M-018

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

Implementation of Agent-less DHCP Gateway Type Network Access Quarantine Control

趙　昕† 安井 浩之† 松山 実†
Xin Zhao Hiroyuki Yasui Minoru Matsuyama

1．まえがき

コンピュータウィルスは，いまも次々と新種が登場し，その脅威は日々増大している．Blaster などによるワーム騒ぎでは，従来の不正侵入予防策であるファイアウォール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．その原因の 1 つが，ほぼ無防備状態の内部ネットワークに持ち込まれたワーム感染持ち込み PC である．そこで，ワームの社内ネットワークでの蔓延を防ぐ手法として，検疫ネットワークが提案された．

本報告では，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ネットワークの実装について述べる．

従来の DHCP 型検疫ネットワークでは固定 IP アドレスが設定されたクライアントに対応できないという問題があるが，本システムでは DHCP サーバを検疫実施セグメントの出入り口(ゲートウェイ)に設置し，IP レベルと MAC レベルでアクセス制御を行うことで対処する．

2．システム概要

本システムのネットワーク構成を Fig.1 に示す．

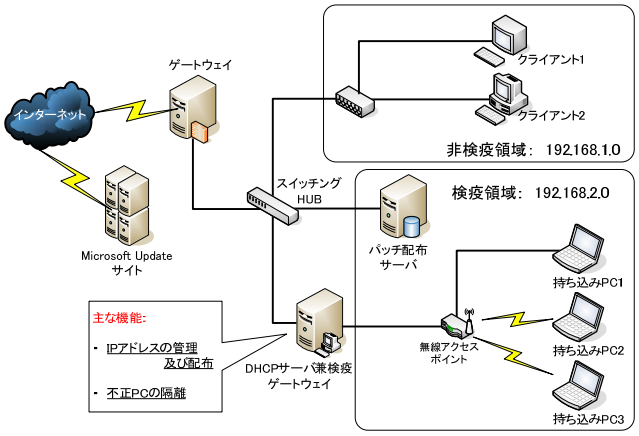

Fig.1 システムのネットワーク構成

まず内部ネットワーク(LAN)を論理的に 2 つの領域に分ける．1 つは非検疫領域，すなわち検疫を行わずデスクトップ PC が通常業務用として使われる領域である．もう 1 つは検疫領域である．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．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．従来の DHCP 型検疫ネットワークでは，対応するクライアントソフトや ActiveX プログラムなどを持ち込み PC にインストールする必要があったが，本システムでは検疫ゲートウェイで，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．

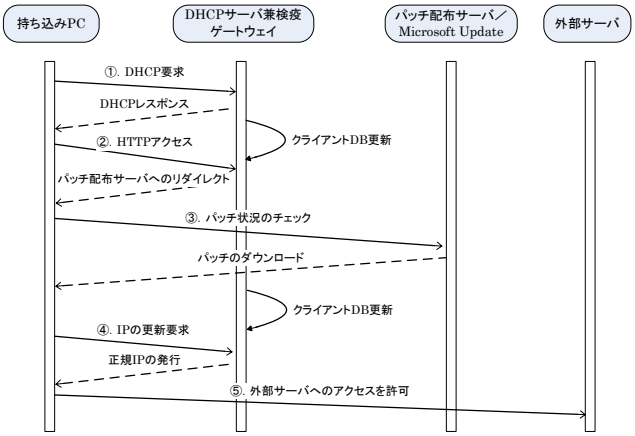

Fig.2 シーケンス図

検疫の流れは Fig.2 のシーケンス図に示しているように 5 つのフェーズからなる．(①) 検疫領域で情報コンセントを利用すると，まず持ち込み PC 側の DHCP クライアントが DHCP サーバ発見(DHCP Discover)パケット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．DHCP サーバが動作している検疫ゲートウェイはこの DHCP 発見パケットを受信し，発信元の PC が検疫済みかどうか，自分が保持しているクライアントデータベース(以後，クライアント DB)の情報を調べる．検疫がまだ行われていない PC と判明したら検疫領域用の一時 IP アドレスを発行し，クライアント DB の情報を更新する．一方，検疫済みの PC と判明した場合は外部と通信できる正規の IP アドレスを割り当てる．(②) 次に未検疫の PC が HTTP 通信しようとすると，検疫ゲートウェイがその HTTP パケットを捕らえ，Microsoft Update サーバ，また

† 武蔵工業大学
Musashi Institute of Technology

はパッチ配布サーバへリダイレクトするよう送信元の PC に指示する．(③) Microsoft Update サーバで検査を受け，未適用のセキュリティパッチがあったらそれをダウンロードし，インストールする．その適用過程を検疫ゲートウェイが捕捉し，パッチの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 のリース期間が満了直前の持ち込み PC から DHCP サーバに IP 更新要求を送信すると，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 PC は外部サーバにアクセスできるようになる．

3. IP 割り当てと隔離・検疫機能

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 サーバを機能拡張し，隔離・検疫モジュールを組み込んだ．既存の DHCP 機能を変更し，未検疫 PC に対する一時 IP の発行と，検疫済み PC への正規 IP の発行機能を追加した（Fig.3 フローチャート）．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．ゲートウェイにパケットが届いたときにまず IP アドレスをチェックし，一時 IP である場合は，Microsoft Update サイトへのアクセス以外のパケットはすべて破棄する設定になっている．

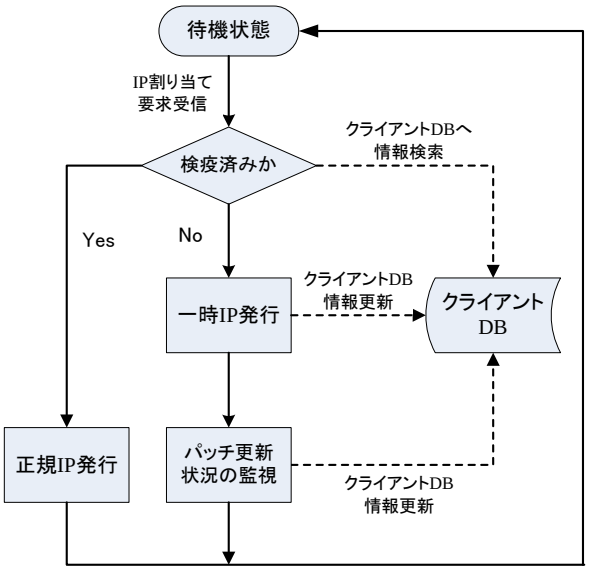

Fig.3　検疫ゲートウェイの動作フローチャート

パッチの更新状況を判断する基準は，Microsoft Update 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．Fig.4 に実際にパッチ検査プロセスで捕らえたパケットを示す．色が反転いるデータ部分は暗号化されており，内容を知ることはできないが，いくつかの OS について，複数の PC で実測した結果，パッチ適用が済んでいる PC には同じメッセージを送られていることが推測でき，そのデータ部分の長さは常に一定サイズになっていることが分かった．したがって本システムでは，検疫ゲートウェイでこのアプリケーションデータ部の長さを確認することで，持ち込み PC が OS の全てのパッチを適用済みであるかどうかを判断している．

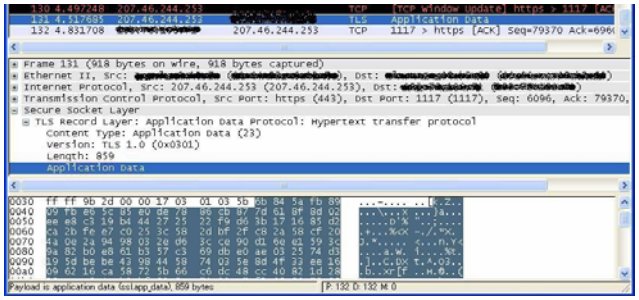

Fig.4　パッチ更新可否の判断基準となる部分

4　固定 IP 不正設定の問題について

従来の DHCP 型検疫ネットワークが固定 IP を設定されたクライアント PC に対応できない問題に関しては，Windows で IP アドレス設定の際に確認のために必ず発信される「Gratuitous ARP」(以後，GARP)というパケットを監視することで解決する．DHCP による IP 割り当ての後に出された GARP パケットであるか，それとも DHCP 要求がされないうちに出されたものなのか，検疫ゲートウェイ側でクライアント DB を参照し，判別する．DHCP 要求の無い場合は，不正であると判断し， GARP に対する偽装の返事パケットを返すか，検疫ゲートウェイ側のファイアウォールと連携し，不正端末からのアクセスを遮断するように実装する．

5　まとめと今後の課題

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，たとえワーム感染 PC がローカルネットワークに持ち込まれても，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と思われる．

今後の課題は，実運用環境での試験と検証を行うことと，パッチ適用後の Microsoft Update サイトから送られてくるアプリケーションデータが変更された際の対処方法の検討である．

参考文献

[1]　RFC2131－DHCP
http://www.rfc-archive.org/getrfc.php?rfc=2131
[2]　検疫ネットワークとは
http://www.atmarkit.co.jp/fnetwork/tokusyuu/27keneki/01.html