのNWFは，その解析対象をサーバやネットワーク機器のシステムログに頼ってきた[3]。システムログの解析やログの視覚化技術などがこれに含まれるが，これらはトラフィックの増加に伴い，ネットワーク機器等から膨大なログが出力されるようになるに従って重要情報を短時間で発見することが困難になってきている。そこで最近は，ネットワーク機器やIDS（Intrusion Detection System：不正アクセス監視装置）などのシステムログから異常状態を検知する研究が盛んに行われている[4]（図1）。また，膨大なログ情報を要約することにより，それぞれのログの発生原因を発見する研究がなされている。このようなシステムの課題としては，膨大かつ連続的なログを解析すること，自動的に特徴を抽出し異常を検知すること，といったことが挙げられる。しかしながら，サーバやネットワーク機器のログ解析から得られる情報は限定的であり，インシデントに対する決定的な証拠能力性が低いため，近年ではパケット取得型のNWFシステムが主流になりつつある[5)6]。パケットキャプチャ型のNWFシステムを使用することにより，ネットワークを介して盗まれた情報が何であるか，どのような手段で盗まれたのか，いつ盗まれたのかという情報を記録しておき，原因究明，被害特定が容易に行えることが期待される。

NWFシステムの使用により，電子商取引

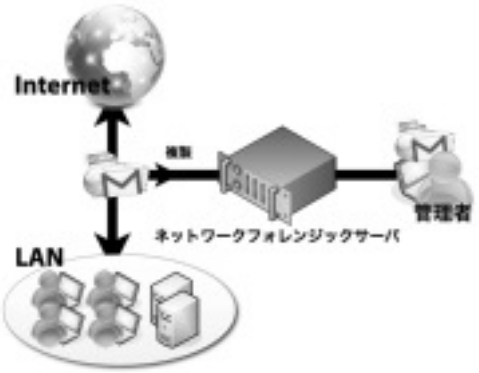

図1　パケット取得型ネットワークフォレンジックシステム

でのやりとりを追跡し，契約の成立時期前後の情報を証拠として保持することができるため，トラブルを解決するための強力な手段になりうる。なぜならば，NWF システムにより，詐称メールの内容，不正にアクセスした場合の形跡，改ざん等の被害といった犯罪行為の証拠を収集することが可能となるため，解決が容易になり，また，犯罪証拠が確実に残るため，導入した旨を公知することによってコンピュータネットワークを介した犯罪に対する抑止力効果が期待できる。

パケット収集型の NWF システムは，一般的に，次の４つのフェーズで実現される。LAN 上を流れるトラフィックはルータやスイッチといったネットワーク機器のミラーポート機能，あるいはトラフィック複製専用機器であるネットワークタップ等を用いて複製され，複製されたトラフィック（パケット）は NWF システムによってキャプチャされ，ファイルストレージ等に保存される。このとき，トラフィックデータは PCAP フォーマット[9] 等の汎用的なファイルフォーマットで時間やサイズで分割されファイル単位で分割されて保存される（図２）。また，パケットキャプチャとストレージ，通信内容の解析を昨日ごとに別筐体上で運用されるケースや同一機能を複数のサーバ筐体で受け持ち，クラスタリングにより処理性能の向上を行うシステムもある。

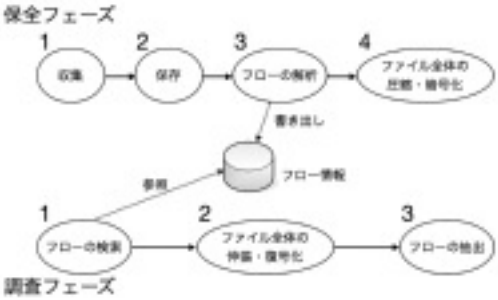

図２　パケットキャプチャ型ネットワークフォレンジックシステムの処理フェーズ

高速ネットワーク環境下においては，パケットキャプチャ処理自体が高負荷になり得ることや，収集されたパケットに対して逐一，通信内容の解析処理を行い，フロー情報等のデータベース化を構築する処理コストが大きいことに由来する。フロー情報等のデータベース化は，不正アクセス等のセキュリティインシデントが発生した際に，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，調査分析を行う為に必要な処理であり，パケットキャプチャと同時にリアルタイムに処理が行われることが期待される。またこのとき同時に，トラフィックデータの保存には，機密性，また改ざんされていないことを証明するための完全性が求められるため，暗号化や，ハッシュ値の計算などが同時に行われる必要がある[7)8)]。

2-3　トラフィックデータの保存における要件と技術的課題

NWF を行うにあたって，トラフィックデータの保存において必要とされる要件とその要件に対する技術的課題について述べる。

パケット取得型 NWF システムでは，基本的に LAN 上を流れる全パケットの収集を前提としているため，保存されるトラフィック量は必然的に膨大な量となる。トラフィックデータは最終的にファイルとしてファイルストレージに書き込まれるが，巨大ファイルの扱いは既存の汎用ファイルシステムや OS の構造上から困難であるため，基準となる，何らかの単位にファイル分割され保存される必要がある。このとき，トラフィックデータを分割するための基準としては，①一定ファイルサイズによる分割，②一定の時間ごとによる分割，③ネットワークフローごとによる分割　が考えられる。しかしながら，保存されるトラフィックデータに対して暗号化や圧縮などを施す場合，①や②ではその妨げとなる恐れがあるため，本来は③のフロー単位で

保存することが望ましいが，これをリアルタイムに処理して記録することは現段階において技術的に困難な点である。

NWFは，過去に発生した通信を調査するものであるため，出来る限り長期間に渡ってトラフィックデータを保存したいというニーズが存在している。しかしながら，発生するデータ量が膨大であるため，大容量ストレージの導入等のコスト面で課題がある。このシステム導入にかかるコストがNWFシステム普及の妨げになっているとも考えられる。また，トラフィックデータに対して法的な証拠能力が必要とされるため，トラフィックデータに対して暗号化や，完全性の付与が要求される。

以上をまとめると，NWFシステムに対するトラフィック保存に対する要求は，①高速なネットワーク環境に対応可能なトラフィック保存性能で，②インシデント発生時など，任意のタイミングで任意の通信フローを選択して抽出が短時間で可能であり，③トラフィックデータに対する機密性・完全性が確保されている，ということになり，これらを実現するためには，キャプチャしたパケットデータをそのままファイル分割してストレージ上に記録するだけではネットワークフォレンジックシステムとは言えず，キャプチャデータに対する前処理・後処理が必要とされるが，既存手法においては，高速化するネットワークに対するスケーラビリティの観点から，長期間に渡って機密性や完全性を保ちつつ保存することは，技術的にもコスト的にも困難な状況にある。

2-4 既存ネットワークフォレンジック製品の課題

既存のパケット取得型のNWFシステムは，GUIでの操作性もよく，再現可能な通信プロトコルも充実し，既に多くの企業で導入実績があるものの，前述の技術的課題が未解決のままであるためにリアルタイムに通信を解析することが難しくなっている。本節では，既存NWFシステムが抱える技術的課題について整理する。

2-4-1 パケットキャプチャの方法に関する課題

既存製品では，通常のPCでも搭載されているような汎用Network Interface Card（以下NIC）を利用してパケットをキャプチャしている。汎用NICを利用してパケットをキャプチャした場合，OSへの割り込み処理が著しく発生し，CPUへ大きく負担をかける構造となっている。通常のNICを利用した場合には，解析アプリケーションがパケットデータを利用できる様にメモリへパケットデータを移すが，データを移すまでにはOSなどのソフトウェアを通さなければならないためCPUリソースを著しく消費してしまい，もしCPUリソースが残されていない場合はパケットの取りこぼしが発生してしまう。これはNWFシステムとしては信頼性を失う挙動であり，最優先で解決しなければならない課題である。

この課題に対して，キャプチャプロセスを解析プロセス等から独立させ，キャプチャプロセスを優先的に処理させるよう改良している製品もあるが，根本的な解決には至っていない。1 Gbps程度のトラフィックをキャプチャすることを考えた場合，すべて64 Byteの最小サイズのパケットとすると1秒間に約200万パケットをキャプチャ必要がある。パケット一つ一つに対してNICからのパケットのキャプチャとメモリへの転送，メモリからのパケットの読み込みと記録ストレージへの記録をする必要があるが，クロック周波数3 GHz程度のCPUを利用して約200万パケットの通信データをキャプチャし記録することは，ソフトウェア処理では困難を極めているためである。

2-4-2　パケットキャプチャ・通信解析アプリケーションの処理に関する課題

２つ目の課題として，通信データのキャプチャとキャプチャ後の解析処理の一連の動きが挙げられる。既存の製品の多くはパケットキャプチャに汎用ライブラリを利用しているため，ファイル保存にはPCAPフォーマット，またはTCPストリームへ組み立てた状態で保存している[9]（図３）（図４）。GbEフルワイヤレート環境下でPCAPフォーマットにより保存しているシステムで，後にパケットを取りだそうとした際，１分間区切りのファイルで最大15 GByteにもなるファイルの先頭から目的とするパケットを読み込む必要があり効率が悪い。TCPストリームへ組み立てて保存しているものでは，後に取り出す際にパケットを結合する必要がなく効率が良いが，Synフラッド攻撃のような異常状態でパケットキャプチャした場合，１分間のTCPストリーム数が２億3437万ストリームにもなり，この方法では管理が困難となる[10]。

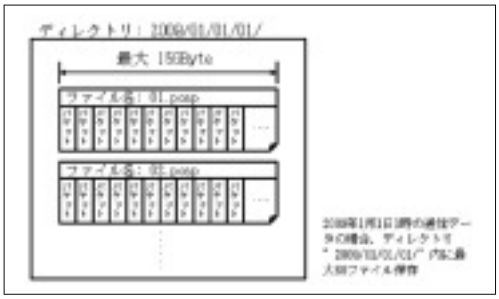

図３　PCAPフォーマットでの記録

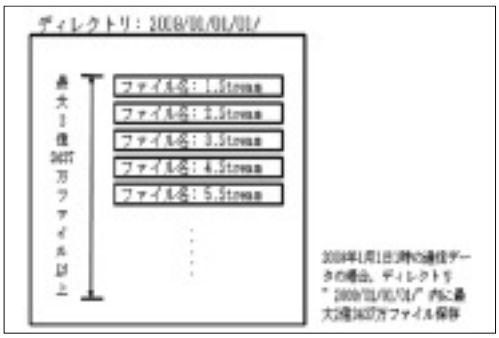

図４　ストリームデータ形式での記録

多くの通信データを取り扱うシステムの場合，いかに高速にパケットを分類しストリーム毎に検索・解析処理するかが重要になる。これは，パケット毎，または，ストリーム毎に発生する作業であり，低速なネットワーク回線では問題とならない程度の負荷であっても，GbEのような高速な通信環境で考えた場合，致命的な問題となる。

2-4-3　システムリソースのスケジューリングに関する課題

３つ目の課題としてキャプチャ後の解析処理を同一タイミングで行っている点をあげることができる（図５）。解析処理をキャプチャ直後に，または通信データの内容を再現するプレイバック時に行う製品が多いが，どちらのタイミングであっても対象ストリームすべての解析を一時に行っているため，処理負荷が集中しパケットキャプチャに影響を生じさせる。加えて，パケットキャプチャ直後に解析処理するものでは，プレイバックの確率が低いストリームに対してもプレイバック可能な状態にまで解析処理を行うために，無駄な処理負荷を増加させてしまっている。また，プレイバック直前に解析を行うものでは，解析の待ち時間が長く，解析結果を表示するまでにかなりの時間を要してしまう構造となる（図６）。

こうした問題を複数台のサーバによりクラスタリングし，マシンパワーで解決することで回避するよう推奨している製品もあるが，パケットキャプチャ後の処理をソフトウェアで行っていること等もあり，GbEに完全に対応することが困難である。また，複数台のサーバを導入することで導入コストの増大やメンテナンス・管理等が複雑化しランニングコストも増大するなどの問題も発生するため，GbEネットワークを１台のサーバ筐体で完

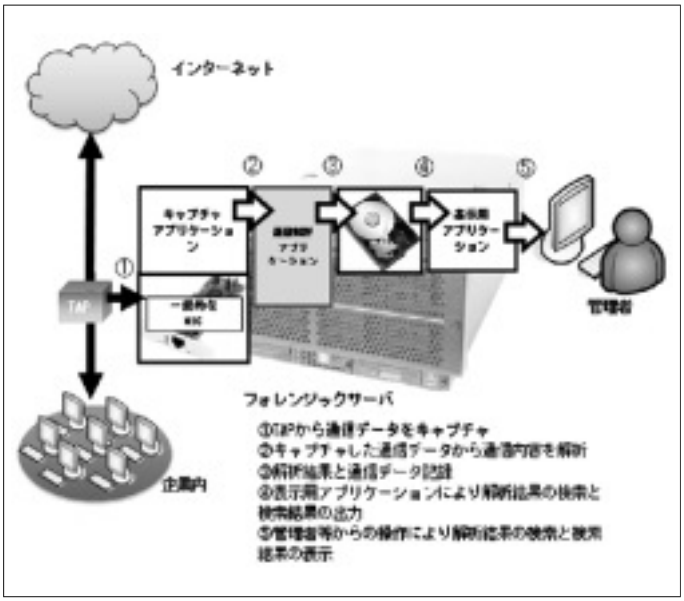

図5　キャプチャ直後での解析処理

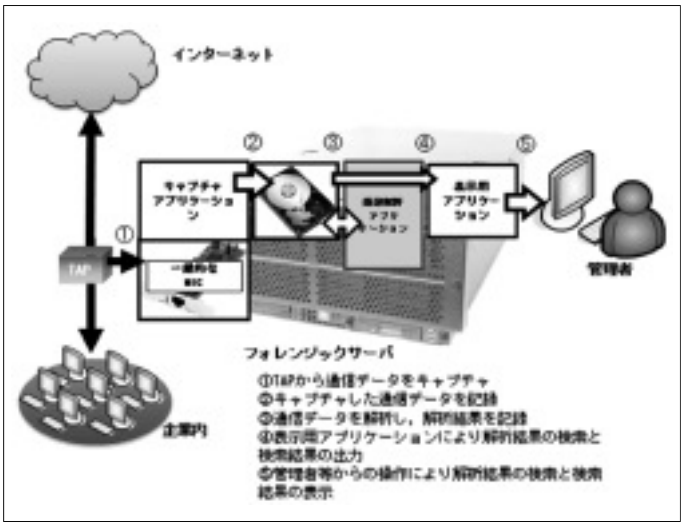

図6　プレイバック直前での解析処理

結し対応できるシステムが求められている。

3　パケットキャプチャ型NWFシステムの処理性能向上方法の提案

前章で述べたパケットキャプチャ型のNWFシステムの技術的課題を，以下の3点により解決することを提案する。

3-1　キャプチャパケット処理アーキテクチャの提案

セキュリティインシデント発生後にNWF

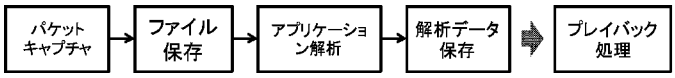

図７　従来型ネットワークフォレンジックシステムの処理プロセス

システムで閲覧する情報は，GbE 環境下であれば 260 万セッション（正常な TCP セッションの場合における理論的最大値）という膨大な情報の中から検索・抽出される必要があるため，階層的に詳細化し，表示する方法が適当である。また，ネットワークフォレンジックシステムが稼働している状況で常時閲覧する項目は，主にネットワークトラフィックやレイヤ３，４でのプロトコル比率等の概要情報に限定される。つまり，キャプチャと同時に行うべき作業はネットワーク上を流れているフローの概要を解析して把握することであり，ネットワークの状況を把握するためにも，これはリアルタイムに行わなければならない。しかも，NWF システムにおいて，一番に優先すべきは，パケットを取りこぼさないということである。既存システムでは，汎用 NIC を利用しているために，パケットキャプチャを優先する結果としてシステムリソースを消費してしまい，その後の解析処理をリアルタイムに行うことを困難なものとしている。

そこで本研究では，通信内容をリアルタイムに解析するために，パケットキャプチャ処理と解析処理プロセスを並行して実行し，システムリソースの不足を回避する 3 Stage Network Flow 解析アーキテクチャを提案する（図８）。

これは，通信データの解析処理を①キャプチャと同時に行うストリーム解析，②システムリソースの閑暇時に行うアプリケーション解析，③通信の再現を表示する際に行うプレイバック処理　の３ステージに分割し，それぞれを独立して動作させることにより，処理負荷を分散し，ステージごとに必要最低限の

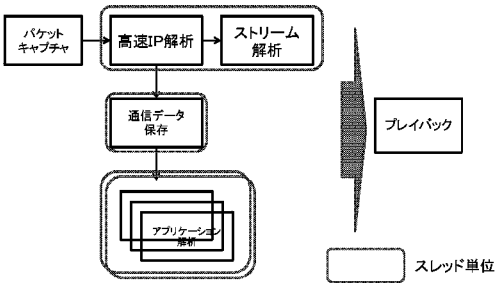

図８　3 Stage Network Flow 解析アーキテクチャ

解析を行うことで，リアルタイムに結果を出力することを可能とする。

また，必要最低限の処理を行うため，パケットキャプチャに割当てるべきシステムリソースを常時使うことがなく，優先的に割り当てることができる。加えて，分散処理によりプレイバック時にもタイムロスのないスムーズな表示を両立させることが出来る。各ステージの詳しい動作を以下に説明する。

3-2　キャプチャと同時に行うストリーム解析

①ステージでは，前項で説明した高速 IP 解析エンジンを使い，キャプチャと同時にセッションの解析を行うため，リアルタイムに Layer4 以下の統計情報や通信リストを閲覧することが可能となる。キャプチャ時の解析では，IP アドレス，ポート番号，トラフィック等の情報のみを解析し HTTP や SMTP 等の解析は行わないため解析処理が高速であり，リアルタイムに通信概要を閲覧できる。また，高速 IP 解析エンジンはハッシュ値を利用することで，瞬時に IP とポート番号の組み合わせを識別出来るようにし，このハッシュ値はシステム全体で共通に利用

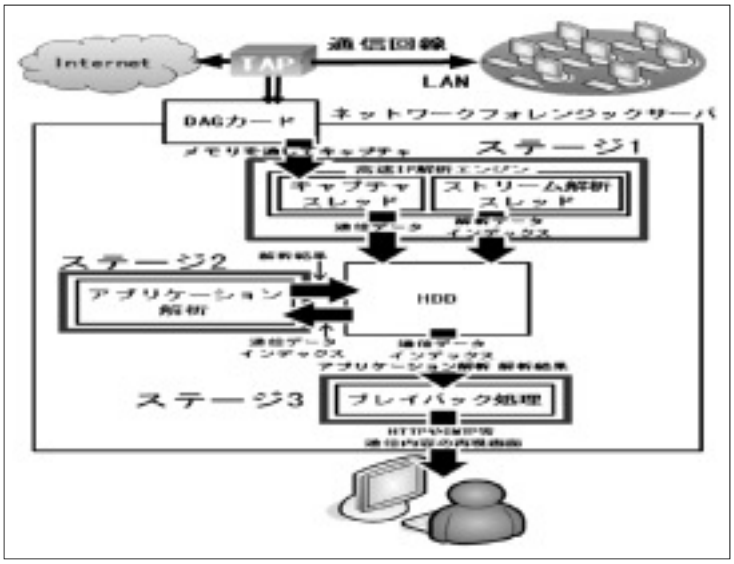

図9　提案するネットワークフォレンジックシステム

することで高速なデータ識別を可能とする。保存される通信データファイルへのインデックスへもハッシュ値が付加され再度パケットを取り出す際も高速にIPとポート番号の組み合わせを識別できる。

3-3　アプリケーション解析処理のタイミングとスケジューリング

②ステージでは，①での概要データとインデックスを元に高速にTCPストリームを再現しHTTP，FTP，SMTP，POP3等のアプリケーションレイヤごとの解析を行う。ここでの解析では，データベースへ解析データを記録するだけであり，既存の製品のように再現したTCPストリームを保存することはない。加えて，キャプチャにおけるシステムリソースを確保するためシステムリソースを監視するコントローラからの呼び出しにより実行される。これにより，パケットキャプチャプロセスでシステムリソースが不足することがなく，IP解析エンジンと合わせることでGbEに対応することが可能となる。

3-4　通信の再現を表示する際に行うプレイバック処理

④ステージでは，プレイバック処理においてプレイバックするデータがセッション中のどの位置に存在するかを検索する。検索したデータは，独自形式のデータフォーマットからHTTPやSMTP等のフォーマットに整えGUIへ出力する。出力フォーマットのデータを保存しておくのではなく，最後のプレイバック時に変換することで，独自形式のデータとHTTPやSMTP等のプレイバックデータを保存しておく必要がなく，保存容量の節約を実現する。

3-5　パケットキャプチャ専用デバイスの利用

本節ではパケットキャプチャ処理の高速化のために，パケットキャプチャ専用デバイスの採用により解決することを提案する。パケットキャプチャ専用デバイスの一例をあげると，Endace社DAG[11]は，PCI-Xを介して接続され，キャプチャパケットをあらかじめ確保しているメモリ領域へダイレクトにア

クセスすることで，OS を介さずに転送することを可能とする。これによりパケットのキャプチャの際に発生する OS への割り込み処理を軽減し，CPU リソースの消費を抑え，結果としてキャプチャ性能の向上が期待できる。

Endace 社が行った汎用 NIC との性能比較では，汎用 NIC で libpcap[9] を使用してキャプチャした場合，298 Byte のフレームで秒間 100,000 パケットをキャプチャした時点でパケットの取りこぼしが大量に発生するが，DAG では秒間 400,000 パケットをキャプチャしても全くパケットの取りこぼしが発生していない[12]。これは OS 等のソフトウェアを通してメモリにコピーしている部分を DAG は DMA 転送しているためで，パケットキャプチャ専用デバイスが汎用 NIC と比較して非常に高速であることが確認できる。

3-6　高速 IP 解析エンジンの開発

本節で提案する高速 IP 解析エンジンは，3 Stage Network Flow 解析アーキテクチャの 1 ステージ目にあたる。高速 IP 解析エンジンでは，DAG を使ったパケットキャプチャ，そしてキャプチャしたパケット及び再現したストリームのサマリデータ（IP やポート番号，ストリームサイズ，パケット数等の情報）を保存する。サマリデータの保存では，パケットを結合することで TCP ストリームや UDP ストリームを再現し，そのサマリーをデータベースやインデックスファイルへ保存する。

本高速解析エンジンにおいて主として考慮されるべき点は，どの状況・段階にあっても，キャプチャパケットがどのストリームに対応するのかをいかに高速に区分するかにつきる。これは，キャプチャしたパケット毎に実行される処理であることと，GbE 環境下の様な高速なコンピュータネットワークでは，ストリームを見分けるためのパケット同士の比較回数が膨大になり，負荷が集中するためである。これはシステム全体で共通したハッシュ値を使うことで，目的パケットまでのアクセスパスを最小に押さえることが可能である。

また，パケットキャプチャや解析処理後に保存されたパケットについても，同様にアクセスパスを最小にすることが望まれる。本研究では，パケットの書込先を独自フォーマットの通信データファイルとし，1 分間隔で新しいファイルへ切り替え，時系列によるディレクトリ構造をとることを提案する。また，キャプチャ時に解析しデータベースへ保存したセッション情報を利用することで，対象パケットが保存されている通信データファイル

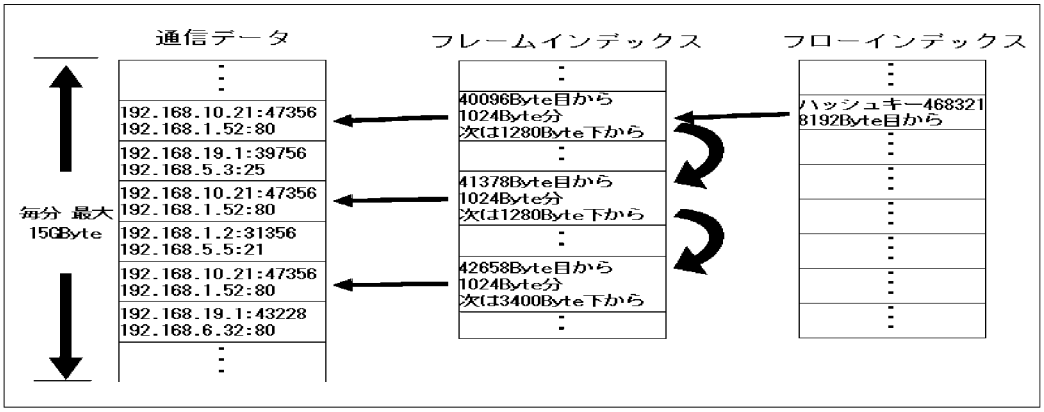

図 10　インデックスファイルの構造

を見分けている。しかし，１分間のファイル容量はGbEの環境下で15 GBにも上るため，データベースからのセッション情報だけでは，ストリームを特定することは困難であることから，通信データに対して，２段階のインデックスをキャプチャと並行して作成する(図10)。まず，１つ目のフレームインデックスでは，保存通信データファイルに対して，含まれているパケット一つ一つに対してのオフセット値，パケット長，そしてパケット同士のつながりがわかるように，同一のストリームに属するパケットのファイル上の位置を記録する。

２つ目のフローインデックスは，フレームインデックスに対するインデックスとして記録し，ストリーム固有のハッシュ値とそのストリームの開始オフセット値として記録してする。つまり，データベースから再現したいTCPストリームまたはUDPストリームを選び，データベースに記録されているIPやポート番号からハッシュ値を計算した上で，フローインデックスで該当するハッシュ値を探し，そのフローインデックス値を元にフレームインデックスを見る。フレームインデックスでは，通信データのどの位置にパケットがあるのかが記録されているので，これを使って通信データから目的のパケットを取り出す。その後は，フレームインデックスに記録されている次のパケットの記録場所まで移動し，フローインデックスを元に通信データファイルから対象パケットを取り出す。この様にしてパケット同士を接続していくことで，ストリームを再現する。ここではフローインデックス，フレームインデックス，そして通信データと３回の最小アクセスパスで対象となるパケットまでたどり着くことを可能とした。これにより既存製品のようにパケット探索でシステムリソースの消費を避けるためTCPストリームやUDPストリームとして記録しておく必要がなくなった。また，プレイバックする可能性の低いデータまで処理する必要も無くなった。前途したように，２重にインデックスを付加することで，キャプチャと同時に高速にストリームを取得することができ，この後の解析でも高速化を図ることができる。

さらにキャプチャした通信データをファイルとして出力するときには，OSの書き込みバッファを利用しない方法をとる。これは，OSではなく解析エンジンにバッファをとることでファイル管理，書き出し処理などのOSへの負担を最小限にし，大きく速度向上を図ることが期待できる。加えて，キャプチャ中は解析処理が行えずキャプチャバッファの肥大化を招き，最終的にはパケットの取りこぼしに至る恐れがあるため，パケットキャプチャとパケット解析処理を同一プロセス内で行い，マルチスレッドで並列処理をする。こうすることによって，解析性能を向上しつつ，パケット落ちを減少させることが期待可能である。

4．おわりに

これまでNWFシステムのようなシステムは機器の導入コストやその規模の大きさから実現が困難であったが，現在はハードウェアの低価格化や小型化といった技術の進歩により実現が可能になっている。しかしながら，依然として導入にはコストがかかり，またNWFそのものに対する知識不足などに由来する躊躇もある。NWFシステムは，現時点においても既にベンダー各社が製造販売しており，提供される機能・性能もさまざまであるが，信頼性や解析処理に時間を要するために即時性が失われる，といったデメリットがあるものがほとんどである。ことに，現在では一般的となったギガビット級の高速LANに対応可能なシステムは未だほとんど存在しない[13)14)]。

本論文では，サーバ１台で完結しGbEクラスの高速ネットワークに対応できるパケットキャプチャ型のNWFシステムのアーキテクチャを提案した。パケットキャプチャ処理の一部をハードウェア化することで，システム負荷を軽減しパケットの取りこぼしを減少させる。高速IP解析エンジンと3 Stage Network Flow解析アルゴリズムにより，解析のリアルタイム性と高速性が両立させる。これによりGbEクラスの環境下でキャプチャと解析を同時に行う場合，既存システムのように複数台のサーバでクラスタリングする必要を無くすることが可能となる。

電子商取引は，コンピュータネットワークを介して行われるBtoB，BtoC，CtoCなどの商取引を言い，インターネットを利用した商談，企業間の受発注取引，商取引にともなう資金決済から，一般消費者が仮想店舗から商品を購入するオンラインショッピングまでに至るさまざまな形態があり，既に広く展開されているところである。本研究ではコンピュータネットワーク上で起こりうる電子商取引に関わるトラブルに対する証拠取得や，個人情報漏洩の原因究明，なりすまし行為よって受けた被害の究明，不正アクセス行為に対する抑止力などに役立つ強力なツールとして期待されているNWFシステムが，従来の目的であった情報セキュリティ対策という観点以外からも企業に対してCSR（Corporate Social Responsibility）を問う社会的要請からも強い注目を集めているシステムである。また，情報爆発ともよばれる現代において，高速化する通信ネットワークに対応可能なネットワークフォレンジックシステムを実現することは依然容易ではなく，今後も更なるフォレンジック技術の研究開発が必要とされる。

参考文献

1）辻井重男，萩原栄幸：デジタルフォレンジック辞典，デジタルフォレンジック研究会（2006）.

2）高橋郁夫：コンピュータ・フォレンジックスとは何か，電子情報通信学会技術研究報告．SITE，［技術と社会・倫理］，Vol.104，No.96（20040521），pp.7-11（2004）.

3）川口信隆，宮地玲奈，小畑直裕，重野寛，岡田謙一：フォレンジックコンピューティングのための安全で効率的なロギングアーキテクチャの提案，情報処理学会研究報告．CSEC，［コンピュータセキュリティ］，Vol.2003，No.126（20031219），pp.7-12，（2003）.

4）江端真行，小池英樹：不正侵入調査を目的とした複数ログの時系列視覚化システム（ネットワークセキュリティ　〈特集〉再考　分散システム／インターネットの運用・管理），情報処理学会論文誌，Vol.47，No.4（20060415），pp.1099-1107（2006）.

5）M.I. Cohen: PyFlag - An advanced network forensic framework, Digital Investigation, Vol. 5, pp.112-120 (2008).

6）Gerard Wagener, Alexandre Dulaunoy, Thomas Engel: Towards an estimation of the accuracy of TCP reassembly in network forensics, Second International Conference on Future Generation Communication and Networking, (2008)

7）居内寛貴，福岡清伸，中島潤：超高速ネットワークに対応可能なIPパケットリアルタイム解析エンジンの開発，情報処理北海道シンポジウム2006　講演論文概要集，p.11（2006）

8）居内寛貴，福岡清伸，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，情報処理北海道シンポジウム講演論文概要集，pp.6（2007）

9）TCPDUMP/LIBPCAP public repository. http://www.tcpdump.org/

10）稲井俊介，福田洋治，溝渕昭二，毛利公美，白石善明，野口亮司：ネットワークフォレンジックのためのホストベースのパケット取得機構の検討，IEICE Technical Report，Vol.11，pp.1-6（2008）.

11）Endace - what we do - Dag cards http://www.endace.com/Default.aspx?pageid=34

12）Comworth online http://www.comworth.co.jp/products/m_a/img/endace_008.html

13）Computer & network LAN 23(3)（通号257）

64～67，オーム社，(2005/3)．
14) 向井徹：フォレンジック・ソリューション紹介
ネット ワーク・フォレ ン ジック・ツール（特 集
不正行為を調査するデジタルフォレンジック）