社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2005－DPS－122（8）
2005－CSEC－28（8）
2005／3／22

動的 VLAN 制御による統合ワーム対策システムの提案

馬場 達也　　角 将高　　稲田 勉

株式会社 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:　{babatt, kadom, inadatt}@nttdata.co.jp

あらまし　近年、Blaster や Sasser、Netsky などの、ワームの被害が大きな問題となっている。これらのワームの被害を防ぐ技術の一つに、PC をイントラネットに接続する際に、ウイルス対策ソフトの動作状況やパッチの適用状況をチェックする「検疫システム」がある。しかし、クライアント PC に、対応しているウイルス対策ソフトをインストールしておかなければならないという問題や、パッチを適用すると動作しないアプリケーションが存在するという問題がある。本稿では、クライアント PC の状態に依らずに、検疫、駆除、防御、検知、隔離などのワーム対策機能をネットワーク側で統合して提供するプラットフォームを提案する。

キーワード　ワーム、検疫ネットワーク、ワーム検知、VLAN

A Proposal of an Integrated Worm Countermeasure System Based on Dynamic VLAN Control

Tatsuya BABA, Masataka KADO, and Tsutomu INADA

Research and Development Headquarters, NTT Data Corporation

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

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

Abstract　Recently, infection of Internet worms such as “Blaster”, “Sasser”, and “Netsky” are becoming a serious problem. To prevent damage from these worms, there are "quarantine systems" that check the installed anti-virus software and the applied security patches on the client PCs when they are connected to the enterprise network. They have some problems, however, such that it is necessary to install certain anti-virus software supported by the quarantine system, and some application programs do not work after certain patch is applied. In this paper, we propose an integrated worm countermeasure system which has functionalities such as quarantine, worm extermination, protection, infection detection, and isolation on network side without depending on client software.

Keyword　Internet Worms, Quarantine System, Worm Detection, VLAN

1. はじめに

近年、システムに感染するワームの被害が増加してきている[1]。ワームは、システムの脆弱性を悪用して自動的に侵入することにより、感染を広めようとする「脆弱性悪用型ネットワークワーム」と、ワームプログラムを添付したメールを送信して感染を広める「マスメーリングワーム」の 2 種類に大別される。脆弱性悪用型ネットワークワームの例としては、2003 年に発生した Blaster や Welchia、2004 年に発生した Sasser などがある。また、マスメーリングワームの例としては、Sobig、Netsky、Beagle、Mydoom などがある。

これらのワームによる被害を防ぐためには、企業のイントラネットにワームが侵入することを防ぐことが重要である。イントラネットへのワームの侵入経路は、図 1 に示すものがあると考えられる。

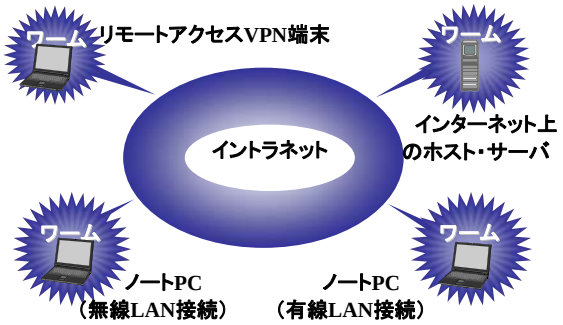

図 1 イントラネットへのワームの侵入経路

インターネットから侵入する脆弱性悪用型ネットワークワームに対しては、インターネットとイントラネットの境界にファイアウォールや IPS（Intrusion Prevention System：侵入防止システム）を導入することで防ぐことができる。また、インターネット経由で侵入するマスメーリングワームに対しては、イントラネット上のメールサーバにゲートウェイ型アンチウイルスソフトを導入することが効果的である。しかし、最近は、外部でワームに感染したノート PC などを、有線 LAN や無線 LAN、リモートアクセス VPN 経由などでイントラネットに接続することによって感染が広まる、「持ち込み PC」からの感染が問題となっている。

現在、この持ち込み PC からの感染を防ぐ技術として、「検疫システム」が注目されている。検疫システムは、イントラネットに接続される PC をチェックし、ワームに感染していないことを確認してから接続を許可するものである。また、同時に接続 PC の脆弱性をチェックすることにより、ワームがイントラネットに侵入した場合でも、被害が拡大しないように対策を行うこともできる。

現在の多くの検疫システムでは、接続 PC 上で、ウイルス対策ソフトが最新のウイルス定義ファイルを使用して適切に動作しているかどうかということや、接続 PC に最新のパッチが適用されているかどうかということをチェックする。そして、これらのチェックの結果、不十分であると判断した場合には、接続を許可させないというアプローチをとっている。これにより、イントラネットに接続する PC のウイルス対策ソフトのウイルス定義ファイルのアップデートやパッチの適用を徹底させることができ、ワームの被害の拡大を防ぐことができる。しかし、この方式では、クライアント PC に、検疫システム側で対応しているウイルス対策ソフトをインストールしておかなければイントラネットに接続できないという問題がある。例えば、お客様などが持ち込んだ PC を、一時的にイントラネットへ接続させたいような場合が考えられるが、使用しているウイルス対策ソフトが検疫システム側で対応していない場合には接続できないという問題がある。また、パッチを適用すると、動作しなくなるアプリケーションが存在するという問題もある。このようなアプリケーションを使用している PC には、該当するパッチを適用することができないため、イントラネットへの接続が許可されない。

さらに、市販の IPS 製品をセグメント境界に設置し、脆弱性を狙った攻撃を遮断することによってワーム感染を防ぐという方法も考えられる。しかし、ワームは、同一セグメント内を狙う場合が多く、このような場合は、セグメント境界に設置した IPS をワームの感染トラフィックが通過しないため、検知することができないという問題がある。

2. 提案方式

著者らは、これまでに、接続 PC にパッチが適用されていない場合には、VLAN（Virtual LAN）設定を動的に制御することにより、ネットワーク側で脆弱性を保護する方式を提案してきた[2]。具体的には、レイヤ 2 スイッチの VLAN の設定を変更し、ネットワーク側に設置したブリッジファイアウォールを経由してアクセスさせることによって、接続 PC の脆弱性のあるポートに対するアクセスを遮断し、ワームの感染から防御する。これにより、パッチを適用できない PC でも、ワームの感染から保護することができ、安全にイントラネットに接続することが可能となる。

今回は、さらに、クライアント PC に特定のウイルス対策ソフトが導入されていない場合でも、ワーム感染をチェックする機能や、万が一、イントラネットにワームが侵入してしまった場合に備えて、未知のものも含めてワームの感染活動を検知し、攻撃を遮断する機能について検討した。以下に、著者らの提案するネットワーク側での防御方式について述べる。

2.1. 処理概要

本システムは、図 2 のように、「ワーム検疫・駆除」「ワーム感染防御」「ワーム検知・隔離」などの機能から構成され、ワーム感染フェーズごとに適切な対策をネットワーク側で統合的に提供することによって、多段防御を実現する。

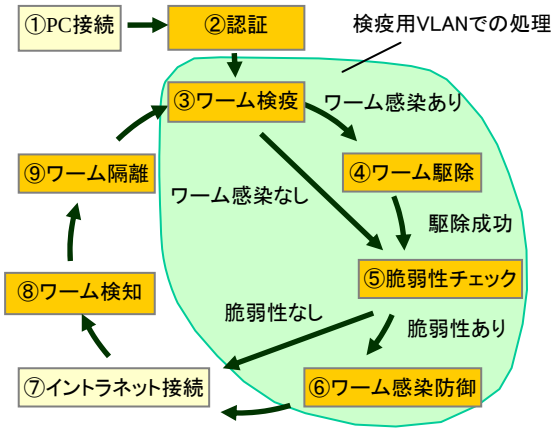

図 2 統合ワーム対策システムの対処サイクル

PC をネットワークに接続すると、ユーザ認証またはデバイス認証が行われる（図 2-①、②）。認証に成功すると、通常の業務ネットワークとは隔離された検疫ネットワークに接続される。そして、検疫ネットワークに設置されている検疫サーバより、ワーム感染チェックを受ける（図 2-③）。ワーム感染チェックの結果、ワームに感染していると判断された場合には、ワームが駆除される（図 2-④）。

さらに、参考文献[2]で報告したように、接続 PC の脆弱性がチェックされる（図 2-⑤）。脆弱性が存在すると判断された場合には、ネットワーク側で脆弱性を保護しながら、業務ネットワークに接続させることで、業務ネットワークにワームが侵入してしまった場合でも、感染の被害にあわないようにする（図 2-⑥、⑦）。脆弱性が存在しないと判断された場合には、ワームの攻撃を受けても感染しないため、直接業務ネットワークに接続させる。

そして、業務ネットワークにワームが侵入した場合に備えて、ネットワークトラフィックを監視して、未知のものも含めてワームを検知するワームセンサを設置する。ワームセンサがワームを検知すると、感染端末からのワーム感染トラフィックを遮断し、業務ネットワークからワームを隔離する（図 2-⑧、⑨）。

2.2. システム構成

図 3 に提案する方式を実現するためのシステム構成を示す。本システムでは、業務ネットワークを構成する業務用 VLAN と、検疫ネットワークを構成する検疫用 VLAN を用意し、レイヤ 2 レベルで通信を制限している。検疫用 VLAN には、接続 PC のチェックや、VLAN およびフィルタリングの設定を動的に制御する検疫サーバと、PC 接続時の認証を行う RADIUS サーバを設置する。また、VLAN 対応レイヤ 2 スイッチのポートの一つを、上位ルータへのアップリンクポートをミラーする設定にし、ワームセンサを接続する。さらに、ブリッジファイアウォールを VLAN 対応レイヤ 2 スイッチに VLAN トランクで接続する。

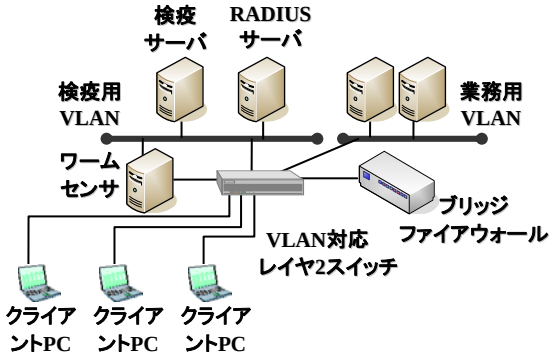

図 3 システム構成

接続 PC を業務用 VLAN に直接接続する場合は、その PC が接続されているポートに対して業務用 VLAN と同じ VLAN ID を割り当てる。PC を業務用 VLAN にブリッジファイアウォールを経由して接続させる場合には、その PC が接続されているポートに対して、ポート毎に異なるユニークな VLAN ID を割り当てる。ブリッジファイアウォールは、異なる VLAN 間をブリッジ接続する機能を備えているため、この場合は、必ずブリッジファイアウォール経由でアクセスされることとなる。

3. 処理詳細

3.1. 認証処理（接続検知処理）

レイヤ 2 スイッチへの PC の接続を検知するために、IEEE 802.1X 認証[3]を利用した。具体的には、検疫サーバに RADIUS プロキシ機能を持たせ、IEEE 802.1X 認証で用いられる RADIUS 認証を、検疫サーバを経由して行うようにした。これにより、検疫サーバは、RADIUS リクエストメッセージから、接続 PC の MAC アドレス、接続先スイッチの IP アドレス、接続スイッチポートの情報を取得することができるようになる。そして、RADIUS 認証中に該当 PC が検疫用 VLAN とのみ通信が可能となるように、ブリッジファイアウォールのフィルタリング設定を行う。検疫サーバは、このフィルタリング設定が完了するまでは、RADIUS サーバからの認証完了メッセージをレイヤ 2 スイッチへ転送しないように制御する。

3.2. ワーム検疫・駆除処理

認証完了後、ユーザは、検疫サーバに対して Internet Explorer を使用してアクセスする。そして、チェック用 ActiveX コントロールをダウンロードして、ワーム感染チェックを行う。

通常、クライアント PC を狙うワームは、OS を再起動した場合に、ワームプログラムが自動的に起動されるように設定する。本システムでは、このワームの性質を利用し、接続 PC の OS の自動起動設定の内容を、あらかじめ定義された、ワームの自動起動設定の内容と比較することで、ワーム感染の有無を判定する。具体的には、接続 PC のレジストリの Run/RunOnce エントリおよびスタートアップフォルダの内容を検疫サーバに送信し、検疫サーバに保管してあるワーム定義ファイルの内容と比較する。もし、ワームに感染していると判断された場合には、自動的に駆除用 ActiveX コントロールをダウンロードさせ、該当ワームプロセスを停止し、該当ワームプログラムを削除する。そして、該当するレジストリエントリを削除する。

3.3. 脆弱性チェック処理

ワーム感染チェックが完了すると、脆弱性チェックを行う。具体的には、チェック用 ActiveX コントロールが、レジストリに記述されているパッチのリストを検疫サーバに送信し、検疫サーバに保管してある最新のパッチリストと比較する。もし、適用されていないパッチが存在した場合には、ワーム感染防御機能によって、該当 PC の脆弱ポートへのアクセスをフィルタリングすることで、ワーム感染から防御する。

3.4. ワーム感染防御処理

脆弱性のある PC をブリッジファイアウォール経由で接続させるために、検疫サーバは、該当 PC が接続されているスイッチポートに対してユニークな VLAN ID を割り当てるように、レイヤ 2 スイッチに SNMP を用いて指示する。脆弱ポートが存在しない PC が接続されているスイッチポートには、業務用 VLAN と同じ VLAN ID を設定し、ブリッジファイアウォールを経由せずに業務用 VLAN に接続させる。

また、接続 PC に脆弱ポートが存在した場合には、該当 PC の脆弱ポートへのアクセスをフィルタリングするようにブリッジファイアウォールの設定を行う。脆弱ポートが存在しなければフィルタリングの設定は行わない。

フィルタリングは、MAC アドレスをベースとして行うこととした。MAC アドレスは詐称することが可能であるが、IEEE 802.1X 認証時に接続スイッチポートと MAC アドレスを関連付けるため、通信可能な MAC アドレスを制限することができる。このため、MAC アドレスを詐称した場合には、通信を行うこと自体が不可能となり、結果として、MAC アドレスの詐称を防ぐことができる。

3.5. ワーム検知・隔離処理

イントラネット内にワームが侵入したことを検知するために、ネットワークトラフィックを監視して、ワーム感染行為の発生を検知するためのワームセンサを設置する。

ワームセンサでは、未知のワームも含めて検知するために、脆弱性悪用型ネットワークワームが感染先を探すために行う水平ポートスキャンと、マスメーリングワームが送信先メールサーバを探すために行う DNS への MX レコードの問い合わせを監視する。

ワームセンサは、アップリンクポートに流れるトラフィックをキャプチャして、他セグメントへのワーム感染行為を監視する。さらに、DHCP で割り当てていない未使用の IP アドレスに対するアクセスを、ARP リプライを偽造することでワームセンサに誘導し、同一セグメント内のワーム感染活動も監視できるようにする。ワーム感染活動を検知した場合には、その発信元 PC からの感染ポート（MX レコード問い合わせを検知した場合は、メールの送信を遮断するため 25/TCP）をブリッジファイアウォールで遮断するように設定する。

4. プロトタイプの実装

本方式の有効性を検証するため、提案方式を実装したプロトタイプを作成した。

(1) ブリッジファイアウォール

VLAN 間ブリッジングは、Linux カーネルの標準機能を用いて実現した。また、フィルタリングには、MAC アドレスベースのフィルタリングが可能な ebtables[4]を使用した。さらに、検疫サーバからの指示を受信して、フィルタリング設定を行うためのプロセスを実装した。

(2) 検疫サーバ

FreeRADIUS[5]を改造し、レイヤ 2 スイッチと RADIUS サーバとの間で RADIUS プロキシとして動作するようにした。さらに、SNMP を使用して、標準の Q-Bridge MIB[6]をサポートするスイッチと、Cisco Catalyst などの独自の

Enterprise MIB を用いるスイッチの VLAN 設定を動的に制御するプロセスを実装した。

(3) ワームセンサ

ISC DHCP[7]を改造し、DHCP で割り当てていない IP アドレスに対して ARP 要求が発生した場合に、ワームセンサの MAC アドレスを返答するようにした。そして、キャプチャされるパケットを監視してワームの検知を行うプロセスを実装した。

5. 動作検証

プロトタイプを使用して、ワームへの対処機能及び処理性能に関する検証を実施した。

5.1. 検証環境

検証用ネットワークの構成は、図 3 と同様である。検疫サーバ、RADIUS サーバ、ブリッジファイアウォールは、すべて表 1 のスペックの PC 上で動作させた。なお、レイヤ 2 スイッチには、Cisco Catalyst 2950T-24 を使用した。

検疫サーバには、ワーム感染チェック用に、1500 種類のワーム（亜種を含む）の情報と、2005 年 2 月 1 日時点で公開されている Windows 2000 および Windows XP のパッチおよび対応する脆弱ポートの情報を登録しておいた。

クライアントの OS は Windows XP を使用し、2002 年 4 月 10 日までのパッチのみを適用した「パッチ未適用 PC」と、2005 年 2 月 1 日時点での最新のパッチを適用した「パッチ適用済 PC」の 2 種類を用意した。クライアントでは、IEEE 802.1X サプリカントとして Funk Software 社の Odyssey Client を使用し、認証方式として EAP / MD5-Challenge を選択した。なお、クライアントの Run/RunOnce エントリおよびスタートアップフォルダには、計 12 のエントリが既に記述されていた。

ワームセンサでは、5 秒以内に同じ PC から 30 以上の宛先に水平ポートスキャンを行った場合に、脆弱性悪用型ネットワークワームに感染しているとして検知するように設定した。また、DNS に対して、5 秒以内に同じ PC から 3 ドメイン以上の MX レコードを問い合わせた場合に、マスメーリングワームに感染しているとして検知するように設定した。

表 1　プロトタイプ実装環境

OS	Linux（Fedora Core 3）
CPU	Pentium 4 3GHz
メモリ	1GB DDR-SDRAM
ネットワークカード	Intel Pro/1000MT

5.2. 検証方法

脆弱性悪用型ネットワークワームである、Blaster.C、Sasser.C、マスメーリングワームである、Sobig.F、Beagle.X、Netsky.Z のそれぞれを PC に感染させ、本システムの各処理で適切に対処できるかどうかを確認した。

また、Blaster.C に感染したパッチ未適用 PC およびワームに感染していないパッチ適用済 PC を接続した場合の処理時間を測定した。そして、接続した PC を Blaster.C に感染させた場合に、ワームセンサが検知してから、実際にワームトラフィックが遮断されるまでの時間についても測定した。処理時間は 10 回ずつ測定し、その平均を求めた。なお、チェック用および駆除用 ActiveX コントロールは、既にダウンロードが完了している状態で測定を行った。

5.3. 検証結果

5.3.1. ワームへの対処機能

本システムの各処理におけるワームへの対処結果は、表 2 のようになった。今回の検証に使用したワームは、ワーム定義ファイルに登録してあるものであったため、すべてワーム感染チェックにて検知され、駆除された。また、Blaster.C が悪用する脆弱性を修正するパッチ（MS03-026）や Sasser.C が悪用する脆弱性を修正するパッチ（MS04-011）などが適用されていないパッチ未適用 PC では、これらのワームが感染に使用するポートである 135/TCP および 445/TCP を含め、8 つの脆弱ポートが発見された。そして、該当 PC のこれらの脆弱ポートへのアクセスが、ブリッジファイアウォールで遮断するように設定された。

さらに、接続した PC を Blaster.C および Sasser.C に感染させた場合に、ワームセンサによって水平ポートスキャンが検知され、ワーム感染に使用されるポートが遮断されるように設定された。また、Sobig.F、Beagle.X、Netsky.Z に感染させた場合には、ワームセンサによって、DNS に対する MX レコードの問い合わせが検知され、メールが外部に送信されないように、25/TCP が遮断されるように設定された。

表 2 各処理における対処結果

	検疫	駆除	防御	検知	隔離
Blaster.C	○	○	○	○	135/TCP
Sasser.C	○	○	○	○	445/TCP
Sobig.F	○	○		○	25/TCP
Beagle.X	○	○		○	25/TCP
Netsky.Z	○	○		○	25/TCP

5.3.2. 処理性能

Blaster.C に感染したパッチ未適用 PC およびワームに感染していないパッチ適用済 PC を接続してからの処理時間は、それぞれ表 3 のとおりであった。また、ワームセンサで Blaster.C の感染活動を検知した後に、ワームトラフィックが遮断されるまでの時間は、0.18 秒であった。

表 3 接続からの各処理の平均時間

処理	パッチ未適用/ワーム感染有	パッチ適用済/ワーム感染無
接続認証/検疫用 VLAN 接続処理	0.33 秒	0.28 秒
感染チェック	0.96 秒	0.55 秒
ワーム駆除処理	0.88 秒	
脆弱性チェック	0.46 秒	0.37 秒
業務用 VLAN 接続処理	0.24 秒	0.41 秒

5.4. 考察

今回の検証によって、OS 起動時に自動起動するように設定を行うワームであれば、ワーム感染チェックによって、高速に検知および駆除を行うことが可能であることを示すことができた。ワームには、CodeRed や SQLSlammer などのように、自動起動設定を行わないものも存在するが、これらは、サーバを狙ったものであり、今回対象としている、OS の再起動を頻繁に行うクライアント PC を狙ったワームは、自動起動設定を行うと考えられるため、十分対応できると考えられる。

ただし、本システムのワーム感染チェック機能では、既知のワームしか検知することができない。仮に、未知のワームに感染した PC が接続された場合には、ワーム感染チェックでは検知することができない。しかし、未知のワームであっても、それが既知の脆弱性を狙うものであれば、本システムのワーム感染防御機能によって、感染を防ぐことができる。また、ワームセンサによって未知のものも含めてワームを検知し、隔離することができるため、ワーム感染の被害が拡大する前に迅速に対処することが可能となる。

しかし、マスメーリングワームの中には、送信先メールサーバを探索するために、DNS の MX レコードではなく、A レコードを問い合わせるものも存在する。この場合には、現在のワームセンサでは検知することができない。今後、検知アルゴリズムを追加して、このようなワームにも対応する必要がある。

また、参考文献[2]において提案した方式では、脆弱性チェックに Nessus[8]を使用していたため、チェックに 1 分近くかかってしまうという問題があった。今回の方式では、ActiveX コントロールを使用して内部からチェックすることにより、0.5 秒以内でチェックすることができ、チェック時間の大幅な短縮を実現することができた。

6. まとめ

イントラネットに接続した PC のワーム検疫、および、脆弱性チェック、トラフィック監視によるワーム検知の結果から、ネットワーク機器の VLAN およびブリッジファイアウォールの設定を動的に制御することによって、統合的にワームによる被害から防御するシステムについて提案した。そして、プロトタイプを実装し、本方式が有効に動作することを示した。

今後は、実運用を想定し、負荷をかけた状態での性能などを評価していく予定である。

参 考 文 献

[1] “コンピュータウイルスの届出状況について[詳細]“, 独立行政法人 情報処理推進機構 セキュリティセンター, 2005 年 2 月 3 日, http://www.ipa.go.jp/security/txt/2005/documents/virus-full0502.pdf

[2] 角将高, 馬場達也, 稲田勉, “動的 VLAN 制御による脆弱ホスト保護方式の提案“, コンピュータセキュリティシンポジウム 2004（CSS2004）論文集 Volume I of II, 情報処理学会シンポジウムシリーズ Vol.2004, No.11, pp.49-54, 2004 年 10 月発行.

[3] "Port Based Network Access Control", IEEE 802.1X, Institute of Electrical and Electronics Engineers, Inc., http://www.ieee802.org/1/pages/802.1x.html

[4] ebtables, http://ebtables.sourceforge.net/

[5] The FreeRADIUS Project, http://www.freeradius.org/

[6] Bell, E., Smith, A., Langille, P., Rijhsinghani, A. and K. McCloghrie, "Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions", RFC 2674, August 1999.

[7] Internet Systems Consortium, Inc., http://www.isc.org/

[8] The Nessus Project, http://www.nessus.org/