M_017

検疫ネットワークにおけるワーム拡散防止の一手法
A study of worm prevention on the quarantine network

豊国明子† 原田道明† 時庭康久† 樋口毅†
Akiko Toyokuni Michiaki Harada Yasuhisa Tokiniwa Tsuyoshi Higuchi

1. はじめに

最近のセキュリティ被害の傾向として、悪意のないユーザであっても、管理が不十分な端末をイントラネットに接続したことが原因となり、そこからワームに感染したり、ネットワークが不正に使用されたりするケースが増えてきた。このような被害を、FWやIDSのような外部からの侵入を監視するタイプの製品だけで防ぐことは難しく、安全な端末しかネットワークに接続させない"検疫ネットワーク"という仕組みが注目されている[1]。検疫ネットワークでは、ネットワークに接続しようとする端末のセキュリティ対策状況や稼動状態を自動的に検査し、ネットワークの管理ポリシーに適合する端末のみ接続を許可する。ネットワークの管理ポリシーを満たしていない端末には隔離・治療といった対策が施される。

我々は、セキュリティゲートウェイ（以下、SGW）を用いた検疫ネットワークシステムを提案している[2]。SGWは、検疫ポリシーに違反した不正端末の通信を遮断し、不正端末をSGWの外側ネットワークから隔離することができる。しかし、SGWは、SGWを経由しない端末同士の通信は制御できない。このため、例えば端末がワームに感染した場合、SGWで感染端末を遮断しても、SGWの内部ネットワークではワームが拡散してしまう可能性があった。本発表では、この問題を踏まえ、不正端末と同じ内部ネットワークに属する他の端末とを通信させないようにすることで、内部ネットワークにおけるワームの拡散を阻止する方式について提案する。

2. 検疫ネットワークシステム

2.1 概要

我々の提案する検疫ネットワークシステムは、以下の3つの要素から構成される。

ポリシーマネージャ：SGWやAgentから収集したインベントリ情報をもとに端末の検疫ポリシー検査を行い、検査結果に従った対策を指示するポリシー管理サーバ

SGW：端末のネットワークへの接続を検出し、ポリシーマネージャから指定された不正端末の遮断を実行する専用ハードウェア

Agent：端末の稼働状況をポリシーマネージャに通知する端末内蔵型プログラム

本システムの特長を挙げる。

- MACアドレスをベースとした端末認識を行っているため、動的IPを使用した不正行為も見逃さない
- 既存ネットワークの構成に影響を与えないリピータタイプのSGWを使用し、導入をスムーズに行える
- Agentとポリシーマネージャの連携により、きめ細かな検疫ポリシー検査を行うが、Agentをインストールしない端末の監視もサポートする

†三菱電機（株）情報技術総合研究所

2.2 提案システムにおける課題

ポリシーマネージャは、ポリシーに適合しない不正端末を検知したとき、必要に応じてSGWに不正端末の遮断を指示する。しかし、ポリシー検査の隙間をかいくぐり端末がワームに感染した場合、いくらSGWで外側ネットワークへのワームの流出を止めても、構築された検疫ネットワークの構成によっては、内部ネットワークでのワーム拡散に対処することは難しい。

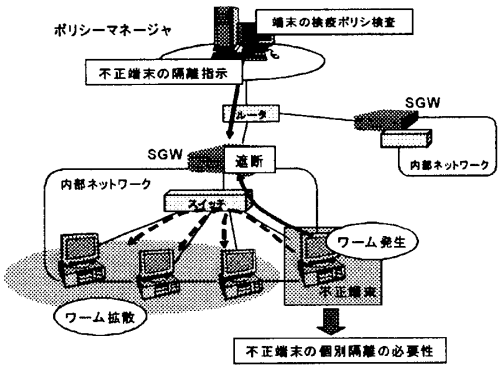

図1：ワームの拡散

図1のように、検疫ネットワークを構築するとき、SGWの導入台数を節約するため、まずSGWの各ポートにスイッチやHUBをつなげ、その下に端末を接続するのが一般的である。SGWの1ポートに複数の端末が属し、内部ネットワークを形成する。このような構成でネットワークを組むと、内部ネットワークにある端末間の通信は、スイッチやHUBで分岐しているため、SGWを経由することはない。従って、これらの端末のうちの1つがワームに感染してしまうと、SGWの存在とは無関係に他の端末と通信できてしまうため、SGWの同一ポートに接続された端末には、感染が広がってしまう可能性があった。

この問題を解決するには、SGWの内部ネットワークにおいても、不正端末を個別に隔離する手段が必要である。我々は、SGWの内部ネットワークにおけるワーム拡散阻止と同時に、感染端末の迅速な復旧の実現を目指し、以下の2つの要件を満たすこととした。

- 要件1：同じSGWの配下にある端末との通信を阻止すること
- 要件2：隔離は行うが、治療サーバなど特定サイトとの通信は可能であること

隔離方法には、(1)不正端末自身による隔離、(2)他端末での通信破棄による隔離、(3)SGWによる隔離が考えられる。(1)については、ウィルス対策ソフト等で実装された既存技術があり、それら専用S/Wの事前準備なしでの実現は難しい。また、端末が重度の攻撃を受けた場合は制御不能となることも考えられるので、本研究では、(2)と(3)について方式を検討した。

3. 端末の個別隔離方式

3.1 他端末での通信破棄による隔離

我々の提案する検疫ネットワークは、端末 Agent からの情報収集により、端末の安全性を確認する仕組みのため、SGW に接続している保護すべき端末には、原則として Agent がインストールされている。そこで、隔離対象となった不正端末と同じ SGW に接続されている Agent 端末に対し、隔離対象となった端末の MAC アドレスリストを一斉通知し、各端末で隔離対象端末からの通信フレームを廃棄させる方式を検討した。

以下に、本方式の具体的の手順を示す。

① ポリシーマネージャは、定期的に接続端末の検疫ポリシーをチェックし、不正端末を見つけると SGW に隔離指示コマンドを送信する。SGW では、コマンドを受信して隔離端末リストを保持する。

② SGW から内部ネットワークに接続された端末 Agent に隔離端末 MAC アドレス一覧を一斉通知する。

③ 各 Agent においても、隔離端末 MAC アドレス一覧を持ち、SGW からの通知により一覧を更新する。

④ 各端末では、この一覧情報に基づき、送受信フレームの廃棄を行う。

以上の手順で、隔離端末と他の端末の通信はできなくなり、ワームの拡散を阻止することができる。SGW の外側との通信は、今までと変わらず SWG のアクセス制御により適切に中継できる。なお、SGW からの一斉通知には、成りすまし・改竄・リプレイ攻撃への対策として、通知パケットの暗号・認証を行う。

3.2 SGW による隔離

3.1 章では、端末 Agent を前提とした隔離方式について述べたが、イントラネットには Agent を使用できない端末が存在することも十分考えられる。そこで、本章では端末 Agent がインストールされていなくとも、ワームの拡散を阻止する方式について説明する。

通常、通信フレームの送受信における最初の動作は、ARP 要求のブロードキャスト送信である。また、Windows PC を LAN に接続すると ARP 広告をブロードキャスト送信することが知られている。我々は ARP のブロードキャストが同一セグメント内の全端末に到達することに着目し、不正端末が関係する ARP ブロードキャストを待ち受けることで、不正端末と他の端末の間で通信が行われるタイミングを掴むことができると考えた。もし、受信した ARP パケットに対応する偽の応答を返すことによって、端末が ARP キャッシュに偽の応答を学習するなら、不正端末の通信相手を SGW に変更し、不正端末と他の端末との通信を回避することができる。

Windows PC が ARP キャッシュを更新する条件を検証したところ、既に ARP キャッシュに登録されている IP に別の MAC を持つ新たな ARP 応答（偽の ARP 応答）を受信させたとき、ARP キャッシュが更新されることがわかった。また、ARP 広告の受信についても同様に ARP キャッシュを更新することを確認した。この結果は、たとえ偽の ARP 要求や ARP 広告を送られても、Windows PC は ARP キャッシュを更新して、IP と MAC の組合せを学習することを示している。

我々は、この特性を利用し、SGW から偽 ARP を応答することによって、隔離端末と他端末の通信を横取り、SGW のフィルタ制御に迂回させる方式を検討した。

ポリシーマネージャから SGW に隔離端末リストを通信した後（3.1 の①と同様）、SGW からの偽 ARP の送信タイミングには、以下の５つのイベントが考えられる。

(1) SGW が新しい隔離端末 MAC を取得した時

SGW は、隔離端末の MAC の代わりに SGW の MAC に付替えた ARP 広告をブロードキャストし、配下の全端末に、隔離端末=SGW であると誤認させる。

(2) 隔離端末から他の端末への ARP 要求を受信した時

SGW は、要求 IP を持つ端末の MAC の代わりに、SGW の MAC に付替えた ARP 応答を隔離端末に返信し、隔離端末に、要求 IP を持つ端末=SGW であると誤認させる。

(3) 他の端末から隔離端末への ARP 要求を受信した時

SGW は、内部ネットワークからの ARP 要求に対してのみ、隔離端末の MAC の代わりに SGW の MAC に付替えた ARP 応答を返信し、ARP 要求送信元の端末に、隔離端末=SGW であると誤認させる。

(4) 隔離端末からの ARP 広告を受信した時

SGW は、隔離端末の MAC の代わりに SGW の MAC に付替えた ARP 広告をブロードキャストし、配下の全端末に、隔離端末=SGW であると誤認させる。

(5) 他端末からの ARP 広告を受信した時

広告された他ホストのアドレスを隔離端末に知らせないように、隔離端末に SGW の MAC アドレスを ARP 応答することが考えられるが、一方的なアドレス通知に効果が得られるか疑わしいので、今回は実装しないこととした。

(2)と(3)では、SGW からの ARP 偽応答の後、本来の ARP 応答が到達し、ARP キャッシュが上書きされてしまう場合に備え、偽 ARP の応答は一定の間隔で複数回送信する。また、(2)について、全端末に対して偽の ARP 応答を返信すると、要件 2 が満たせなくなるため、特定サイトの IP アドレスを登録しておき、偽 ARP を返信しないようにする。これら一連の処理によって、内部ネットワークでの隔離端末と他の端末間の通信を SGW に迂回しながら、特定サイトとの通信路は確保することが可能となる。

4. まとめ

本発表では、検疫ネットワークシステムの構成、ポリシー管理の概要を述べ、このシステムを前提としたワーム拡散に対する防御策として、２つの端末の個別隔離方式を提案した。これらは併用することも可能である。

今回は、Windows PC を用いたシンプルなネットワーク構成を想定して検討を進めたが、今後は様々なタイプの端末を取り入れ、実運用に近い環境での検証が必要であると考えている。

参考文献

[1] @IT “特集：検疫ネットワークとは”
http://www.atmarkit.co.jp/fnetwork/tokusyuu/27keneki/01.html
[2] 樋口 毅他, “アタックトレラントシステムの開発 －(4)不正接続端末検知”, 電子情報通信学会, 2005 ソサイエティ大会, B-6-43