福井大学 大学院工学研究科 研究報告 第59巻 2011年3月
Mem. Grad. Eng. Univ. Fukui, Vol. 59 (March 2011)

DTIハブを用いたネットワーク管理の自動化

牧野 潤* 白井 治彦** 黒岩 丈介*** 小高 知宏* 小倉 久和***

Automatic Network Management Using the DTI Hub

Jun MAKINO*, Haruhiko SIRAI, Jousuke KUROIWA*** Tomohiro ODAKA* and Hisakazu OGURA***

(Received February 10, 2011)

We propose a novel device that makes a PC disconnect from the network if the device detected an abnormal data traffic. This device monitors the network traffic and decides a behavior based on the rules that have been set by a network administrator. This device forces the security policy to user. This device makes a PC disconnect based on the rule from the network and prevents expansion of the damage. We manage the network using this device and reduce the burden of the administrator by this device.

Key words : Firewall, IDS, IPS, Network Management, Network Security

1. はじめに

ネットワークにおいて，ネットワーク管理者が末端の各PCへ管理ポリシを徹底させることは，セキュアなネットワークを構築するにあたって重要なことであるが，ネットワーク管理者にとっては困難なことである[1]．端末側ではユーザがどのような挙動をしているかわからず，それにより危険なコンピュータウイルスがネットワークへと流出し，被害が拡大する可能性がある．本研究では端末側を監視し，ネットワーク管理者の定める管理ポリシに反する挙動を検知した際に端末側のネットワーク接続の権利を奪うデバイスとしてDynamic Traffic Inspection(DTI)ハブ[2]を実装した．これは問題となるPCを強制的にネットワークから切り離すことによって被害の拡大を防ぐものである．これを用いてネットワーク管理の自動化，省力化を進め，ネットワーク管理者の負担軽減を目指す．

2. 既存の防御対策とDTIハブ

DTIハブはネットワーク末端のPCからもっとも近いハブにおいてネットワークベースでトラフィックの監視を行い，ネットワーク管理者が定める管理ポリシに反する挙動を行う端末を自律的にネットワークから強制的に切り離すシステムを実装した．これはファイアウォール(FW)やIntrusion Detection System(IDS)，Intrusion Prevention System(IPS)，検疫ネットワークとは異なるものである．DTIハブはネットワーク管理者の定める管理ポリシに反する挙動を行うPCからネットワークへ接続する権利を奪い，強制的にネットワークから切り離す(図1)．これによりネットワークの安全を確保し，管理者の作業負担を軽減するためのデバイスである．

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

末端PCからのパケットを監視対象とするため複数のポートを監視でき，ネットワークトラフィッ

*大学院工学研究科 原子力・エネルギー安全工学専攻
**技術部
*** 大学院工学研究科 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

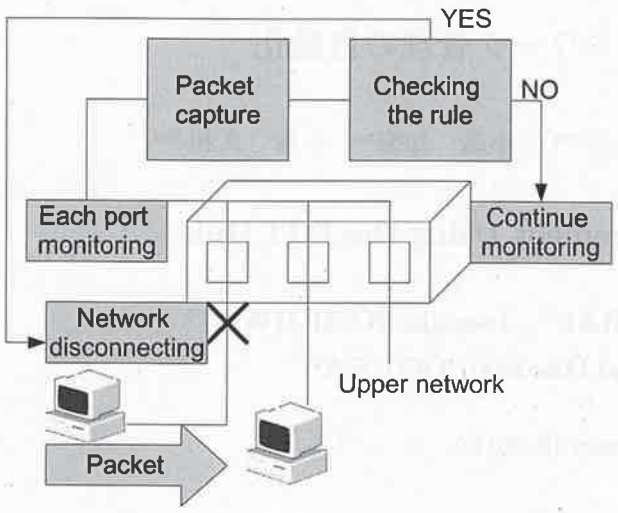

図 1: DTI ハブシステム

クを監視することができるネットワーク型の接続方法を用いる．そこで，内部ネットワークに手軽に設置することができるネットワーク装置のハブにおいて常時トラフィックを監視し，パケットの取得・解析を行う．接続位置は，スイッチングハブが使用される位置であり，ユーザに最も近い位置に接続する．

- 異常であると判断した際に異常元を切断

ネットワーク管理者の定める管理ポリシに反して，異常であると DTI ハブが判断した場合に違反 PC をネットワークから強制的に切り離す．異常であるかどうかの判断は切断ルールを用いることによって行う．切断ルールは，管理ポリシに基づいて作成することができる．FW や IDS はネットワーク全体を保護しているが，DTI ハブはネットワークの一部分を保護するためのデバイスである．ある末端 PC がネットワーク管理者の定める管理ポリシに反する挙動を行っていると判断された場合，PC を利用しているユーザの意思に関わらず強制的にネットワークから切り離すことによってネットワークの安全を確保するものである．

3. DTI ハブの実装

DTI ハブの構成とその実装方法について述べる．また，DTI ハブにおいて重要な切断ルールについての説明も行う．本研究で開発を進めている DTI ハブは，デスクトップ PC をネットワーク装置であるハブのように機能させ動作させたものである．DTI ハブは，ネットワークトラフィックを監視し，ネットワーク管理者の定める管理ポリシに反する挙動を行う PC をネットワークから強制的に切断させる．

本研究で開発を進めている DTI ハブは，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．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 として働かせるという機能を有している．Bridge 機能をもったカーネルで PC を起動させてこれを有効にすることで，Bridge 機能を使用することができる．

本研究で DTI ハブに使用した PC のスペックは表 1 に示した通りであり，Linux ディストリビューションには Fedora を使用した．また，USB-LAN アダプタを用いて複数ポートのハブとして動作させた．

表 1: DTI ハブ使用 PC スペック

OS	Linux Fedora 10
CPU	Intel Celeron 2.8GHz
メモリ	512MB

プログラムは，ネットワークトラフィックを監視し，管理ポリシに反する挙動をした違反 PC をネットワークから強制的に切断させるプログラムで，そのプログラムには pcap ライブラリを使用して作成している．pcap ライブラリは Van Jacobson 氏らが開発したライブラリで，このライブラリを使用することによって，ネットワークインタフェースが取得することができるすべてのパケットをデータとして取得することが可能になる．

切断判定には，管理ポリシに基づいて作成された切断ルールを用いて行う．切断ルールベースを作成し，記法に基づいて切断ルールを記述していく．切断ルールベースとトラフィック監視システムを独立して実装するために，切断ルールベースを字句解析と構文解析を用いて解析した．切断ルールベースを監視システムとは別に作成し，そのファイルを監視システムに定期的に確認させることによってトラフィック監視システムと切断ルールとを独立して実装している．切断ルールベースの内容を一文字ずつ取り込み，構文解析を行うことでその切断ルールが何を示しているかを判断させる．切断ルールの記述方法について述べる．まず，先頭に識別子を記述する．この識別子を用いることで，この後にどの切断ルールを記述するかを判別させる．識別子を記述した後は，切断判定に用いる切断ルールを記述する．実際の記述としては，送信流量についての記述は「a20000」と記述する．このように記述した場合は，送信流量が

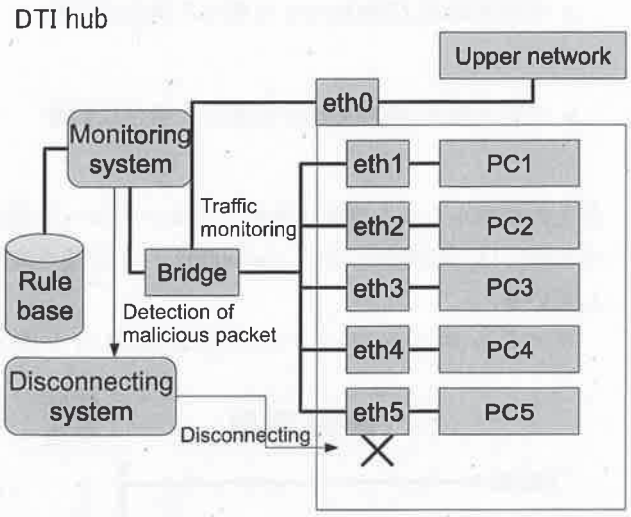

図 2: DTI ハブ構成図

20000 を超えると切断する，と解釈する．さらに切断ルールを追加する場合は，次の行に記述する．また IP アドレスの記述については,「b192.168.111.147」のように記述する．この場合は，IP アドレス 192.168.111.147 を検知した際に切断すると解釈している．ポート番号の記述についても,「c22」のように記述する．この場合，ポート番号 22 を検知した際に切断するルールとなっている．このように，先頭から順番に文字を取り込み，解析を行っている．識別子を先頭につけることによって，その行に何の切断ルールが書かれているかの判別を可能にした．現在の識別子は，送信流量を「a」，IP アドレスを「b」，ポート番号を「c」と設定している．この識別子は字句解析と構文解析のプログラムを変更することで，さらに追加していくことが可能である．

この切断ルールベースをトラフィック監視システムに定期的に確認させることによって切断ルールの更新を行う．トラフィック監視システムと切断ルールベースを独立させて実装しているため切断ルールベースの置き換えも可能であり，切断ルールの追加・変更を容易に行うことができる．また，DTI ハブを停止させることなく，非同期的に切断ルールの追加・変更を行うことが可能である．

4. 動作実験

DTI ハブをネットワーク内に設置し，管理ポリシに反する挙動をした PC を切断する実験を行った．DTI ハブをキャンパスネットワークの末端に設置し複数ポートのハブとして運用して，実際にキャンパスネットワーク内の PC の大部分を DTI ハブによって管理する．DTI ハブは LinuxPC をスイッチングハブとして動作させ，5 ポートのハブとして実装した (図 2)．末端 PC を DTI ハブに接続させて外部ネットワークへ通信するために必ず DTI ハブを通過させることで末端 PC を管理する．ネットワークトラフィックを監視して,管理ポリシに基づいて切断ルールを作成する．作成した切断ルールに反する挙動を行う端末をネットワークから切断する．また，DTI ハブ動作中にも切断ルールの変更が行えることを示すために DTI ハブ動作中に切断ルールの変更を行い，切断ルールの変更が正常に行われるか実験を行った．

動作実験として 3 つの実験を行った．

実験 1 では，パケットを監視し，ネットワークセキュリティを脅かす脅威である可能性がある場合に異常元の PC をネットワークから切断する実験を行った．DoS 攻撃やワーム攻撃などが見せるトラフィックの増大を想定した．切断ルールの設定のため，実験 PC のトラフィック調査を行った結果，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った．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，切断ルールを設定した．ファイルダウンロード時にトラフィックが増加するが，パケットの総流量が PC から送信されるパケット流量の 5 倍以上である場合はファイルダウンロードとみなすよう切断ルールに設定している．

正常な通信時は，バースト的なトラフィックが生じたが，これは Web ページ閲覧で発生したものであり，パケットも離散的に発生しているため切断ルールに異常と判断せず監視を続けた．

DoS 攻撃で使用される攻撃の 1 つの ICMP Flood 攻撃がある．ICMP Flood 攻撃は，Ping コマンドを利用してターゲットサーバに大量の ICMP パケットを送りつけることでサーバを過負荷状態にする攻撃である．この攻撃を用いて図 3 のように実験 PC2 から実験 PC4 へ攻撃を行い実験した．パケットの総流量は，送信されるパケットとその応答パケットの二つを足した値になり，連続してパケットが発生した．20 秒連続してパケットを観測した場合，異常とみなすため 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．

実験 2 で，各ユーザごとに異なる管理ポリシを強制させ，各端末ごとに管理できることを示す．管理ポリシに反する PC はネットワークから強制的に切り離す実験を行った．キャンパスネットワークの管理を行うにあたり，以下のような管理ポリシを設定した．

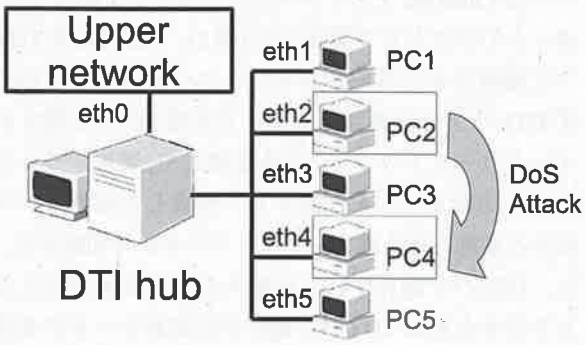

図 3: DoS 攻撃実験図

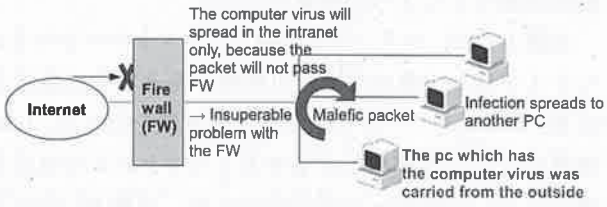

図 4: 内部ネットワーク内でのウイルス感染拡大

- 学生の中で指定した学生のみ動画サイトを閲覧してはいけない.
- 指定した学生以外は指定した動画サイトを閲覧しても良い.

以上の管理ポリシから以下のような切断ルールを作成した.

- 動画サイトを閲覧する際に使用するポートを検出時に切断

この切断ルールを用いて DTI ハブの動作実験を行った. 切断ルールとして, HTTP, HTTPS, DNS のポート番号, それぞれ 80, 443, 53 を検出時に切断するというルールを設定し実験を行った. DTI ハブに接続されているすべての実験 PC において, Web サイト閲覧を行ったが, 切断ルールを適用している実験 PC2 と 4 は Web ページ閲覧を試みると切断されることを確認した. 以後, 管理者が復旧させるまでネットワーク利用不可状態が継続した. これ以外の PC においては, この切断ルールを適用していないため, 問題なく Web ページの閲覧ができた.

実験 3 で, 切断ルールの変更が DTI ハブ動作中に行えることを示す. DTI ハブ動作中に切断ルールの送信流量の閾値を変更し, 正常に切断動作が行われるか実験を行った. あらかじめ DTI ハブに与える切断ルールと変更する切断ルールを以下のように設定した.

- 送信流量が 25000byte/s を超えた場合に切断
- 送信流量が 20000byte/s を超えた場合に切断

以上の切断ルールを実際に切断ルールベースへと記述する際には,「a25000」から「a20000」へと記述を変更している.

ファイルダウンロード中に送信流量の上限を

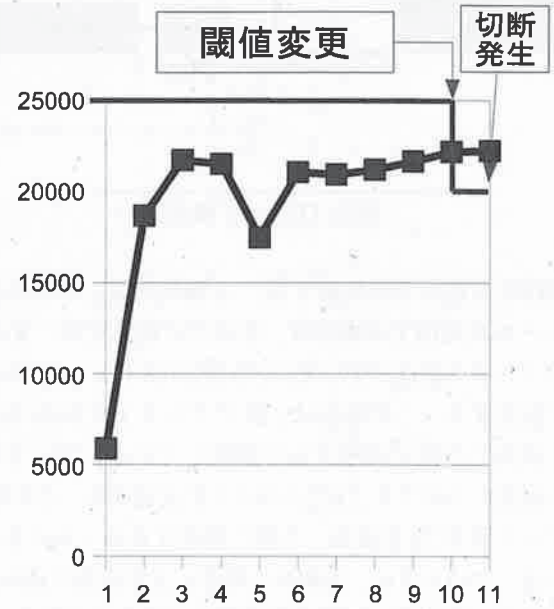

図 5: 切断ルール変更実験図

25000byte/s から 20000byte/s へと変化させる実験を行った. トラフィック監視システムには定期的に切断ルールの確認を行わせている. 今回の実験では, 1 秒毎に切断ルールを確認させている. 図 5 のようにファイルダウンロードを開始するとパケット流量が増加した. しかし, 流量の上限が 25000byte/s であるため異常であると検知されず, トラフィックの監視を継続した. ファイルダウンロードを開始してから 10 秒後に切断ルールの変更を行った. 送信流量の上限を 25000byte/s から 20000byte/s へ変更した. トラフィック監視システムには, 1 秒毎に切断ルールの確認を行わせている. そのため, ファイルダウンロード開始から 11 秒後にはルールが変更されており, 11 秒後の送信流量が上限の 20000byte/s を超えている. その時点で DTI ハブは異常であると判断し, 切断動作が発生した. その後, 復旧するまでネットワーク利用不可状態が継続した.

5. 考 察

ネットワーク装置であるハブにおいて，異常元を自律的にネットワークから切断するシステムを組み込んだDTIハブを提案し，実装した．動作実験からDTIハブは，ネットワークに害をもたらすような挙動を行う端末を強制的にネットワークから切り離せることを確認した．DTIハブを用いることで各端末ごとの管理が可能になり，またネットワーク内部からの攻撃に対処できるため既存の防御策と併用することでよりセキュアで管理のしやすいネットワークを構築できると考える．

本研究では，DTIハブの切断ルールベースを監視・切断システムから切り分け，独立させた．今までのDTIハブはトラフィック監視システムと同一のプログラム上に切断ルールを記述していた.[2]そのため，切断ルールの変更を行うためにはDTIハブを停止させ，再コンパイルを行う必要があった．切断ルールベースをトラフィック監視システムから独立して実装させることでDTIハブを停止させることなく，非同期的に切断ルールの追加・変更が可能である．これは，DTIハブについて詳しい知識を持っていないネットワーク管理者が切断ルールの追加・変更を行う必要があったとしても，容易に変更することが可能であると考える．また，切断ルールを監視・切断システムと切り分けたことは，DTIハブの可能性を広げたと考える．例えば，いくつかの切断ルール群が存在する場合でも，切断ルール群Aを切断ルール群Bに置き換えるだけで変更が可能である．

また，サーバ-クライアント型を用いて切断ルールの変更を行うことが可能になったと考える．現在のDTIハブは，ネットワーク管理者が手動で切断ルールの更新を行うようになっている．切断ルールの更新をネットワーク管理者に行わせることは，切断ルールの変更があるたびに，その都度更新作業を行わなければならず，管理の負担を増加させてしまう可能性がある．ネットワーク管理者は，DTIハブを設置するだけで自動で運用してくれる形が望ましい．この問題を解決するために，サーバ-クライアント型を用いて切断ルールを自動的に更新させることで解決できるのではないかと考える．これは，サーバ-クライアント型を用いてDTIハブ管理サーバで追加・変更された切断ルールをネットワーク経由でダウンロードを行わせて更新させるという方法である．この方法を用いることで切断ルールの更新を自動的に行うことができる．そのため，DTIハブを利用するネットワーク管理者にとっては，DTIハブをネットワーク内に設置するだけで自動的に切断ルールの更新を行い，運用し続けることができる．これにより，ネットワーク管理者の行う切断ルール更新作業を削減できるため，よりネットワーク管理者の負担を減らすことができるのではないかと考える．

既存の防御対策であるFWは，パケットをチェックすることでトラフィックの流れを制御するシステムである．FWは外部ネットワークと内部ネットワークとの境界に設置して内部ネットワークを保護するが，外部のネットワークからウイルスに感染したPCを内部ネットワークへ持ち込み，接続した場合はFWを通過しないため図4のように内部ネットワークへとウイルスが拡散してしまい，ウイルスなどの脅威から末端PCを保護することができない[3]．また感染したPCをネットワークから切断するには管理者が再設定する必要があり，管理者の手間が増加するなどFWは動的な変化に弱い問題がある．DTIハブは，全体ではなくネットワークの一部分の端末を管理者の管理ポリシに基づいて，これに反する端末をネットワークから強制的に切り離している．そのため，内部ネットワークからの攻撃に対処することが可能である．また，ハブであるため設置する数を増やすことで大多数の端末を管理することができる．

IDSを用いた対策での問題は，ネットワークの異常を管理者に通知するだけであるため，異常な通信を防ぐことはできない点である．また，広域ネットワークで使用した場合，現在のネットワークIDSでは処理が問に合わない可能性がある[4]．そのためパケットを取りこぼし，見逃してしまう可能性がある．DTIハブは，接続されている端末に異常が発生した場合に自律的にネットワークから切り離すことができるため，管理者が連絡を受けて対処を行うという作業をする必要がない．そのためネットワークへの被害拡大を防ぎ，管理者の負担の軽減が可能であると考える．

IPSは，ネットワークにおいて特定のネットワーク及びPCへの不正な侵入を防御するシステムである．IPSはIDSの持つ機能に加えて，検知した侵入行為を自動的に切断する機能を持つものである．IPSを用いた対策での問題は，bridgeとは異なりパケットを詳細に分析して検知処理を行う必要があるため，転送処理だけでなく，検知処理も含めたスループットが高くないと，ネットワークの性能がダウンしてしまうという問題がある[5]．また，IPS装置をネットワークに挿入しているため，IPS装置が故障などした場合，ネットワークがストップしてしまう問題もある．DTIハブは，bridgeを用いて実装しているため問題にならない．また，DTIハブはネットワークの末端に設置するため，DTIハブが故障してもDTIハブに接続しているPCのみの影響にとどめることができる．

検疫ネットワークを用いた対策での問題は，検疫ネットワークに対応しているネットワーク機器を導入する必要があるため，費用がかかることとネットワークの再構築に手間がかかることである．また，最新のパッチやウイルス定義ファイルを適用したくても，ネットワーク内で使用されているアプリケーションとの動作確認が取れないためにそれらを適用できないという運用にかかわる問題がある．この場合，最新のパッチやウイルス定義ファイルのチェックが行われると適用されていない端末は隔離されてしまう．そのため，ポリシの定義更新を遅らせる，特定の端末に対して例外的にセキュリティ対策状況のチェックを行わないという運用が必要となるため管理者の負担が増加してしまう可能性がある．DTI ハブはネットワーク装置であるハブであるため，ネットワークの再構築などを行う必要がなく容易にネットワーク内に設置することができる．また，DTI ハブは管理者ベースのデバイスであり，管理ポリシに反する端末は強制的にネットワークから切り離す機能を持っている．そのためユーザを考慮にいれる必要はなく，管理者の負担を軽減できると考える．

DTI ハブはネットワーク内に容易に設置でき，管理ポリシに反する端末を個別にネットワークから切り離す機能を持っているため，内部ネットワークからの攻撃を防ぎたい場合や端末を個別に管理したい場合に効果を発揮すると考える．しかし，現在の DTI ハブは端末をネットワークから切り離した後，手動で復旧作業を行っているため負担軽減効果が半減している．そのため，自動で復旧するシステムを実装するか，管理者の負担が少ない復旧システムを構築する必要がある．

6. 結　言

本論文では，新たなセキュリティ機器として DTI ハブの設計と実装を行った．DTI ハブは，ネットワーク装置としてトラフィックを監視し，ネットワーク管理者の定める管理ポリシに反する動作を行う端末をネットワークから強制的に切断するシステムを組み込んだハブである．DTI ハブは既存の防御対策である FW や IDS，IPS，検疫ネットワークとは違い，ネットワークの一部分のみを保護するシステムである．外部からコンピュータウイルスに感染したノート PC などが持ち込まれ，内部ネットワークへの感染の拡大を防止できる．また，現在の DTI ハブはデスクトップ PC で実装しているため，検疫ネットワークを構築するよりも低コストで運用が可能である．

DTI ハブの重要な要素である切断ルールベースを監視システム等から独立して実装することにより，DTI ハブの可能性が広がった．いくつかの切断ルール群が存在する場合でも，ルール群 A をルール群 B に置き換えるだけで切断ルールを一括で変更することが可能であるため，切断ルールの変更が容易になった．また，サーバ-クライアント型を用いて切断ルールを自動的に更新させることも可能になった．DTI ハブは，既存の防御策である FW や IDS，IPS，検疫ネットワークと併用することで，よりセキュアで管理のしやすいネットワークを構築できると考える．

参考文献

[1] 村瀬一郎．インシデント対応におけるミクロ分析とマクロ分析の融合に向けて．情報処理，Vol. 48 No. 7 pp. 718-725，2007.

[2] 富田陽祐，白井治彦，黒岩丈介，小高知宏，小倉久和．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-．福井大学大学院工学研究報告，Vol. 56，pp. 61-68，Mar 2008.

[3] 前田 秀介，馬場 達也，大谷 尚通，角 将高，稲田 勉．感染プロセスに着目したワーム感染防止システムの実装に関する検討．電子情報通信学会技術研究報告. ISEC, 情報セキュリティ 105(193), 7-14, Jul 2005.

[4] 林 経正，横山 幹，高原 厚，岩橋 政宏．Snort を用いた侵入防止システムの構築と侵入検知処理高速化の検討．情報処理学会研究報告. CSEC, [コンピュータセキュリティ] 2003(45), 59-64, May 2003.

[5] 菊池 一平，佐藤 友暁，深瀬 政秋．不正アクセス防御システムのハードウエア実装．情報処理学会研究報告．CSEC，[コンピュータセキュリティ]，2007(126)，13-18，Dec 2007.