Vol.2011-IOT-12 No.38
2011/3/1

侵入検知とモニタリングシステムを組み合わせた異常トラヒックの自動保存

中村豊[†]　戸田哲也[†]　井上純一[†]　福田豊[†]

インターネットの普及に伴い，各組織では何らかの侵入検知システムやトラヒックモニタリングシステムを導入する必要に迫られている．その運用は容易ではなく管理者の経験や技術が要求される．一方で，組織の運営側ではインシデント発生時に通信の履歴や証拠を調査しなくてはならない．トラヒックモニタリングシステムでのトラヒックの長期保存は高コストであり，かつ，その解析は困難である．そこで我々は，異常トラヒックを侵入検知システムにより検出し，自動的にモニタリングシステムから抽出して保存するシステムを構築した．本システムを用い，2ch への書き込みに対して自動的に，その通信内容を保存することが可能となった．これにより，管理者の運用コストを削減することができた．

Automatic preservation of unusual traffic which combined intrusion detection and a monitoring system

Yutaka Nakamura[†]　Tetsuya Toda[†]　Junichi Inoue[†] and Yutaka Fukuda[†]

The network management cost is increasing with the spread of the Internet. In each organization, an intrusion detection system and traffic monitoring system are operated. However, the management is not easy and experience and skill are required of an administrator. On the other hand, the executive of the organization has to investigate a communicative history and its proof at the time of the occurrence of an incident. Long-term preservation of the traffic in a traffic monitoring system is high cost, and its analysis is difficult. We constructed the system for automatic preservation of unusual traffic. Our system can automatically save the communication to the writing to the 2ch. Therefore, the administrators operation cost was reducible.

1. はじめに

インターネットは社会インフラとして広く普及している．それに伴い多様なアプリケーションの開発が進み，それらを利用した法令違反やモラル違反が発生している．例えば，P2P アプリケーションの利用による情報漏洩や著作権法違反，また，匿名掲示板への誹謗中傷の書き込みなどがあげられる．このようなセキュリティインシデントに対して，企業のネットワーク管理者は，社内で利用できるアプリケーションを限定したり，WEB の URL フィルタリングにより業務以外の利用の制限を設けるなど，法令に基づいた厳しい対策を実施している．一方，大学では教育・研究利用を前提としているため，極端な制限を設ける事が難しい．そのため，様々な侵入検知システムを用いて，トラヒックを監視する必要が生じている．

既存の侵入検知システムでは，様々なアプリケーションを検出することが可能である．しかし，その運用の際にはシステム側の問題である誤検知であったり，大量の異常トラヒックによるアラートストームという問題があり，システムの設定方法に高度な知識が要求されるため，管理者の勘と経験が必要となる．さらに，留学生が用いる外国製のアプリケーションは，開発動向や特性などの情報取得が困難であるため，管理者の負担をさらに重くさせる．また，既存システムではアプリケーション上で流通しているコンテンツの中身までは確認することができない．よって大学のネットワーク管理者がセキュリティインシデントに対処するには，侵入検知システムが出力する IP アドレスや通信時刻などの情報を基に，トラヒックのダンプデータを用いて，コンテンツを調査する必要がある．

一方で，全トラヒックのダンプデータの保存は，非常に困難である．具体的に，九州工業大学では，約 1 カ月間のトラヒックのダンプデータを保存するためには約 30〜50 TB のストレージ容量が必要となる．この様な大容量のストレージを維持・管理し，かつ，インシデント発生時にトラヒックの解析作業を実施すると，ネットワーク管理者の負担は非常に重くなる．インシデント対処処理は緊急を要し，他の全ての業務を停止させてトラヒック解析に時間を費やすことになるため，その負担を軽減させる事は重要な課題である．

そこで我々は，上述した問題を解決するために，既存の侵入検知システムとトラヒックモニタリングシステムを連動させ，異常トラヒックを自動的に保存するシステムを構築した．具体的には，既存の侵入検知システムを用い，2ch への書き込みや P2P アプリケーションを検出し，次に，それらの検出結果を syslog として保存する．保存

[†] 九州工業大学，情報科学センター
Kyushu Institute of Technology, Information Science Center

された syslog は自動的に解析され，IP アドレスや時刻などの必要な情報が取り出される．最後に syslog サーバはトラヒックモニタリングシステムに対して，遠隔操作により特定のトラヒックを取り出し外部ストレージへ出力させる．この様なシステムを構築したことによって我々は 2ch への書き込みに対して，自動的にその前後の時刻を取り出して抽出し，個別に保存することが可能となった．また，P2P アプリケーションに対しても同様の手順で処理し，外部ストレージへ手動で保存できるようになった．これにより，ネットワーク管理者のセキュリティインシデントに対する作業負荷を軽減させる事が可能となった．

2. 関連研究

本章では，本研究における関連研究について述べる．

2.1 侵入検知システム(Intrusion Detections System)

侵入検知システムには，フリーソフト，商用含めて様々な製品が存在する．フリーソフトウェアではネットワーク型 IDS である snort[1)]が広く知られており，数多くのシグネチャが提供されている．snort は Libpcap[2)]を用いてパケットをキャプチャし，シグネチャとのパターンマッチによって異常の判定を行う．管理者が自らシグネチャを作成することもできるが，その運用や出力の管理は熟練した技術が求められる．

商用の製品では，Juniper Networks IDP[3)]，Cisco IPS[4)]，PaloAlto[5)]，OnePointWall[6)]などの様々な製品が存在する．これらの製品では，様々な P2P アプリケーションを検出する機能や，自動的にトラヒックを遮断する機能を有している．企業ネットワークの様な，ネットワーク運用ポリシーを厳格に規定して，業務以外のインターネット利用を制限する場合は，これらの製品は有効に機能する．しかし，大学では教育・研究目的での利用を前提としているため，インターネット利用の厳格な制限はできない．したがって，商用製品で異常トラヒックを検出した後に，それらの通信を監視する必要が生じる．

2.2 トラヒックモニタリングシステム

トラヒックモニタリングシステムも侵入検知システムと同様に，フリーソフトおよび商用製品が存在する．フリーソフトウェアでは tcpdump[7)]，wireshark[8)]などが存在する．tcpdump は汎用のパケットキャプチャアプリケーションであり，様々な入力・出力フィルタを記述することができる．wireshark は，パケット解析ソフトウェアであり，tcpdump で記録したパケットの内容を詳細に解析することができる．これらのツールは手軽に利用することができるが，大規模な運用に用いるためには高度な技術が要求される．

商用の製品では，NetDetector[9)]，clearsight[10)]などの製品が存在する．これらの製品では，パケット解析も可能で，容易に扱うことのできる GUI を備えている．しかし，パケットロスを防ぐために，高性能ハードウェアを搭載しているものが多く，購入コストが非常に高い．

2.3 デジタルフォレンジック

中島ら [11)12)]は通信の証拠保全を目的としたフォレンジックシステムを提案，開発している．11)では，広帯域化したネットワークに対応したフォレンジックシステムを開発している．また，12)では WEB proxy サーバ，postfix，SNMP trap などのアプリケーションと連携したセッションの抽出を行っている．これらの研究は本研究と同様，大容量ストレージの運用・維持・管理およびインシデント発生時のトラヒック解析が困難であることに着目している．相違点としては，これらの研究が，トラヒックモニタのイベントトリガーにアプリケーションサーバを用いているのに対して，本研究では侵入検知システムを用いている点である．

3. 要求要件

本章では，システムの要求要件について述べる．

・侵入検知システム

1. P2P アプリケーションを検出する機能が必要である．本学では winny 系，bittorrent 系，gnutella 系を代表的な P2P アプリケーションとして，それらのプロトコルに基づいたアプリケーションを検出できることが要求される．現在の設定では，winny，gnutella，perfect-dark，100bao，azureus，direct-connect，fasttrack，fileswire，flashget，kazaa，pando，share，warez を検出対象としている．
2. 2ch などの掲示板への書き込みを検出する機能が必要である．掲示板への公序良俗に反する書き込みなどは，学内規定により禁止されているため，掲示板への書き込みを検出する機能が要求される．
3. TAP モードで動作できることが必要である．本学における通常トラヒックには影響を与えずに，トラヒック分配器を用いて分配されたデータに対して，解析できる機能が要求される．
4. 1 Gbps 以上のスループットが必要である．本学の対外接続回線は 1Gbps であるため，1Gbps 以上のスループットが要求される．
5. ログを syslog サーバへ出力できる機能が必要である．侵入検知システムに負荷をかけないために，解析を syslog サーバで行う必要がある．したがって，ログを syslog サーバに出力する機能が要求される．

・トラヒックモニタリングシステム

1. ssh で遠隔からコマンドを投入できる機能が必要である．syslog サーバで解析された結果を基に，トラヒックモニタリングシステムを遠隔操作し，必要なダンプデータだけを抜き出す必要がある．これらの操作を自動で行うため，遠隔から操作できることが要求される．
2. 約 1 日程度のトラヒックを保存できる必要がある．本学のトラヒック流量の場合，1 日約 500 GB 程度のストレージが必要である．

・syslog サーバ

1. 侵入検知システムとして採用した PaloAlto 社製 PA-2050 が出力するログから，異常を検出した場合に IP アドレスおよび時間帯を取り出すスクリプトが必要である．
2. 1 のスクリプトに連動して，NetDetector のローカルストレージから外部ストレージへ異常トラヒックをエクスポートするスクリプトおよび，異常検出のサマリをメールにて管理者へ通知するスクリプトが必要である．

4. 設計

本章では，本研究で構築した異常トラヒックの自動保存システムの設計とその構成要素について述べる．

4.1 構成要素

図 1 に本提案システムの構成図を示す．本システムは以下に示す要素から構成されている．

・トラヒック分配器

本学はトラヒック分配器として L1 スイッチである APCON 社製 IntellaPatch[13]を設置している．この L1 スイッチを大学の出入り口に設置し，全てのパケットを上流と下流毎に別々のポートに出力している．また，IntellaPatch は 1 ポートを複数の装置へ分配することができるため，図 1 に示すように，侵入検知システムとトラヒックモニタリングシステムへトラヒックを分配している．またこれら以外にも実験系のモニタリングシステムにもトラヒックを分配している．

・侵入検知システム

侵入検知システムは，要求要件で示した要件を満たしている PaloAlto Networks 社製の PA-2050 である．PaloAlto は 2ch への書き込みや，winny，bittorrent，gnutella などの P2P アプリケーションを検出すると，syslog サーバへログを出力する．大量の異常トラヒックによるアラートストームの問題を回避するために，必要最小限の P2P アプリケーションに関してのみ検出する様な設定としている．

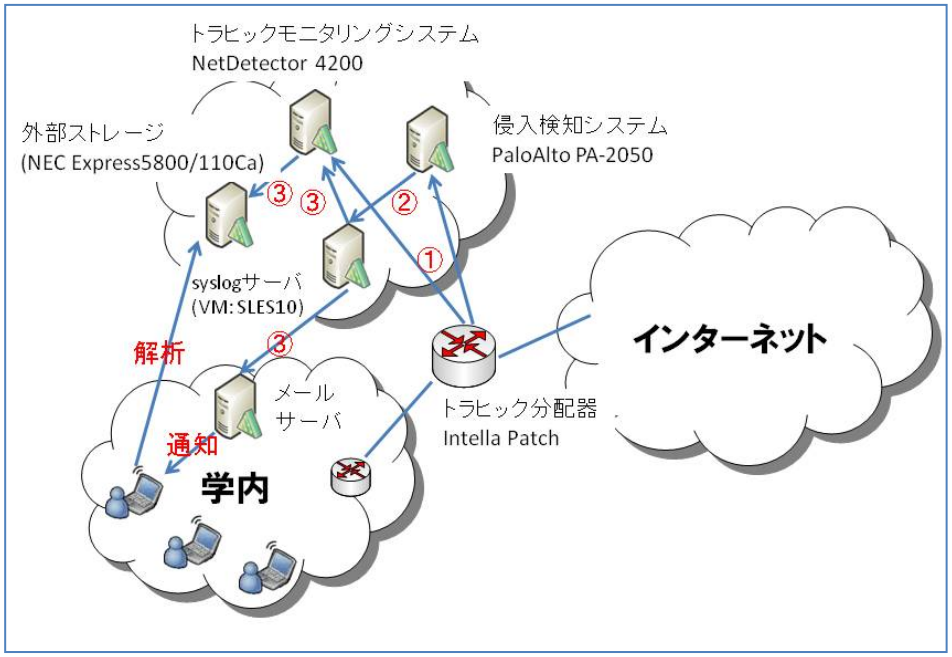

図 1　システム構成図

・トラヒックモニタリングシステム

トラヒックモニタリングシステムは NIKSUM 社製 NetDetector 4200 である．NetDetector では，パケットをローカルディスクへ保存し，WEB 経由での解析も可能である．また，syslog サーバから ssh 経由でコマンドを実行し，条件にヒットしたパケットのみを外部ストレージへ出力することも可能である．

・syslog サーバ

本学の教育システムで導入されている HP BladeSystemc7000 上で動作している VM に，SUSE Linux Exterprise Server が動作している．syslog サーバでは， 異常トラヒックを検出した際の IP アドレスの取得や時間帯の取得，さらにトラヒックモニタリングシステムに対する操作を行うスクリプトが cron により定期的に動作している．

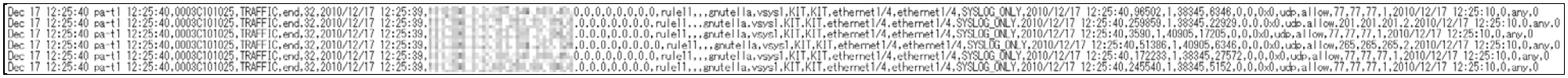

図 2 syslog の出力例

・外部ストレージ

NEC Express5800/110Ca に USB 接続で 1 TB の外部ストレージを接続し，OS には FreeBSD を用いている．外部ストレージに保存された個別の異常トラヒックに対して，管理者は NetDetector の GUI を用いた解析や，wireshark を用いた解析を行う．

・メールサーバ

日々の業務に用いているメールサーバである．syslog サーバから通知された警告を受信する．

4.2 処理手順

1. トラヒック分配器を通ったパケットは，侵入検知システムおよびトラヒックモニタリングシステムへコピーされて配送される．侵入検知システムでは，異常パケットであるかどうかを判断する．また，トラヒックモニタリングシステムでは，ローカルディスクにパケットを保存する．

2. 侵入検知システムにおいて異常パケットであると判断した場合，侵入検知システムは syslog サーバへ異常トラヒックの通知を行う．図 2 に syslog サーバの出力例を示す．syslog 中のアプリケーションを示すフィールドを確認して異常トラヒックの内容を識別する．図 2 では gnutella 系のプロトコルが検出されている．

3. syslog サーバは cron により以下の様な処理手順でスクリプトをする．
   I. 前回のチェック以降の検知の確認
   II. 新しい検知があった場合，以下の処理を行う．
   III. 書き込み元の IP アドレスの取得
   IV. 書き込み先の IP アドレスの取得
   V. 書き込み時刻の取得
   VI. トラヒックモニタリングシステムからの書き込み時間帯のパケットの取得
   VII. 外部ストレージへのパケットの出力（2ch の書き込みの場合，解析に NetDetector を用いているため，外部ストレージから再びパケットモニタリングシステムにデータを書き戻している)
   VIII. 検知ログのメール送信

4. 図 3 に syslog サーバでログ処理した後に管理者へ送られる通知メールの例を示す．図 3 では 30 分間の間に 7 回の 2ch への書き込みが検出され，書き込み元の IP アドレスが列挙されている．

5. 外部ストレージに出力されたパケットを解析するために，pcap ファイルを strings コマンドにより確認したり，wireshark などを用いてトラヒックの詳細を分析する．

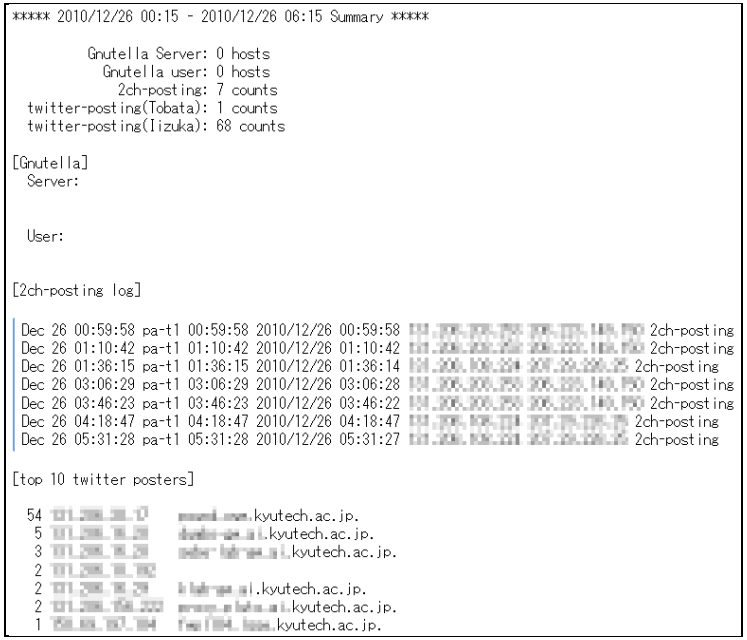

図 3 syslog サーバからのメール通知例

5. 運用例

本章では，本提案システムを用いた運用例について述べる．

5.1 2ch 書き込みの検出例

図 4 および図 5 に 2ch への書き込みを解析した例を示す. 図 4 は NetDetector を用いた解析結果である. NetDetector の GUI では日本語の文字列がコード化されて正しく表示できない．そこで文字コードを解析するスクリプトを通した結果が図 5 である．この例では，書き込みの内容については問題ないと思われる．

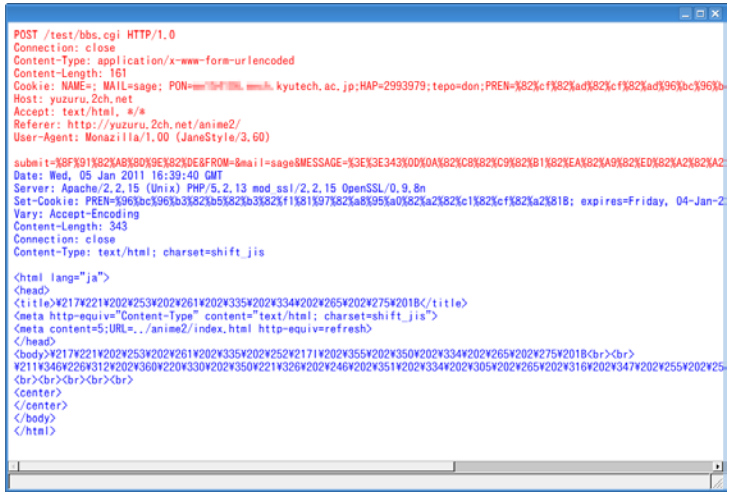

図 4　2ch 運用例（１）

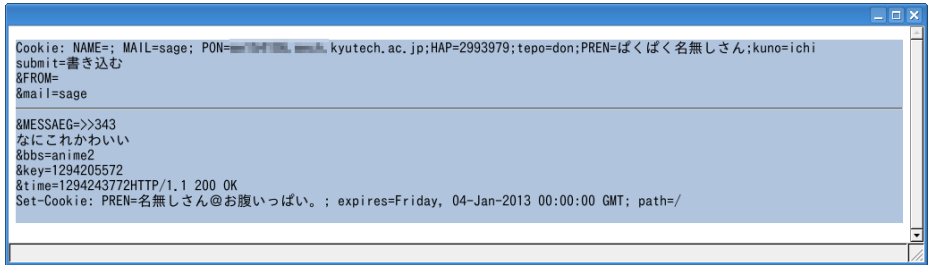

図 5　2ch 運用例（２）

5.1 cabos の検出例

図 6, 7 および 8 に P2P アプリケーションの 1 つである cabos の検出例を示す. Paloalto では cabos は gnutella として検出される．したがって，syslog サーバのログにおいて gnutella が検出された場合，IP アドレス，時間帯を元にダンプデータを NetDetector より pcap 形式で取り出す．取り出されたデータは wireshark で解析を行う．図 6 は wireshark において cabos のセッションを取り出す作業を行っている．

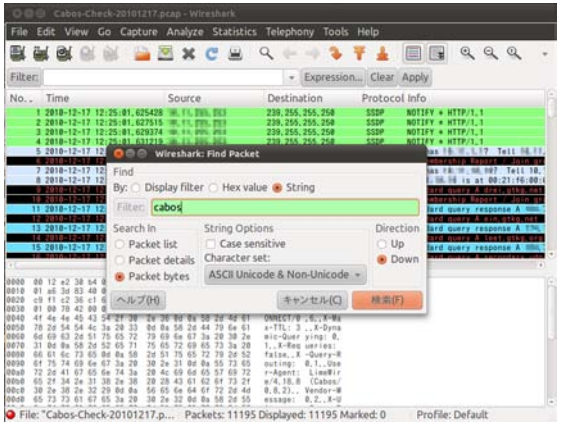

図 6 cabos　運用例（１）

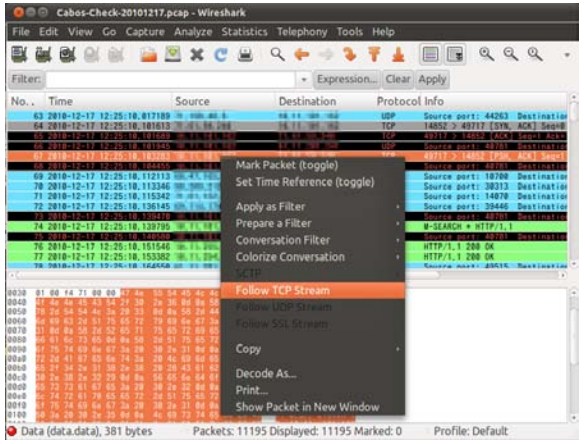

図 7 cabos 運用例（２）

cabos に関連するパケットが抽出されたのちに TCP フローの再構成を行い，通信の内容を確認する．図 7 では TCP フローの再構成を行っている．図 8 はフローが再構成され通信の内容が判別した結果である．図 8 の結果より、limeware/4.18.8(cabos 0.8.2) が用いられていることが分かる．cabos の場合は user-agent フィールドにこの様に情報が入っているためアプリケーションの判別は容易であるが，P2P アプリケーション毎に挙動が異なるため，解析作業は容易ではない．

P2P アプリケーション検出後は IP アドレスより収容しているスイッチとポート番号を特定し，全学の管理責任者へ報告を行う．その後，各組織の管理責任者にインシデント対応を依頼する．

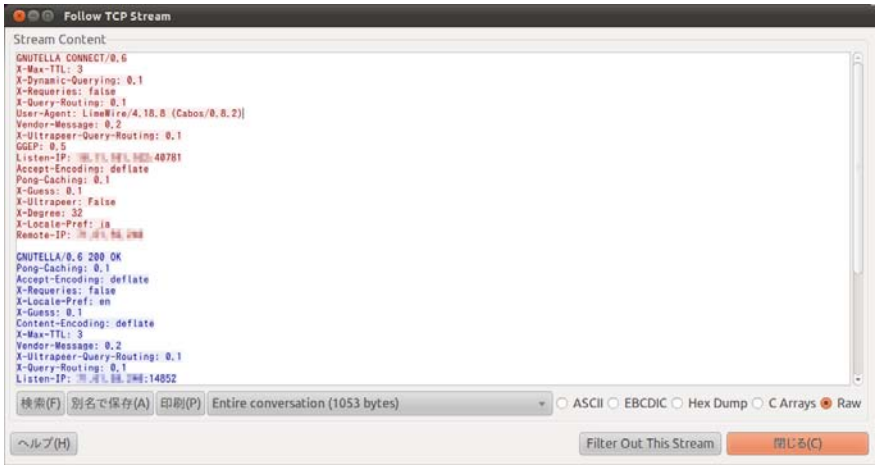

図 8 cabos 運用例（３）

6. まとめと今後の課題

本研究では，既存の侵入検知システムとトラヒックモニタリングシステムを連動させ，異常トラヒックを自動的に保存するシステムを構築した．具体的には，既存の侵入検知システムを用い，2ch への書き込みや P2P アプリケーションを検出し，それらの結果を syslog として保存させる． cron により定期的に syslog は解析され，IP アドレスや時刻などの必要な情報が取り出される． syslog サーバはトラヒックモニタリングシステムに対して，遠隔操作により特定のトラヒックを取り出し外部ストレージへ出力させる．本システムを構築したことによって我々は 2ch への書き込みに対して，自動的にその前後の時刻を取り出して抽出し，個別に保存することが可能となった．また，P2P アプリケーションに対しても，同様の手順で処理し，外部ストレージへ手動で保存できるようになった．これにより，ネットワーク管理者のセキュリティインシデントに対する作業負荷を軽減させる事が可能となった．

今後の課題として，P2P トラヒックの自動保存が考えられる．2ch と同様にスクリプトにより外部ストレージへ出力することは可能であるが，実際の P2P 利用に関して，コンテンツの判断や，誤検知などの問題があるため，自動化には至っていない．また，取得したダンプデータの解析も難しい．今後管理者の負担を軽減させるためには，インターネットを通して運ばれるコンテンツの内容がポリシーに従っているかそうでないかを判断する必要がある．これは各組織のポリシー策定とも関連するため技術的に解決することは容易ではないと考えられる．

参考文献

1) snort http://www.snort.org/
2) libpcap http://www.tcpdump.org/
3) Juniper Networks http://www.juniper.net/
4) Cisco Systems http://www.cisco.com/
5) Palo Alto Networks http://www.paloaltonetworkds.com/
6) NetAgent http://www.onepointwall.jp/
7) tcpdump http://www.tcpdump.org/
8) wireshark http://www.wireshark.org/
9) NIKSUN http://www.niksun.com/
10) Fluke Networks http://www.flukenetworks.com/
11) 中島潤:「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」北海学園大学経営論集 7(3), pp.51-63, 2009-12-25
12) 中島潤, 居内寛貴, 岸本裕之:「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」情報科学技術フォーラム講演論文集 7(4), pp.123-124, 2008-08-20
13) APCON http://www.apcon.com/
14) eEye http://www.eeye.com/