福井大学 大学院工学研究科 研究報告 第 56 巻 2008 年 3 月
Mem. Grad. Eng. Univ. Fukui, Vol. 56 (March 2008)

トラフィックの常時監視に基づくネットワークセキュリティの向上
– DTI ハブの設計と実装 –

富田 陽祐* 白井 治彦** 黒岩 丈介*** 小高 知宏* 小倉 久和***

Network Security System Based on the Constant Monitoring of Traffic
– Designing and Implementation of the DTI Hub –

Yosuke TOMIDA*, Haruhiko SHIRAI**, Josuke KUROIWA***
Tomohiro ODAKA* and Hisakazu OGURA***

(Received January 31, 2008)

We propose a network security system that separates the machine that causes abnormality. We developed the Dynamic Traffic Inspection (DTI) hub that autonomously cut off the machine emitting abnormality from the network. Firewall and Intrusion Detection System (IDS) that the exist as defense methods are not suitable for defense of the attack from the inside on the network. We designed the DTI hub that intend to prevent the attack from the inside on the network. The attack that cannot be prevented by firewall and IDS can be prevented by using the DTI hub. We experimented the performance of the DTI hub about some network attacks. As a result, we confirmed the availability of the DTI hub. The security of the network is expected to improve by combining the DTI hub with firewall and IDS that exist as defense methods.

Key words : Network Security, Traffic, DTI Hub, Firewall, Intrusion Detection System

1. 緒 言

ネットワークセキュリティの管理は，昨今の社会にとって重要な課題となっている．特にインターネットの普及や情報技術の活用は，生活の利便性を向上させる一方で，社会のネットワーク攻撃に対する脆弱性を増大させている[1],[2]．それらの問題に対してファイアウォールやネットワークの不正行為を検知し通知するシステムである IDS(侵入検知システム) といった対策が施されてきた[1]．しかし，それらの防御対策だけではネットワークの内側からの攻撃に対しては不十分である．ネットワーク攻撃の知識に乏しいエンドユーザがワーム等に感染した PC を内部ネットワークに接続した場合，ネットワークに感染が蔓延し多大な被害を出す恐れがある．さらには，本来被害者であるエンドユーザが第三者の加害者になってしまう危険性がある．

本研究では，ネットワーク装置であるハブにおいて，エンドユーザから送信されるパケットを監視し，異常を検出した場合に異常元をネットワークから切断する機能を有する新しいネットワークセキュリティ機器を提案する[3]．この機器は，ネットワーク装置として，自律的に異常元を完全に切り離すというこれまでにないシステムを組み込んだハブであるので，システム名の Dynamic Traffic Inspection の頭文字をとって DTI ハブと呼ぶことにする[3]~[5]．本稿では，DTI ハブの設計と実装を行い，動作実験を行う．

*工学研究科原子力・エネルギー安全工学専攻
**技術部
***工学研究科知能システム工学専攻
*Nuclear Power and Energy Safety Engineering Course, Graduate School of Engineering
**Dept. of Technology
***Human and Artificial Intelligent Systems Course, Graduate School of Engineering

DTI ハブを用いることで，ファイアウォールや IDS といった既存の防御策では防ぐことができないネットワークの内側からの攻撃に対応することができ，よりセキュアなネットワークが構築できるとともに，本来被害者であるエンドユーザが第三者の加害者になることを防ぐことができると考えられる．

2. 既存防御策での問題点

2.1 ファイアウォールを用いた対策での問題

ファイアウォール[1]とは，外部のネットワークから不正なアクセスによるアタックを防御するための全てのメカニズムである．ファイアウォールの防御方法の仕組みとしては，パケットフィルタリングとアプリケーションゲートウェイの二つに分類できる．

パケットフィルタリングは送信元や送信先の IP アドレス，ポート番号などによって通信データを通過させるかどうかを判断する方式である．しかし，一般的なパケットフィルタリングでは，パケットが正常に受信されたことを意味する ACK 信号は通過させている．これを利用することでパケットフィルタリング機能を無効化した不正アクセスが問題となっている．この問題に対応すべく最近では，LAN 側から送信したデータをセッションログとして保存しておき，WAN 側から到着したパケットがセッションログと矛盾しないかを確認する，ステートフルインスペクションと呼ばれる方式を使用する製品もある．

アプリケーションゲートウェイは，通信を中継するプロキシプログラムを使用することで，内部ネットワークとインターネットを切り離して，内部ネットワークのマシンが外部と直接接続することなく，セキュリティ的に安全にサービスを利用することができる．

しかし，ステートフルインスペクションを採用した高性能なファイアウォール製品でないかぎり，ワームが送り込んでくる異常なパケットをすべてチェックすることは不可能である．例えば，不正な HTTP リクエストという形で侵入する Nimda のようなワームを遮断することはできない．また，ファイアウォールは，外部ネットワーク (インターネット) と内部ネットワーク (内部 LAN) との境界に設置するが，図 1 に示す様に，内部ネットワーク外でワームに感染したパソコンをそのまま内部ネットワークに接続した場合にはファイアウォールを通過しないので，内部ネットワークにワームが拡散してしまうことになる．

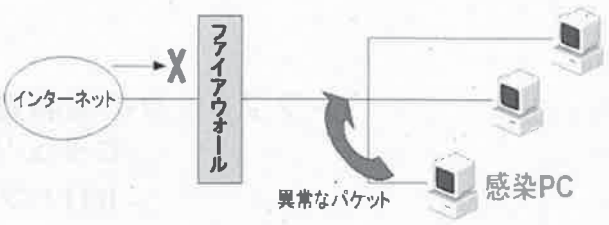

図 1: 内部ネットワーク内でのワーム感染拡大

2.2 IDS を用いた対策での問題

IDS は Intrusion Detection System の略で，侵入検知システムとよばれ，コンピュータやネットワークに対する不正行為を検出し，通知するシステムである．さまざまな製品が市場に出回っているが，IDS は侵入検出の方法により，不正検出と異常検出に分類できる．

不正検出は，あらかじめ登録されたシグネチャと呼ばれる侵入手口のパターンとマッチングさせることにより検出する手法であり，既知の攻撃に対しては検出が可能である．

一方，異常検出は，通常とは異なる振る舞いを検出する方法である．ログイン時刻や使用コマンド，ネットワークのトラフィック状況などから判断することで未知の手法による攻撃も発見できる．また，設置方法からホスト型とネットワーク型の二つに分類できる．ホスト型 IDS は，保護したいコンピュータにインストールし，ログファイルやファイルの改竄の監視を行う．ネットワーク型 IDS は，接続しているネットワークのセグメントのトラフィックをすべて監視するものである．しかし，IDS は，異常をネットワーク管理者に通知するだけであり，異常な通信を防ぐことはできない．

現在の IDS は検知機能の他に遮断機能を実装したものも多い．IDS に実装された遮断機能は，TCP を用いた攻撃であった場合，TCP リセットパケットを送信してその TCP セッションを切断したり，ファイアウォールの設定を動的に変更することによってその送信元 IP アドレスからの通信を遮断したりするものである．図 2 は，IDS による TCP リセットを使用したセッション切断の仕組みを示している．IDS が TCP を使用した攻撃を検知すると，そのパケットの送信元と宛先の両方に対して TCP リセットパケットを送信する．これにより，攻撃に使用されている TCP セッションを切断することができる．図 3 は，ファイアウォールと連携することによって攻撃を遮断する仕組みを示したものである．IDS が攻撃を検知すると，ファイアウォールのフィルタリングルールを動的に追加して，その攻撃ホストからのアクセスを一定時間受け付けないように設定す

る．これにより，あとに続く攻撃ホストからのアクセスを遮断することができる．

しかし，IDS に実装されている遮断機能は完璧とはいえない．IDS が攻撃を検知したときにはすでに不正なデータの入ったパケットは宛先に届いており，その後に TCP リセットパケットを送信したり，ファイアウォールの設定を変更したとしても，その間に攻撃が成功しており，手遅れになる場合がある．また，IDS の不正検出や異常検出は，外部ネットワークからの攻撃を対象に設定されているので，内部ネットワーク内からの攻撃に関しては，防御機能が優れているとはいえない．

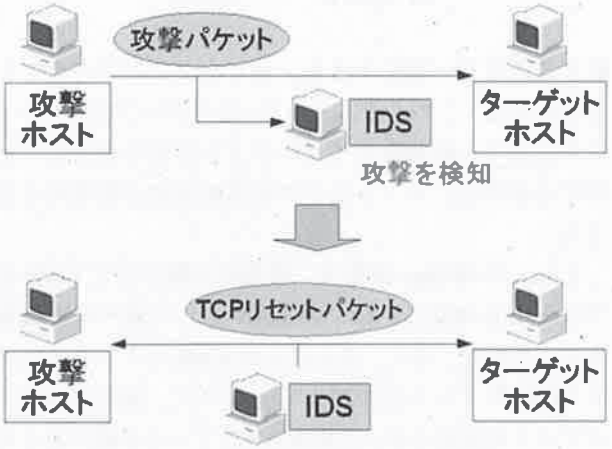

図 2: TCP セッションを使用した切断の仕組み

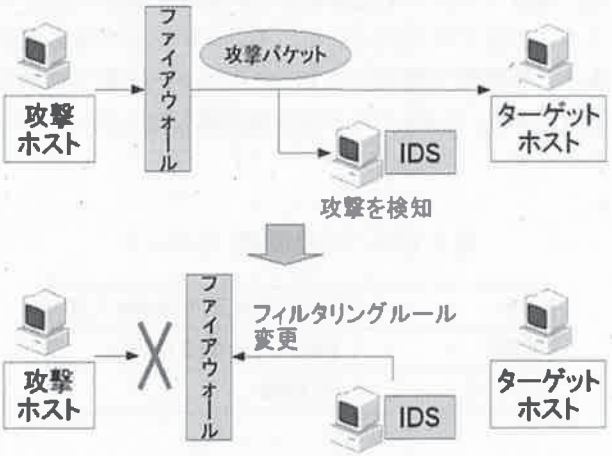

図 3: ファイアウォールと連携した遮断の仕組み

3. DTI ハブの設計

3.1 DTI ハブに要求される機能

前節では，既存の防御策であるファイアウォールや IDS の問題点を指摘した．本研究では，それらの問題点を考慮し，新たなセキュリティ機器として DTI ハブの設計を行った．ファイアウォールや IDS は外部ネットワークの攻撃を対象とした防御策であり，内部ネットワーク内からの攻撃の防御には向いていない．したがって DTI ハブでは，内部ネットワークからの攻撃を対象とした防御機能が要求される．以下に DTI ハブに要求される機能をあげる．

- ネットワーク装置のハブとしてパケットを取得，解析

エンドユーザのパケットを監視対象とするので複数のポートを監視でき，ネットワークのトラフィックを監視できるネットワーク型の接続方法を用いる．そこで，内部ネットワークのセグメント間に手軽に設置できるネットワーク装置であるハブにおいて常時パケットを監視，解析する．接続ポイントは通常のスイッチングハブが使用される位置であり，エンドユーザの使用する PC から物理的に一番近い位置に接続する．

- 異常と判断した場合に異常元を切断

異常があると判断した場合には，異常元をネットワークから切断する．異常かどうかの判定は inspection ルールによって判定を行う．DTI ハブの inspection ルールは，異常検出の方法を用い，パケット流量の統計に基づいて切断判定を行う．したがって，DTI ハブを導入するネットワークのトラフィックを事前に調査する必要がある．DTI ハブは，事前のトラフィック調査によってそのネットワークに合った inspection ルールを設定できるようになっている．図 4 に，DTI ハブを導入したネットワークを示す．これらの機能を持った DTI ハブをネットワークに導入することで，攻撃を起こしている PC をネットワークから切断し，被害拡大を防ぐことが可能であると考える．

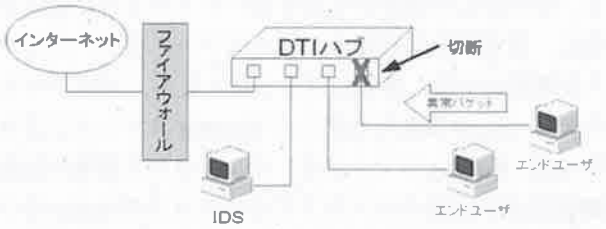

図 4: DTI ハブの設置

3.2 inspection ルールの設定

inspection ルールの設定において，異常を判断する方法として以下のような方法を用いる．過去の一定時間のトラフィック状態を正常な状態としたときに，次の

時間に観測されたトラフィック状態が正常状態からどの程度のゆらぎがあるかにより，正常であるか異常であるかを判断する [6].

各種の攻撃は大量のパケットをネットワーク上に出力するが，Web アクセスやファイル転送など正常通信時も同様にトラフィックが増加する．しかし，エンドユーザの PC からパケットを常に出し続ける状況は正常な通信時には考えにくい．本研究では，パケットの流量を一秒毎に測定し，一定時間内においてパケットが流れていない回数を測定する．この回数が正規分布に従うとして，有意水準 $\alpha = 5\%$ において判定を行う．本稿では，300 秒間のパケット流量が 0(byte) である回数を測定し，そのネットワークにおいて 30 秒間でのパケット流量が 0(byte) になる回数を有意水準 5% で異常判定を行う．

4. DTI ハブの実装

4.1 システムの実装

本研究で作成した DTI ハブは PC をハブのように機能させ，プログラムを組み込んだものである．プログラムは，異常なトラフィックを検出し，切断するプログラムで pcap ライブラリを利用している．pcap ライブラリは Van Jacobson 氏らの開発したライブラリで，このライブラリを用いることで，ネットワークインタフェースが手に入れることができるすべてのパケットを，データとして得ることが可能である．

4.2 システムの構成

本研究で作成したシステムは図 5 に示すような流れになっている．システムが実行されると，ネットワークインタフェースを取得する．そこからパケットを取得し，次にパケットからヘッダ情報を取り出す．ここで，取り出した情報から異常なパケットであるかを判定し，異常がある場合は，ネットワークインタフェースを無効にする．無効にする方法として，プログラム内から system 関数を利用して ifconfig コマンドにより行った．ifconfig コマンドは，ネットワーク環境の状態確認/設定のためのコマンドでオプションの down をつけることで，指定したネットワークインタフェースを停止することができる．

4.3 DTI ハブハードウェア構成

本研究で設計した DTI ハブのハードウェア構成は，Linux の Bridge 機能を使用することで PC をスイッチングハブの役割を果たすものとした．

スイッチングハブは，パケットの伝送先をハブが解

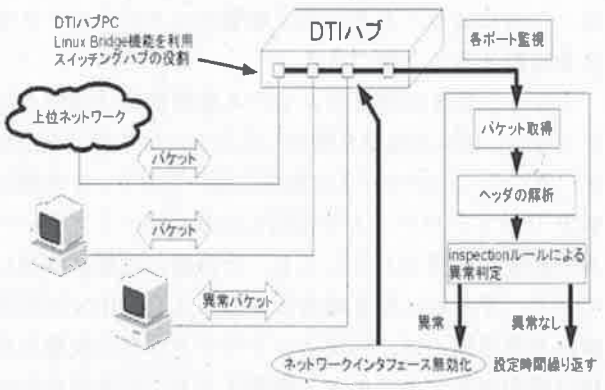

図 5: DTI ハブシステム

析することで，関係するコンピュータにだけパケットを伝送する．このように，スイッチングハブは，パケットを伝送する経路をスイッチのように切り替えることができるので，ネットワーク全体の通信が効率的に行える．

Linux の Bridge 機能は，複数の分離された LAN セグメントを接続し，単一の LAN として働かせる機能をもっている．また，それぞれの LAN セグメントにある MAC アドレスを管理しているので，適切な経路でパケットを伝送させ，不要なトラフィックを避けることができる．

Bridge 機能を使用するためには，Bridge 機能をもったカーネルで PC を起動させ，これを有効にする．また，brctl コマンドを使用するため bridge-utils からソフトウェアをダウンロードし，インストールする必要がある．本研究で使用した PC のスペックは表 1 に示す通りであり，LAN カードを 3 枚搭載した 3 ポートのハブとした．

表 1: DTI ハブ使用 PC スペック

OS	Linux 2.6.22 Ubuntu 7.10
CPU	Intel Celeron 2.8GHz
メモリ	512MB

4.4 DTI ハブソフトウェア構成

本研究で作成したプログラムは図 6 に示す構成になっている．

main 関数内では，設定時間内に sig_alarm 関数が呼び出される．sig_alarm 関数は，パケット流量の標準出力と inspection ルールによる切断判定を行う役割を持つ．ここで，異常なパケットと判断された場合は system 関数よりネットワークインタフェースを停止するコマン

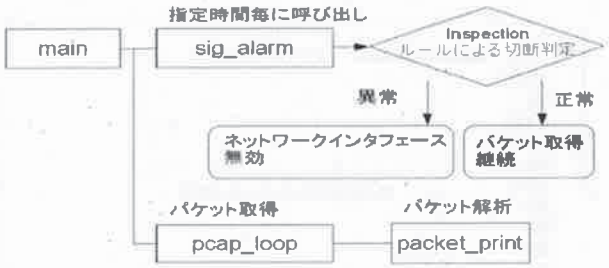

図 6: 関数構造

ドが呼び出される．次に，pcap ライブラリで用意されている pcap_loop 関数を呼び出す [7]．pcap_loop 関数は pcap によるパケット取得を繰り返し実行する関数である．更に，pcap_loop 関数は packet_print 関数を呼び出す．packet_print 関数は，パケットの大きさを取り出し，パケットの合計を計算する．このようにして合計されたパケットの流量は，設定された時間毎に呼び出される sig_alarm 関数によって inspection ルールによる切断判定が行われる．正常なパケットと判断された場合は sig_alarm 関数は改めてアラームをセットし，パケット流量を標準出力に書き出す．最後に変数をクリアした上で標準出力をフラッシュする．

5. DTI ハブ動作実験

5.1 ネットワークの構成

DTI ハブ動作実験でのネットワークの構成を図 7 に示す．DTI ハブからの接続は，eth1 の LAN ポートからは上位ネットワーク (インターネット)，eth0 の LAN ポートからは実験 PC1，eth2 の LAN ポートからは実験 PC2 へとそれぞれ接続されている．eth0 と eth2 は，それぞれエンドユーザを想定した同一のセグメントに繋がっているものとする．使用した実験 PC の構成は表 2，3 に示す通りである．DTI ハブと実験 PC との間はクロスケーブルで接続している．

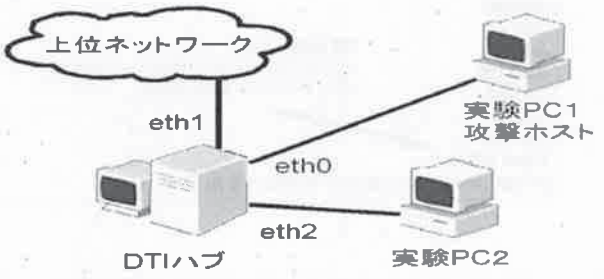

図 7: ネットワーク構成図

表 2: 実験 PC1 スペック

OS	Linux 2.6.22 Ubuntu 7.10
CPU	Intel Pentium4 3.0GHz
メモリ	1GB

表 3: 実験 PC2 スペック

OS	Linux 2.6.22 Ubuntu 7.10
CPU	Intel Celeron 2.8GHz
メモリ	512MB

5.2 inspection ルール設定の予備実験

inspection ルールの設定のための実験 PC1 のトラフィック調査の結果を図 8 に示す．調査時間は 300 秒とし，その間のパケット流量が 0(byte) となる回数を調べた．その結果，離散的にパケットが発生していることが確認できる．このネットワークにおいて 30 秒間でのパケット流量が 0(byte) になる回数は，有意水準 5%で考えると，11 から 21 回の間で観測されると考えられる [8]．したがって，パケット流量が異常と判断できるのは，30 秒間にパケット流量が 0(byte) である回数が 10 回より少ない場合となる．

前述から，30 秒間でパケット流量が 0(byte) となる回数が 10 回だと異常とみなしているので本研究では，20 秒連続してパケットを観測した時点で異常が発生したものとみなし，inspection ルールを設定した．

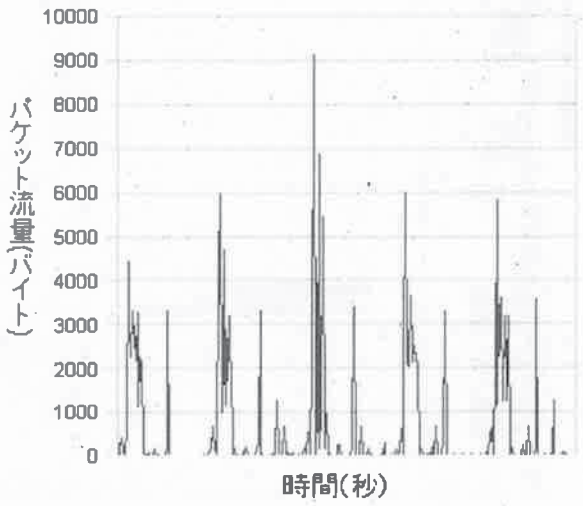

図 8: トラフィックの特徴

5.3 DoS 攻撃に対する動作実験

本研究で行った動作実験は，攻撃ホストである実験 PC1 からターゲットホストである実験 PC2 に DoS 攻撃を行った．DoS 攻撃には，ICMP Flood 攻撃を用いた．ICMP Flood 攻撃は，ping コマンドより膨大な数の ICMP Echo 要求パケットを送信する攻撃方法である [1]．攻撃者側がターゲットホストよりも処理能力が優れていた場合，ターゲットホストの処理が追いつかずサービスが停止してしまう．

本実験での DTI ハブの監視ポートは，攻撃ホストである実験 PC1 が接続されている eth0 に注目して動作を確認した．

図 9 に正常な通信時の DTI ハブの eth0 監視画面を示す．図 9 では，バースト的なトラフィックが生じているが，これは Web ページの閲覧により一時的にパケット流量が増加したものである．しかし，パケットは離散的に発生しているので，inspection ルールにおいて異常と判断されない．したがって，DTI ハブは監視を継続的に行う．

図 10 は，攻撃ホストである実験 PC1 からターゲットホストである実験 PC2 への ICMP Flood 攻撃を模倣した時の DTI ハブの動作画面である．パケット流量は，多くはないが断続的にパケットが発生している．本実験での inspection ルールでは，20 秒連続してパケットを観測した場合異常とみなしている．20 秒目を観測した瞬間にネットワークインタフェースを無効にすることで，異常元をネットワークから切断したことを確認した．

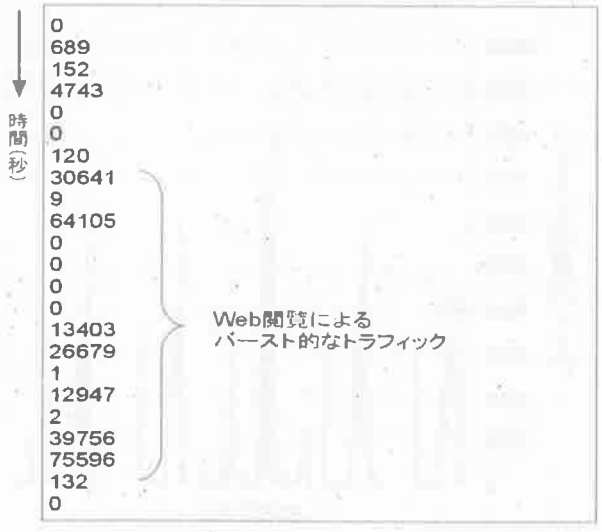

図 9: 正常時の DTI ハブ動作

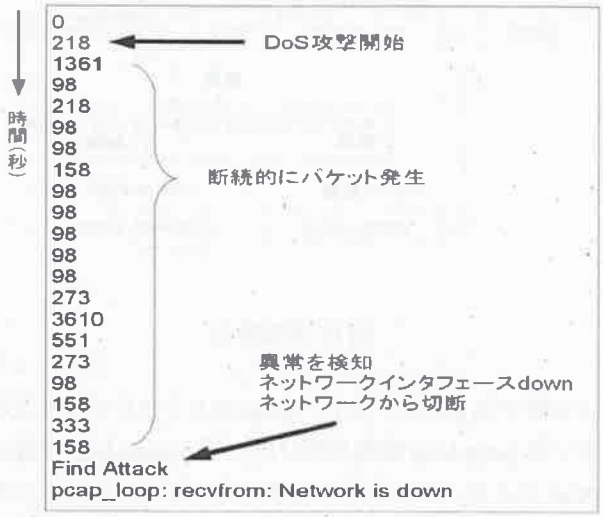

図 10: DoS 攻撃時の DTI ハブ動作

5.4 ポートスキャンに対する動作実験

2 つめの動作実験として，攻撃ホストである実験 PC1 からターゲットホストである実験 PC2 へのポートスキャンを行ったときの動作実験を行った．ポートスキャンは，クラッカーやワームが不正侵入を試みる際に，セキュリティホールを探るために行うものである．

動作画面を図 11 に示す．ポートスキャンが実行されると，大量のパケットが断続的に観測される．inspection ルールにより，20 秒連続してパケットを観測した場合，異常が発生しているとみなしているので，異常元をネットワークから切断している．

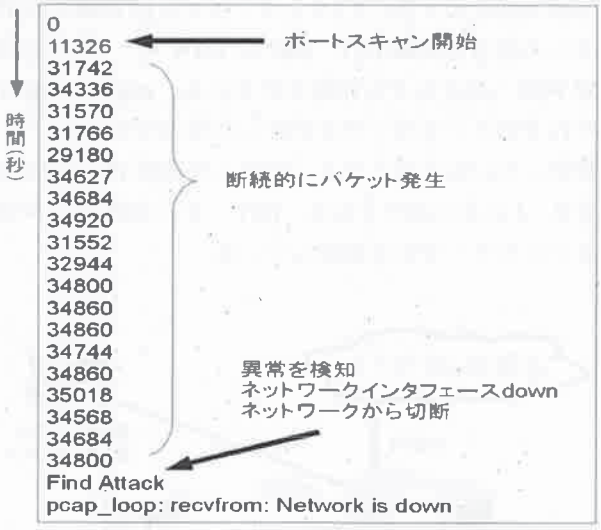

図 11: ポートスキャン時の DTI ハブ動作

5.5 ワームに対する動作実験

ワーム検出の動作実験は，実際のワームを用いずに，ワームの挙動を ping によりシミュレートしたパケットを攻撃ホストである実験 PC1 からターゲットホストである実験 PC2 に送信した場合の動作確認を行った．

動作画面を図 12 に示す．ワームが送り出すパケットを模倣した攻撃が実行されると，大量のパケットが断続的に観測され，DTI ハブが異常元をネットワークから切断することを確認できた．

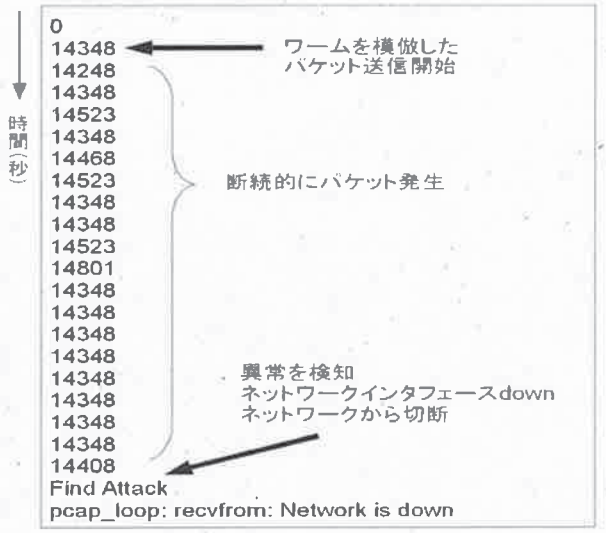

図 12: ワームの検出時の DTI ハブ動作

6. 考 察

動作実験より，DTI ハブが異常なパケットを送信する PC を検知し，すばやくネットワークから隔離することが確認できた．IDS と違い，ネットワークから自律的に切断することでネットワークに及ぼす影響を最小限に抑え，ネットワーク管理者の負担を軽減できるとともに，エンドユーザが第三者の加害者になることを防ぐことができると考えられる．また，ネットワークから切断され，使用できなくなることで，エンドユーザのセキュリティ意識の向上にもつながると考えられる．

inspection ルールにおいては，異常の検出方法にパターンマッチングではなく，トラフィックの統計に基づく検出方法で設定した．これにより，パターンパッチングのようにシグネチャを常に最新版に更新する手間が省けるとともに，未知の攻撃にも対応できると考えられる．

今回は DoS 攻撃，ポートスキャン時の動作実験，ワームの動作をシミュレーションした場合の動作実験を行ったが，大量のパケットを送信するような攻撃に対しても十分防御可能であると思われる．ネットワークのリソースを枯渇させる目的の攻撃には非常に有用であるといえる．しかし，インターネットから大容量のデータをダウンロードする場合や，P2P 通信でデータをやりとりする場合には，本研究で提案した inspection ルールでは誤検知してしまうことが予想され，さらなる inspection ルールの改良が必要と考える．また，本実験では DoS 攻撃とポートスキャンが行われた時の動作実験を行ったが，さまざまな攻撃に関しても，動作実験を行い，inspection ルールの検討を行うことが必要である．

7. 結 言

本研究では，ネットワーク装置であるハブにおいて，エンドユーザから送信されるパケットを監視し，異常を検出した場合に異常元をネットワークから切断する機能を有する DTI ハブの設計と実装を行った．DTI ハブをファイアウォールや IDS といった既存の防御策と組み合わせて導入することで，導入したネットワークのセキュリティを向上できると考えられる．

参考文献

[1] Ipusiron：ハッカーの教科書 完全版，データハウス (2001)

[2] S. Northcutt, M. cooper, M. Fearmow, K. Federick：ネットワーク侵入解析ガイド-侵入検知のためのトラフィック解析法-, Pearson Education (2001).

[3] 富田陽祐，白井治彦，黒岩丈介，小高知宏，小倉久和：セキュリティ機能を有したハブにおける実装方法の検討 -DTI ハブ装置の実現-，平成 19 年度電気関係学会北陸支部連合大会講演論文集，E-26 (2007).

[4] 永山健太郎，白井治彦，高橋勇，黒岩丈介，小高知宏，小倉久和：分散サービス妨害に対するネットワークセキュリティの検討と実装 -DTI ハブの設計と導入-，平成 17 年度電気関係学会北陸支部連合大会講演論文集，E-29 (2005).

[5] 永山健太郎，白井治彦，高橋勇，黒岩丈介，小高知宏，小倉久和：分散サービス妨害に対するネットワークセキュリティの検討と実装，電気情報通信学会技術研究報告，105-396, 23-26 (2005).

[6] 中村信之，中井敏久：トラフィック内部状態変化を利用したネットワーク異常検知，電子情報通信学会技術研究報告，105-12, 17-20 (2005).

[7] 小高知宏：基礎からわかる TCP/IP アナライザ作成とパケット解析，オーム社 (2004).

[8] 和田三樹, 十河清：キーポイント確率・統計, 岩波書店 (2001).