4W-5

エージェントレス型 DHCP ゲートウェイ方式 検疫システムの実装及び評価

趙　昕　　安井 浩之　　松山 実

武蔵工業大学

1　まえがき

Blaster などによるワーム騒ぎでは，従来の不正侵入防止策としてのファイアウォールや侵入検知システムだけでは感染を防ぐことができず甚大な被害が出ていた．それを機に，内部ネットワークに持ち込まれたワーム感染 PC によるウィルス拡散を防ぐ手法として，新たに検疫ネットワークソリューションが提案された．

本報告では，すでに提案している IP 割り当てと検疫誘導の機能を有する DHCP サーバ兼検疫ゲートウェイ(以後，検疫ゲートウェイ)によるエージェントレス型の検疫システム[1]の実装方法と評価について述べる．

2　システム概要

本システム[1]の構成を Fig.1 に示す．

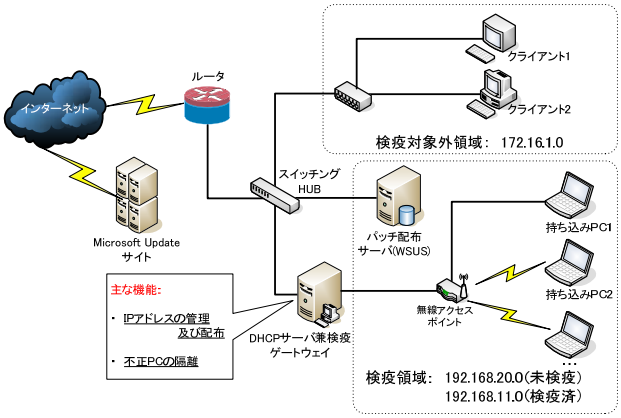

Fig.1 ネットワーク構成図

まず内部ネットワーク(LAN)を検疫ゲートウェイにより，物理的に 2 つの領域に分ける．1 つは検疫対象外領域，すなわちパッチ当てやウィルス対策などが組織により管理されており，検疫不要な PC が設置される領域である．もう 1 つは論理的に構成される検疫領域である．持ち込み PC は Windows OS とし，検疫領域にてネットワーク接続を行う．検疫ゲートウェイを設置することで異なる 2 つの領域間における通信を制御できる．本システムは主に学校や，公衆無線 LAN サービス（HOTSPOT）などの不特定多数のユーザが利用する有線／無線の情報コンセントを対象とする．検疫では，持ち込み PC の OS が最新の状態であるかどうかを判定する．クライアントソフトを必要とする従来の DHCP 型検疫システムに対して，本システムでは検疫ゲートウェイのみで，IP アドレスの割り当て，パッチダウンロードへの誘導及び未検疫 PC を隔離する機能を実現している．

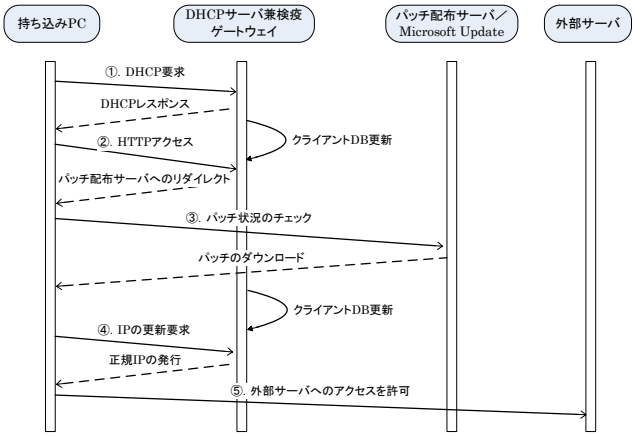

Fig.2 シーケンス図

検疫の流れは Fig.2 のシーケンス図に示すように 5 つのフェーズからなる．

① 持ち込み PC は情報コンセントに接続すると，DHCP Discover パケット[2]をブロードキャストし，IP アドレスの割り当てを要求する．検疫ゲートウェイはこのパケットを受信し，検疫がまだ行われていない PC と判明したら検疫領域の未検疫用の一時 IP アドレスを発行し，クライアント DB の情報を更新する．

② 未検疫の PC が HTTP 通信しようとすると，検疫ゲートウェイは未検疫の PC に対して Microsoft Update サイト(以後，MU サイト），またはパッチ配布サーバへリダイレクトするよう指示する．

③ MU サイトで検査を受け，未適用のパッチがあったらそれをインストールする．その適用過程を検疫ゲートウェイが監視し，パッチが適用済みであることを確認の上，クライアント DB の情報を更新する．

④ 一時 IP リース期間の半分が過ぎたところで，持ち込み PC から DHCP サーバに IP 更新要

Agent-less DHCP Gateway Type Network Quarantine System
－Implementation and Evaluation－
Xin Zhao,Hiroyuki Yasui,Minoru Matsuyama
Musashi Institute of Technology

求を送信すると，外部にアクセスできる正規な IP アドレスが発行される．

⑤ その後持ち込み PC は外部サーバにアクセスできるようになる．

3 隔離・検疫機能の実装

本システムでは，UNIX や Linux システムで数多く用いられている ISC DHCP[3]サーバを採用し，それと連携動作する検疫サーバプログラムを実装した．IP アドレスの割り当ては DHCP サーバが担当し，一時 IP と正規 IP のどちらを割り当てるのかを決定するのは検疫サーバが担当する．DHCP サーバと検疫サーバとの連携は ISC DHCP サーバに付属する API－OMAPI[4]を用いることで実現している．

パッチの適用状況を判断する基準は，MU サイトでのパッチ検査を終了した際に送られてくるパケットのデータ部分の長さがある特定のサイズになっていることである[1]．パッチ検査のプロセスでこの特定サイズの HTTPS ペイロードを検出できれば，持ち込み PC は全てのパッチが適用済みと見なし，検疫サーバは OMAPI を通し，この持ち込み PC に対して次のリース期間更新時に正規 IP を割り当てるよう DHCP サーバを動的に設定する．一時 IP のリース期間を短く設定することで，パッチ適用後に速やかに正規 IP の発行が行なわれるようにしている．

なお，検疫ゲートウェイに設置されるファイアウォール(iptables)により，一時 IP の持ち込み PC からのアクセスは MU サイトへのアクセスを除き，すべて破棄される．

4 実験と評価

システムの基本機能を実装し，動作テストを行った．Fig.3 は実験用ネットワークの構成を示す．

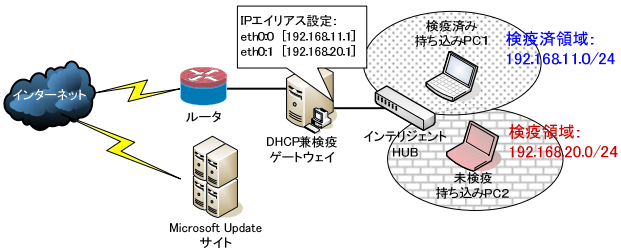

Fig.3 実験用ネットワークの構成

Table1 各マシンのスペック

マシン名	CPU	メモリ	OS
持ち込み PC1	866MHz	256MB	WinXP
持ち込み PC2	1GHz	256MB	WinXP
検疫 GW	600MHz	512MB	CentOS4

ネットワーク： Ethernet 100BASE-TX
DHCP サーバ： ISC DHCP ver.3.0.4
一時 IP リース期間： 3 分間
正規 IP リース期間： 6 時間

上記の構成において，テストを行った結果，未検疫の持ち込み PC1，PC2 に対して DHCP サーバが一時 IP(192.168.20.9，192.168.20.10)を割り当てたことをまず確認できた．その後，PC1 の次に PC2 の順番で Microsoft Update サイトにアクセスし，パッチの検査を行った．PC1 の場合，全てのパッチが適用されているため，正規 IP(192.168.11.20)が割り当てられた．一方 PC2 の場合，未適用のパッチがあったため，正規 IP の割り当てが行われなかったことも確認できた．

第 2 段階の実験において，すでに正規 IP が割り当てられた PC1 を一度検疫ネットワークから切り離し，正規 IP リース期間以上の時間を経ってから再接続し，動作確認を行った結果，正規 IP が割り当てられたことを確認した．

最後の実験，未検疫の持ち込み PC2 において固定 IP を設定した場合の動作確認では，DHCP による IP 割り当てのプロセスがないまま送信された「Gratuitous ARP」(以後，GARP)パケット[1][6]が検出されたため，検疫ゲートウェイから GARP に対する偽装の ARP 返事パケットが返され，固定 IP の設定ができないことを確認した．

5 まとめ

本検疫システムを用いることでセキュリティレベルの低い持ち込み PC を制限し，ワーム感染 PC による被害を最小限に抑えることができる．本システムの特徴であるエージェントレスで実装されていることと，従来の DHCP 型検疫ネットワークが対応できない固定 IP の不正設定問題[1]の解消で，より低コスト，管理負担の少ない検疫ネットワークを実現することができることを確認できた．

ただし，本システムは MU サイトを利用している場合，業務用など特定のパッチを当てないような運用には向かないというデメリットもあるが，パッチ適用サーバを WSUS[5]へ切り替えることで細かい適用ルールを設定できるようシステムの改良をしている．

参考文献

[1] 趙，安井，松山：“エージェントレス型 DHCP ゲートウェイ方式検疫システムの実装”，FIT2006（第 5 回情報科学技術フォーラム）講演論文集 pp.227-228

[2] RFC2131－DHCP
http://www.rfc-archive.org/getrfc.php?rfc=2131

[3] ISC DHCP
http://www.isc.org/index.pl?/sw/dhcp/

[4] OMAPI(Object Management API)
http://www.die.net/doc/linux/man/man3/omapi.3.html

[5] WSUS(Windows Server Update Services)
http://www.microsoft.com/japan/windowsserversystem/updateservices/default.mspx

[6] Gratuitous ARP
http://www.7key.jp/nw/garp.html