2005－ＣＳＥＣ－30（２）
2005／7／21

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

前田 秀介　馬場 達也　大谷 尚通　角 将高　稲田 勉

(株)NTT データ 技術開発本部

〒104-0033 東京都中央区新川 1-21-2 茅場町タワー

E-mail: {maedasu, babatt, ootanihs, kadom, inadatt}@nttdata.co.jp

あらまし: 近年, Blaster や Sasser のような自己増殖するプログラム“ワーム”による被害が深刻化している. 脆弱性を悪用した感染は, その脆弱性を塞ぐためのパッチやウィルス対策ソフトによって防ぐことができる. しかし, 未知のワームには対応する手段がない. また, 侵入を防ぐためにファイアウォールなどの境界での対策を強化しても, 持込みのノート PC などの端末によって内部感染が拡大してしまうといった事例もある. 本稿では以前に提案した“動的 VLAN 制御”と “ワームの感染プロセスに着目した感染端末検知アルゴリズム”を応用することで, 未知のワームによる被害からセグメント内の全てのクライアント端末を守るシステムを提案する.

キーワード: ワーム, 侵入検知システム(IDS), 侵入防止システム(IPS), 振る舞い, ビヘイビア

A Study on Implementation of the Worm Prevention System Following the Infection Process

Shusuke MAEDA　Tatsuya BABA　Hisamichi OHTANI　Masataka KADO　Tsutomu INADA

Research and Development Headquarters

NTT Data Corporation

Kayaba-Cho Tower, 1-21-2, Shinkawa, Chuo-ku, Tokyo, 104-0033 Japan

E-mail: {maedasu, babatt, ootanihs, kadom, inadatt}@nttdata.co.jp

Abstract: The network incidents caused by Internet worms are increasing every year. Infection of worms that exploit the vulnerabilities can be prevented by applying software patches or installing anti-virus software. However, it is impossible to prevent an infection of worms that exploit unknown-vulnerabilities. Although enhancements of security measures at the network boundaries such as firewalls are effective, such enhancements cannot prevent the internal-infection caused by connecting infected terminals to the intranet. In this paper, we propose a system that prevents infections of unknown-worms and internal infections, applying “the dynamic VLAN control” and “the worm detecting method following the infection process”.

Keyword: Internet Worm, Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Behavior

1. はじめに

近年, ネットワークを通じて広域に拡散する自己増殖プログラム“ワーム”が問題となっている. 特に Blaster や Sasser のように OS の脆弱性を悪用して増殖するネットワーク型ワームは, メールによって感染するものと異なり, 端末が起動していれば人手を介さずに感染することが可能であり, 非常に高速に感染が拡大してしまうという問題がある. 2003 年の Blaster 出現以降, ワーム対策への関心は高まっており, 様々な対策製品・ソリューションが登場している. しかし, 大きく分けて 2 つの課題が残っている.

1 つめは未知のワームへの対策である. 脆弱性・パッチ情報の公開から, 実環境でワームが出現するまでの期間は徐々に短くなってきており, 次々と出現する新種や亜種に対しては, 最も普及している対策方式であるシグネチャマッチングによる検知方式では対応しきれない. また, ワームの特徴をもとに検知を行うことで未知のワームを検知する方法も様々考案されているが誤検知が多く, 強制的な通信の遮断やプログラム削除のトリガに用いるには問題がある.

2 つめは実施形態に関する課題である. ワーム対策の形態は大きく分けてホストベースとネットワークベースの 2 種類に分けられる. ホストベースとは防御対象となる端末に対策ソフトウェアのインストールなどを行う方式であるが, この方式はユーザの端末管理状態に強く依存する. 近年, セキュリティ対策が不完全な持ち込み端末などによる内部からのセキュリティ被害が問題になっているが, ホストベースの対策だけで

はシステム全体のセキュリティを守るには不完全であると言える．他方のネットワークベースの形態では侵入防止システム(IPS = Intrusion Prevention System)などのアプライアンスをネットワークにインラインで設置する．このような装置は未だに高価なため，セグメントの境界部などへの設置が一般的である．しかし，これでは装置を通過しないセグメント内の端末同士の通信は監視できないため，セグメント内感染を防ぐことは難しい．以上のように，ホストベースでもネットワークベースでも実施形態としては不完全だと言える．

著者らは以前に，ワームが感染するために必要とするプロセス(挙動とその順序)に着目することでワーム感染端末を誤検知なく検知するアルゴリズムを提案し，上記の1つめの課題である未知ワーム対策の解決方法を示した．本稿では，ネットワークエッジに設置されているスイッチの機能を利用して感染プロセスの初期の挙動を検知し，“動的 VLAN 制御”[3]によって早期に感染端末を隔離することで，後者の課題である実施形態に関する問題を解決し，システム全体をセキュアに保つ方式を提案する．

2. 従来のワーム対策の問題点

従来のワーム対策の実施形態は大きく分けて端末側で行うホストベースの対策と，ネットワーク側で端末を守るネットワークベースの対策の2つがある．

ホストベースの対策とは，防御すべき端末にアンチウィルスソフトのインストールなどを行うことで端末のセキュリティを確保する方法である．しかし，この方法はユーザの端末管理状態に依存する部分が大きく，当然，未対策の端末をワームの脅威から守ることはできない．セキュリティ分野では一部分の対策不足がシステム全体の問題に波及する可能性があり，実際に持ち込みノート PC からのワーム感染拡大などが問題視されている．以上のように，ホストベースでの対策だけではシステム全体のセキュリティを確保するためには不十分であると言える．

一方のネットワーク側での対策としては，従来から導入が進んでいるファイアウォールや，最近では IPS のような機器のインライン設置が考えられる．このような機器を端末毎に設置することで，ユーザの端末管理常態に依らずセキュリティを確保することができると考えられるが，このような機器は未だ高価であるため，セグメント境界部などに設置することが一般的である．しかし，これでは設置した機器を通過しないセグメント内の端末同士の通信などは監視できないため，セグメント内感染を防ぐことは難しい(図 1).

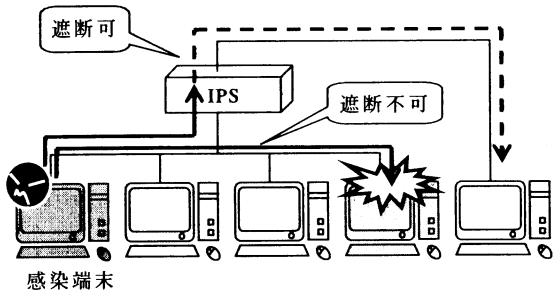

図 1 : IPS では防げない感染経路

以上のような理由から ホストベースでもネットワークベースでも実施形態としては不完全だと言える．

3. 提案システム

本章では，上記の問題点を解決する，システム全体でワーム感染の拡散を防止する現実的なシステムを提案する．具体的には以下の 4 つの条件を満たすことを要件とする．

(要件1) 未知のワームを確実に検知する
(要件2) 正常端末を誤検知しない
(要件3) 端末の状態に依存しない
(要件4) 個々の端末を監視する

3.1. ワーム感染端末検知アルゴリズム

ワームは感染を拡大するために次のような手順を踏まなくてはならない．

(I-1) ポートスキャンを行い，感染対象となる端末を探す．
(I-2) 脆弱性攻撃コードを送信し，感染対象端末を自由に操作するためのバックドアを開く．
(I-3) 感染対象端末のバックドアに対して命令スクリプトを送信する．
(I-4) 攻撃元端末から自己の複製プログラムをダウンロードするように要求させる．
(I-5) 感染対象端末にワームの複製がダウンロードされる．
(I-6) 感染対象端末上で複製プログラムを実行させる．

著者らは文献[2]でワームが感染を行うためには(I-1)～(I-6)が順番通り行われることの必要性を示し，このうち (I-1), (I-4), (I-5)によって発生するトラフィックに着目し，次のようなアルゴリズムを提案した[2].

【アルゴリズム】ワームの感染プロセスに着目した感染端末検知アルゴリズム

Step 1 (ポートスキャン検知)
ある端末 X が ts 秒以内に ns 台以上の端末の同じポートに対してアクセスしたことを検知する.

Step 2 (ダウンロード要求検知)
端末 X がスキャンした端末 Y から X に対して, 新たにセッションが張られたことを検知する. (tq 秒以内に該当する通信が発生しない場合は Step 1 に戻る)

Step 3 (ワームプログラムの転送)
端末 X から端末 Y に対して, TCP(UDP)パケットのデータロード長の合計が sf バイト以上となるようなセッションを検知する. (tf 秒以内に該当する通信が発生しない場合は Step 2 に戻る)

Step 4
端末 X をワーム感染端末として検知する.

※1 ただし, セッションとは一般的な TCP のセッションではなく, UDP も含めた, 特定の IP アドレス・ポートの組の間でやり取りされるパケットの集合を指す.

※2 ns : ポートスキャンと見なすアクセス IP アドレス数
sf : ワームプログラムと見なす最小のデータサイズ
ts : ポートスキャン監視時間
tq : ダウンロード要求監視時間
tf : プログラムダウンロード監視時間

このアルゴリズムでは, ワームの感染活動に不可欠な挙動(ポートスキャンなど)を検知しているため, 未知のワームであっても検知できる. また, 単に挙動を検知するのではなく, 順序という挙動間の関係性を考慮することで, 個々の挙動に対する誤検知が増加しても, アルゴリズム全体の誤検知を削減できる. このアルゴリズムを実装したインライン装置を使用すれば, 未知のワームを検知し, かつ正常端末の誤検知を防ぐことができ, 要件 1, 2 を満たすことができる.

以下では, このアルゴリズムを適用したワーム感染端末検知装置の実装について検討する.

3.2. ワーム感染端末検知装置の実装

ワーム検知装置は前節のアルゴリズムによってワーム感染端末を検知し, その通信を遮断するインライン型の装置とする. 上記の検知アルゴリズムで感染端末の通信を遮断するには, 以下の 6 つのモジュールが必要となる.

- パケットキャプチャ部
- ポートスキャン検知部
- ダウンロード要求検知部
- プログラムダウンロード検知部
- 感染プロセス検知部
- 端末遮断部

以下では, これらの個々のモジュールに必要な機能について論じる.

パケットキャプチャ部
ワーム感染端末検知装置を通過するパケットを収集し, ワームの個々の挙動を検知するためのモジュールであるポートスキャン検知部, ダウンロード要求検知部, プログラムダウンロード検知部に必要な情報を送る.

ポートスキャン検知部
特定のプロトコルによる(セッションの)アクセス先 IP アドレス総数, または ARP リクエストパケットの総数が一定時間(ts 秒)内に既定数(ns 台)以上になった場合, 感染プロセス検知部にスキャン元の IP アドレスを知らせる.

ダウンロード要求検知部
監視対象となっている端末に対するアクセスがあり, 新たな TCP(または UDP)のセッションが張られた場合, 監視対象端末の IP アドレスを感染プロセス検知部に知らせる. さらにそのセッション情報をプログラムダウンロード検知部に送信する. (ただし, ここでいう UDP のセッションとは, 送信元と受信先の IP アドレスとポート番号の組が固定された一連のパケットのやり取りを指す).

プログラムダウンロード検知部
ダウンロード要求検知部から受け取ったセッションにおいて, 監視対象から送信されるパケットの TCP (UDP)の総ペイロード長が既定サイズ (sf バイト)以上となった場合, その送信元の IP アドレスを感染プロセス検知部に知らせる. ただし, セッションが終了した段階でワームプログラムのダウンロードは完了しており, 感染も完了してしまっているため, 感染プロセス検知部への通知は, セッションが終了する前, つまりペイロード長合計が既定サイズを超えた段階で行われなくてはならない.

感染プロセス検知部
ポートスキャン検知部, ダウンロード要求検知部, プログラムダウンロード検知部から取得した IP アドレス情報と取得時の時刻情報から, 感染プロセス検知アルゴリズムで用いてワーム感染端末かどうかを判断する. 感染端末と判断した場合には,

端末遮断部にその IP アドレスを送信する.

端末遮断部

感染プロセス検知部から受け取った IP アドレスの通信を遮断するようにファイアウォールを設定する.

ただし, ダウンロード要求と実際のプログラムダウンロードは同じセッションで行われる可能性がある. そのため, ダウンロード要求検知部とプログラムダウンロード検知部の間で情報のやり取りにタイムラグが生じた場合は, 感染行動が終了してしまいワームが拡散してしまいかねない. そのため, 実際にはダウンロード要求検知とプログラムダウンロード検知は同じモジュールで処理することが望ましいと考えられる(図 2).

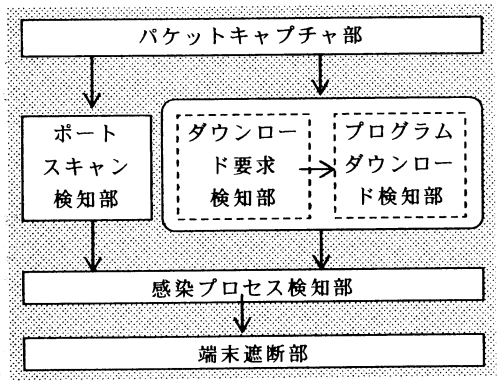

図 2: ワーム感染端末検知装置のモジュール

このワーム感染端末検知装置では通信を UDP も含めたセッションという単位で認識するため, セッションを TCP ヘッダのフラグのみで判断できず, パケットが到着するたびに通信記録の照合と更新を行う必要がある. 正常な通信を妨げないためには, 高い処理能力が必要とされる.

3.3. 動的 VLAN 制御を用いた通信の誘導

図 3では端末毎に個別の VLAN が割り当てられているので直接端末間で通信を行うことはできなが, ブリッジを異なる VLAN 間を接続するよう動作させることで, 端末同士はブリッジを経由しての通信が可能となる. このブリッジの部分にワーム感染端末検知装置を設置することで, ワーム感染端末検知装置は全ての端末の通信を監視することができる.

しかし, 3.2節で述べたようにワーム感染端末検知装置には高負荷がかかることが予想されるため, できるだけワームと関係ない通信は経由させないようにしたい. そこで動的 VLAN 制御を利用して, ワーム感染の兆候がみられる端末のみ, ワーム感染端末検知装置を接続する仕組みを検討する.

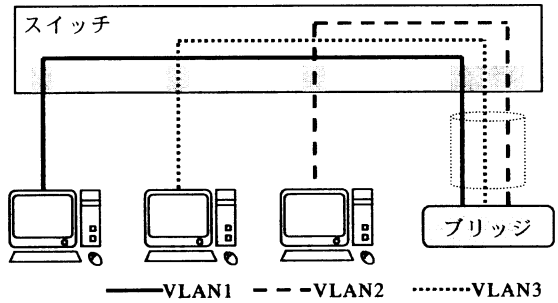

図 3: VLAN を利用した通信の誘導

文献[3]では VLAN を動的に制御することで, セキュリティ対策が不十分な端末の通信のみをファイアウォール経由に設定する方式を提案している. 本稿ではこの方式を応用して, ワームに感染している疑いのある端末のみを, 通常の VLAN からワーム感染端末を監視するための VLAN に切り替える (以下, 前者を通常 VLAN, 後者を監視 VLAN と呼ぶことにする). 感染の疑いがある端末を, 早期に通常 VLAN とは異なる VLAN に隔離することで, ワーム感染端末検知装置への負荷を軽減しつつ, セグメント内感染も含めたワームの拡散を防止できる. セグメント内に設置する機器は次のようなものを想定する.

- VLAN 対応レイヤ 2 スイッチ
- VLAN 制御装置
- ワーム感染端末検知装置 (異なる VLAN 間を接続するブリッジとして動作)
- ユーザ端末
- ルータ

図 4にシステム構成の例を示す. 初期状態での VLAN の割り当てを表 1のように設定すると, 通常状態ではユーザ端末の通信はワーム感染端末検知装置を介さずに行われる. もし, セグメント内でワーム感染の兆候が見られる端末が現れた場合, システムは次のシナリオように動作し, 監視対象となる端末とセグメント外も含めた他の端末との通信を全て監視できるようになる.

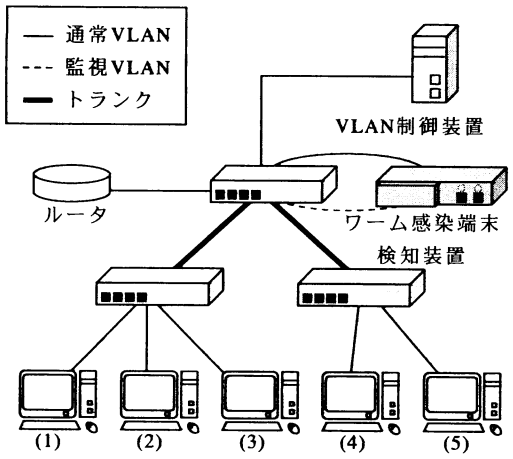

図 4: システム構成例

表 1: 初期状態の VLAN 割当て状況

設定個所	割当て VLAN
UT－SW	通常
WDA－SW(1)	通常
WDA－SW(2)	監視
VLC－SW	通常
SW－SW	通常+監視(トランク)

※ UT=ユーザ端末, SW=スイッチ,
WDA=ワーム感染端末検知装置,
VLC=VLAN 制御装置

シナリオ 1

まず, VLAN 制御装置は感染兆候が見られた端末(以下, UT_w とする)と UT_w が直接繋がっているスイッチポートとの接続を通常 VLAN から監視 VLAN に切り替える. これによって UT_w は他の正常端末と隔離され, 通信ができなくなる.

シナリオ 2

UT_w の通信は各スイッチの監視 VLAN がトランクされているスイッチポートを経由して, ワーム感染端末検知装置(以下, WDA とする)に誘導される(図 5 は端末 5 にワーム感染の兆候が見られた場合の例で, 斜線部が隔離されたネットワークとなっている).

シナリオ 3

WDA によって監視 VLAN と通常 VLAN はブリッジ接続されているので, UT_w の通信は WDA 経由で通常 VLAN と接続される. したがって, WDA は UT_w と他の端末との通信を全て監視できるようになる.

ただし, 複数の端末にワーム感染の兆候が見られる場合に, 各端末を同じ監視 VLAN に切り替えてしまうと, ワーム感染端末検知装置を経由せずに端末間での通信が行えてしまう. これを防ぐためには, 端末毎に異なる監視 VLAN を予約しておき, スイッチ間, 及びスイッチとワーム感染端末検知装置間には全ての予約された VLAN をトランクしておけばよい. すると, 監視 VLAN に隔離されている端末同士でも, VLAN が異なるため, ワーム感染端末検知装置のブリッジを経由しなければ, 通信できなくなる.

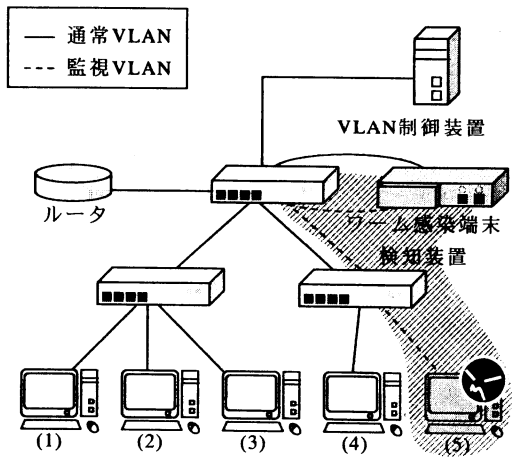

図 5: 感染端末の VLAN による隔離例

以上のような仕組みを導入することで, 端末毎にワーム感染端末検知装置が設置された状態を仮想的につくり出すことができる. これにより, 個々の端末毎に, そのセキュリティ状態に依らずにネットワーク側でワーム感染の有無を判別することができ, 要件 3, 4 を満たすことができる.

3.4. SNMP によるワーム感染兆候の検知

3.3節では VLAN を利用してワーム感染の兆候が見られる端末を隔離する方法を示したが, 何をもって感染兆候とするかは示さなかった. 本節ではその方法について検討する.

動的 VLAN 制御で端末を隔離するためには, 感染兆候のある端末が, どのスイッチのどのポートに接続されているかを知る必要がある. そのためには, スイッチ自身が感染兆候を検知し, VLAN 制御装置に監視 VLAN への切り替えを指示できることが望ましい.

本提案システムは, スイッチに備わっている SNMP (Simple Network Management Protocol)機能を利用することによってこれを実現する. SNMP は管理する側の機器(マネージャ)が, 管理される側の機器(エージェン

ト)の情報を取得するためのプロトコルである．SNMPではMIB (Management Information Base)と呼ばれるデータ構造が利用される．MIBには一意な値が割り振られ，これをOID (Object ID)という．

文献[4]ではtcpActiveOpens (OID: 1.3.6.1.2.1.6.5)のMIB情報などを利用して，TCPのSYN送信回数の増加を監視することでワームの発生を検知する方式を提案している．しかし，これはルータや端末そのもののMIB情報を監視する方式である．ルータでの監視では，セグメント内で閉じた通信を監視することができない．また，Windowsクライアントには SNMP機能はデフォルトではインストールされていないので，端末のユーザ管理状態に依存してしまい，提案システムの要件に反してしまう．また，TCPはレイヤ4のプロトコルであり，レイヤ2スイッチでは詳細情報を取得できない．レイヤ2(データリンク層)で扱えるEthernetパケットレベルの情報でワームの感染兆候を検知する方法を考える．

ワームは拡散するためにポートスキャン，ダウンロード要求の取得，プログラムの転送を順番に行う．この中で，ポートスキャンは感染行動のもっとも始めに行われる．つまり，ポートスキャンをしている端末はワームに感染している疑いがあると言える．ポートスキャンの際には端末から大量のパケットが送信される．

SNMPの拡張機能であるRMONv1 (RMON = Remote Monitoring)を利用すると機器のポート毎にレイヤ2の統計情報を用いてしてトラップを上げることができる．SNMPエージェントであるレイヤ2スイッチは，スイッチポートに入ってくるパケット数を表すMIB(表2)のどちらかが既定値以上になった場合に，SNMPマネージャであるVLAN制御装置にトラップを上げるよう設定する．トラップを受信したVLAN制御装置は，対象のスイッチポートを監視VLANに切り替え，対象端末の通信がワーム感染端末検知装置を通過するようにする．

表 2: ユーザ端末の出力に関するMIB (一部)

MIB名 (OID)	説明
ifInUcastPkts (1.3.6.1.2.1.2.2.1.11)	受信したユニキャストの総パケット数
ifInNUcastPkts (1.3.6.1.2.1.2.2.1.12)	受信した非ユニキャストの総パケット数

ワーム特有の通信エラーのパターン[5]や，入出力の相関関係を監視することでワーム感染の兆候を検出することも可能であるが，これらはスイッチからのトラップを受信してからSNMPリクエストで情報を取得するなどのいくつかの手順を踏まなければならず，迅速性に欠ける．本提案システムにおいては，感染拡大を防ぐために可能な限り早期に監視VLANへの切り替えを行う必要があるので，スイッチが自身の持っている機能だけで直接VLANの切り替えを要求できる，パケット数の増加のみに着目する方式を採用する．

図 6に本提案システム全体の処理フローを示す．

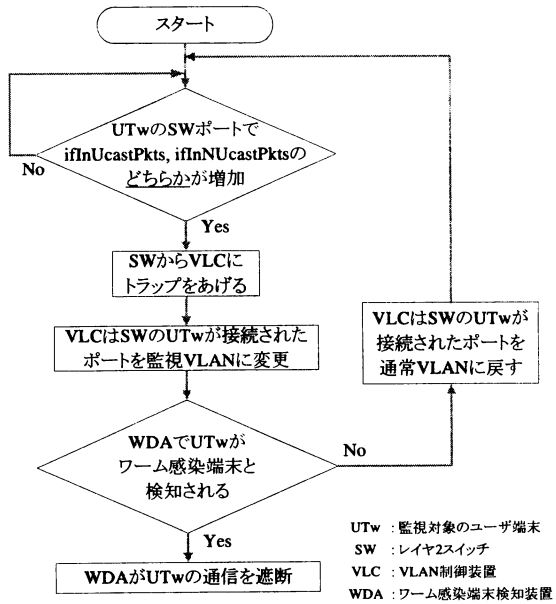

図 6: 提案システムの処理フロー

4. 検証実験

ワーム感染端末検知に使用するアルゴリズムの有効性は文献[2]で示したので，今回はSNMPを用いて感染兆候のある端末を検知する方式（3.4節の部分．図6の1つめの分岐）について，その有効性を検証する．

4.1. 検証内容

通常オフィス端末とワーム感染端末の2種類を，それぞれレイヤ2スイッチに接続し，スイッチから得られるMIB情報の変化を比較する．取得するMIB情報は端末の送信パケット数に関するMIB(表2)である．

本検証はSNMPを利用したワーム感染兆候の検知が有効かどうかを調べることが目的である．通常オフィス端末ではあまり見られないが，ワーム感染端末からは常に観測できるような現象が現れれば，提案方式が有効であると言える．

4.2. 検証条件

監視対象となる端末をレイヤ2スイッチに接続する．

スイッチにはSNMPマネージャも接続し，20秒毎にスイッチに対してSNMPリクエストを行い，端末が接続されたスイッチポートのMIB情報の変化を調査した．実験条件を以下に示す．

共通条件

監視対象端末：Windows端末(Windows XP)
SNMPエージェント：Cisco Catalyst 2950
SNMPマネージャ：Linux端末(Fedora Core 3)
MIB：ifInUcastPkts (ユニキャストパケット数)
ifInNUcastPkts(非ユニキャストパケット数)
MIB取得間隔：20秒

通常オフィス端末用 実験環境

レイヤ2スイッチに通常オフィス端末とSNMPマネージャを接続し，アップリンクポートを社内ネットワークに接続する(図 7)．

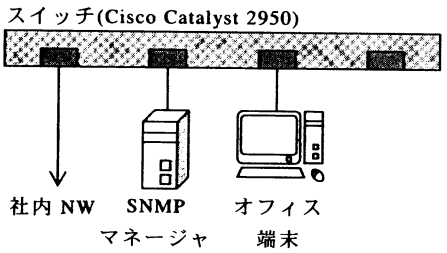

図 7: 検証実験環境 (オフィス端末用)

ワーム感染端末用 実験環境

レイヤ2スイッチにワーム感染端末とSNMPマネージャを接続し，アップリンクポートには外部ネットワークに接続されていないルータをゲートウェイとして設置する(図 8)．ワームはSasser.C, Sasser.A, Blaster.Cを使用した．また，実験環境のローカルネットワークは192.168.0.0 / 28とした．

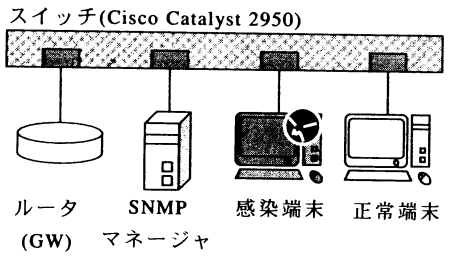

図 8: 検証実験環境 (ワーム感染端末用)

4.3. 実験結果

オフィス環境とワーム発症環境について，ifInUcastPkts (端末が送信するユニキャストパケット数)の値の変化を比較した結果を図 9に示す．

通常のオフィストラフィックでは，Webサーフィン，メール送受信などを行う際に多量のパケットが送信されるが，それ以外の定常状態ではほとんどユニキャストパケットは送信されないことが分かった．それに対して，ワーム発症時は倍以上のユニキャストパケットが送信されている．

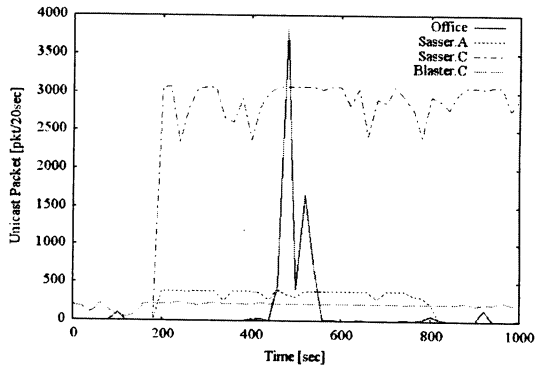

図 9: 端末が送信したユニキャストパケット数の比較

また，ifInNUcastPkts (端末が送信する非ユニキャストパケット数)については，オフィス環境ではほとんど送信されず(多くて20秒に2パケット)であり，ワームの発症時に発生する非ユニキャストパケット数(図10)に比べてかなり少なく，違いは明らかだった．

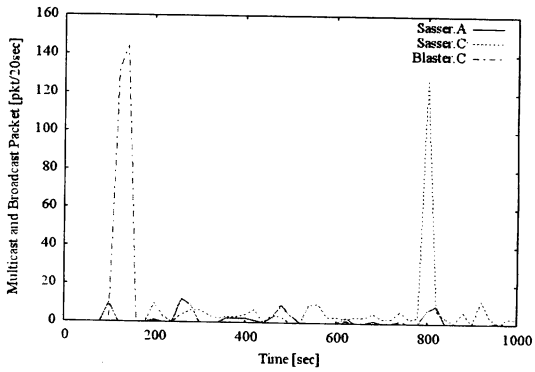

図 10:攻撃時に送信される非ユニキャストパケット数

4.4. 考察

以上のように，ユニキャスト，非ユニキャストの両

方のパケットがワーム感染時には通常のオフィス環境よりも明らかに増加することがわかり，これらがワーム感染兆候の検知に有効な指標であることが分かった．正常な通信を誤検知する可能性はあるが，ワーム感染端末検知装置による検知までを含んだシステム全体による誤検知を増加させるものではないと考えられる．

ただし，セグメント内への攻撃とセグメント外への攻撃ではトラフィックのパターンが異なるので，その違いによって問題が生ずるかどうかを検討しなくてはならない．ローカル以外のIPアドレスへのアクセスは，ゲートウェイ経由で直接ターゲットの IP アドレスに送信される．それに対して，ローカルのIPアドレスへのアクセスの場合，MAC アドレス解決のためにまずARPリクエストをブロードキャストで送信し，ARPリプライが返ってきた場合に，その MAC アドレスに対して改めてポートスキャン用のパケットが送信される．そのため，ローカルの端末を対象にしたポートスキャンが行われた場合にはifNUcastPktsの値が増加すると考えられる．

しかし，ARPリクエストはアドレスが解決できない場合，数回送信される．Windows XPの場合，デフォルトで4回までARPリクエストが送信されるため，サブネット長が 24bit，端末が存在する IP アドレス数を n とすると，パケット数 p は

$$p = n + 4\,(2^{32-24} - n) = 1024 - 3n$$

となり，存在するローカル端末のIPアドレスが増加するほど，非ユニキャストパケット数が減少することがわかる．逆に，端末に割り当てられたIPアドレス数が増加するほど，解決された MAC アドレスの端末にポートスキャン用のパケットが送信され，ユニキャストパケット数は増加すると考えられる．

以上のことを検証するため，ワーム感染端末用の検証環境でポートスキャンツール nmap を使用しローカルネットワーク内のIPアドレスに対してTCP 445番ポートへの接続スキャンを行った．割り振られているIPアドレスの数が増えるほど，ユニキャストパケットは増加し，非ユニキャストパケットが減少するという，仮説どおりの結果を得ることができた(図 11)．

このように，ローカル端末に割り振られたIPアドレスの増減があっても，ifInUcastPktsとifInNUcastPktsのどちらかは確実に増加するために，どちらかの基準の超過によるトラップがあがり，対象端末を監視 VLAN に移動することが可能であると考えられる．

以上より，ネットワークエンドのスイッチに対するSNMP, RMONv1によるパケット量増加の監視が，ワームの感染活動検知に有効であることが示せた．

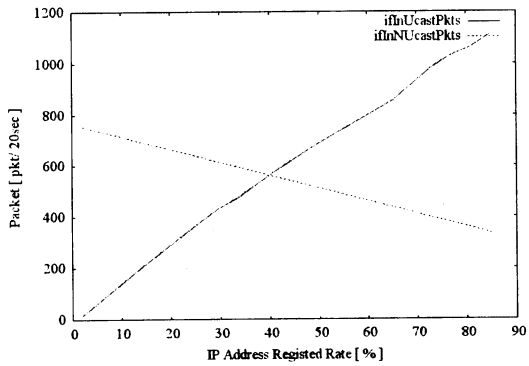

図 11: ローカル端末数に依るパケット数の変化

5. むすびに

本稿ではワームの感染プロセスに着目した感染端末検知アルゴリズムをシステムとして実現する方法について検討し，動的VLAN制御とSNMP RMONv1を用いることでセグメント外への感染に加えて，効率的にセグメント内感染も防ぐ方式を提案した．

今後は提案システムについてプロトタイプを実装し，その実効性や閾値による性能の変化について評価を行う．また，評価結果をフィードバックし，実際にイントラネットに導入可能なワーム感染防止システムの構築について検討していく．

参考文献

[1] 情報処理推進機構,“コンピュータウィルス・不正アクセスの届出状況（5月分）について(別紙1),” http://www.ipa.go.jp/security/txt/2005/documents/virus-full0506.pdf, Jun. 2005.

[2] 前田，馬場，大谷，角，稲田，“感染プロセスに着目したワーム検知方式の提案,” 情処研報，CSEC-28, Vol.2005, No.33, pp.327－332, Mar. 2005.

[3] 角，馬場，稲田，“動的VLAN制御によるホスト保護方式の提案,” CSS2004論文集，Vol.1, pp.49－54, Oct. 2004.

[4] 東角，鳥居，“SNMPによるワーム検知方式の検討,” CSS2004 論文集，Vol.1, pp.115－120, Oct. 2004.

[5] Berk, Bakos, Morris, “Designing a Framework for Active Worm Detection on Global Networks,” Proc. of IEEE Int. Work. On Information Assurance, Darmstadt, Germany, Mar. 2003.