2005.1.20

擬似 Private VLAN における Worm の感染防止と異常検知に関する研究

大阪産業大学大学院 工学研究科 情報システム工学専攻
情報安全工学研究室　03MH01 赤松康介

1　はじめに

現在、コンピュータは様々な危険にさらされている。その中の 1 つに Worm の感染がある。Worm は、ネットワークを使って感染する。そのため、コンピュータがネットワークに繋がっているだけで、Worm は爆発的に広がる。

このような Worm の感染を防ぐために、組織内ネットワークにおいて Worm の感染を防ぐ手法が考えられている。しかし、それらの中には、ユーザが不正に設定を行なうことで、Worm の感染対策が無効になってしまうものや、機器の導入にコストが発生するものがある。本研究では、全てのクライアントコンピュータに対して Worm の感染対策が有効であるようにし、更にコストを低く抑えられる方法を考え、実現した。

2　Worm

Worm は、コンピュータウィルスの一種である。コンピュータウィルスとは、感染・潜伏・発病の機能を持ったプログラムのことをいう。コンピュータウィルスの中でも、ネットワークを使って他のコンピュータに感染するものを Worm という。

Worm の感染方法は以下の 2 種類に分けることができる。

- 感染先のコンピュータに直接通信を行なう
- 間に別のコンピュータを介して通信を行なう

前者は、他のコンピュータに対して直接通信を行ない、セキュリティホールを利用して感染する。

後者は、主にメイルを介して感染する。アドレス帳等に保存されているメイルアドレスに対してメイルを送信する。送信するメイルにファイルを添付し、受け取った人間が実行することで感染する。また、受け取ったメイルを表示すると自動的に添付ファイルを実行するようなセキュリティホールを持つメイラが存在する。それを利用して感染するものもある。

3　既存の Worm 感染対策

メイルを介して感染するものについては、既存のメイルゲイトウェイ等によって防ぐことができる。これはメイルを中継する際にウィルススキャンを行ない、ウィルスや Worm を見つけると削除する。

他のコンピュータに対して直接通信を行ない、セキュリティホールを利用して感染するものについては以下の 2 つが必要となる。

- セキュリティアップデートを行ない、最新の状態に保つ
- ウィルス対策ソフトウェアのパターンをアップデートし、最新の状態に保つ

しかし、これらのアップデートを外部から持ち込まれるコンピュータに対して徹底するのは困難である。これに対する対策として、検疫ネットワークが使われ始めている。検疫ネットワークを用いた対策は、先に述べたアップデートを徹底する方法である。

検疫ネットワークを用いた対策では、コンピュータをネットワークに接続しようとすると、組織内ネットワークとは別の検疫専用のネットワークに接続される (図 1)。そしてセキュリティアップデートが最新かどうか、ウィルス対策ソフトウェアのパターンが最新かどうかの 2 点が強制的にチェックされる。最新でなければ組織内ネットワークには接続されない。そこで、検疫ネットワークからアップデートファイルやパターンファイルを入手し、アップデートを行なう。チェックに合格すれば、組織内ネットワークに接続される (図 2)。これによって組織内ネットワークに繋がっている全てのコンピュータについて、セキュリティアップデートおよびウィルス対策ソフトウェアのパターンを最新に保つことができる。

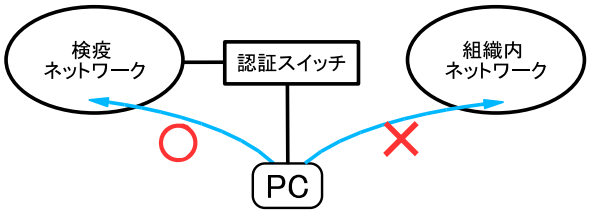

図 1: チェック合格前 (検疫ネットワークに接続)

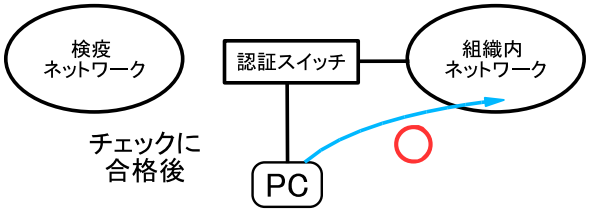

図 2: チェック合格後 (組織内ネットワークに接続)

検疫ネットワークを用いる場合は、チェック合格前と合格後で、接続先のネットワークの切り替えが必要となる。接続先のネットワークの切り替えには、以下の 3 つの方式がある。

- パーソナルファイアウォールを用いる方式
- DHCP サーバを用いる方式
- 認証スイッチを用いる方式

このうち、認証スイッチを用いる方式は、完全に検疫を行なうことができるが、機器の交換にコストが発生する。それ以外の方式は、検疫をのがれる方法があるため、望ましくない。

4 本研究で提案する対策

4.1 擬似 Private VLAN

Private VLAN というものが考えられ、実用化されつつある。Private VLAN とは、同一の VLAN 内においてクライアントコンピュータの間で直接通信をできなくする技術である。そしてクライアントコンピュータと特定のポートに繋がった機器 (ゲイトウェイ) との間の通信のみが許可される。これによって、クライアントコンピュータ間の直接通信を禁止しながら、インタネットやサーバなどへの通信を可能にしている。

しかし、そのようなスイッチの導入にはコストが発生する。そこで本研究では、コストをかけずに同等の機能を実現した。これを、擬似 Private VLAN と呼ぶことにする。DHCP を用いて、全てのクライアントコンピュータを論理的に別のネットワークに接続した。1 つのネットワークに 1 つのクライアントコンピュータとなるようにした。こうすることで、擬似 Private VLAN を実現した。

4.2 擬似 Private VLAN を用いた対策

本研究では、擬似 Private VLAN を構築して Worm の感染を防止することにした。従来の対策と同様に、ウィルス対策ソフトウェアの導入や、セキュリティアップデートの適用は従来通り行なう。そして検疫は行なわない。検疫ネットワークを用いる代わりに、擬似 Private VLAN を用いて Worm の感染を防止する。

コンピュータを接続する際、チェックを行なわずに組織内ネットワークに接続する。組織内ネットワークは擬似 Private VLAN を用いて構築されているため、他のクライアントコンピュータに対して直接通信を行なうことができない。(図 3)。このため、セキュリティホールを抱えたコンピュータが存在しても、通信できないため Worm に感染することはない。

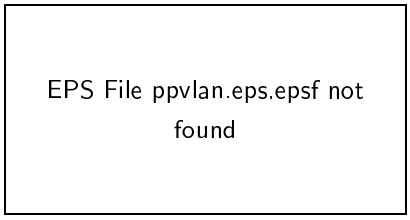

図 3: 擬似 Private VLAN を用いた対策

4.3 異常検知

擬似 Private VLAN を用いて組織内ネットワークを構築した場合、組織内ネットワークにある他のコンピュータに対して Worm は感染しない。しかし外部への攻撃は可能である。このため、なんらかの対策が必要である。そこで、ゲイトウェイに異常検知の機能を持たせることにした。

擬似 Private VLAN を使う場合、ネットワークの構成上、全ての通信はゲイトウェイを経由する。そこでゲイトウェイにおいて異常検知を行なう。本研究では、以下の 3 つの方法で異常検知を行なった。

- 既存の IDS による異常検知
- おとり IP アドレスを用いた異常検知
- パケットの送信先の数による異常検知

まず、既存の IDS(Intrusion Detection System) を用いて異常検知を行なう。IDS は、既知のセキュリティホールに対する攻撃パターンをデータベースとして持っており、パターンに合致する通信を検出する。

おとり IP アドレスを用いた異常検知は、通常時は通信を行なうことのない、未使用の IP アドレスを用意する。そのアドレスに対して通信が行われれば、異常であると判断する。

パケットの送信先の数による異常検知は、パケットの送信先の数を集計する。IP アドレスとポート番号をセットにして送信先とし、いくつの送信先に対してパケットを送信したかを集計する。そして、一定数以上の送信先に対してパケットが送信されれば、異常であると判断する。

5 まとめと今後の課題

以上のように、擬似 Private VLAN と異常検知機能を組み合わせて、Worm の感染を防止するネットワークが構築できた。擬似 Private VLAN によって、Worm が組織内ネットワークに持ち込まれても、他のクライアントコンピュータに被害が広がらなくなる。また異常検知機能を利用することで、持ち込まれた Worm を発見することができる。

本研究の対策を用いる利点として、クライアントコンピュータを利用するユーザの負担が無いことが挙げられる。ユーザは、従来のネットワークと同じ手順で利用することができる。また、導入コストが低いことが挙げられる。本研究の対策の場合、従来のスイッチをそのまま利用することができる。そして、この対策を不正にのがれることはできない。

現在の閾値を用いた異常検知機能は通常時のパケットの送信先が増えると、それに合わせて調整する必要がある。今後は閾値の調整を容易にする方法についても検討する必要がある。異常のあるコンピュータからの通信を遮断する自動遮断機能や、異常なパケットの流れを判別するための、より良いアルゴリズムについても検討していく。