L-007

ユーザ認証システムを用いた DHCP認証ゲートウェイ方式検疫ネットワークの提案

Proposal of DHCP Authentication Gateway Type Quarantine Network Using User Authentication System

折原　義一†　　安井　浩之†　　松山　実†
Yoshikazu Orihara　Hiroyuki Yasui　Minoru Matsuyama

1．まえがき

近年インターネットの普及に伴い，ホットスポットなどの手軽に情報ネットワークへ接続することができる情報コンセント環境が普及してきている．環境が整い便利になる反面，ネットワークへの不正接続や携帯端末を基点としたコンピュータウイルスの拡大などのセキュリティ問題が多発している．

こういった問題は，外部ネットワーク(インターネット)に対する防御策であるファイアウォールや不正侵入検知システム(IDS)では防ぐことが困難である．そこで，内部ネットワークからの脅威を未然に防ぐ手段として，検疫ネットワークが提案された．

本報告では，DHCP 方式検疫ネットワークの隔離機能を向上させるために，筆者等が開発してきた「情報コンセントにおけるユーザ認証システム(Authenticated IP System : AIPS)」[1][2]を利用し，同じネットワーク内での相互通信の抑制や固定 IP を設定している端末からの通信の遮断を実現する DHCP 認証ゲートウェイ方式検疫ネットワークを提案する．

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．

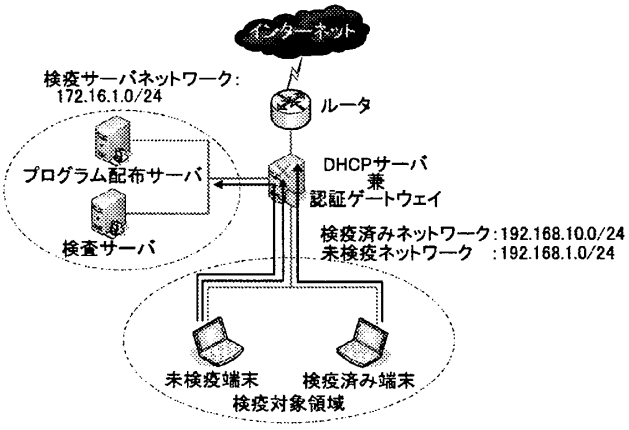

Fig.1　システムのネットワーク構成

本システムは主に学校やホットスポットなどの不特定多数が立ち入ることが可能なスペースに設置する有線または無線の情報コンセント(IPv4 のクラス C で構成)を対象とする．検疫の対象となる端末が接続する検疫対象領域は論理的に 2 つのネットワークに分ける．1 つはまだ検査を行っていない端末または検査に合格していない端末(未検疫端末)が接続する未検疫ネットワーク，もう一つは検査に合格した端末(検疫済み端末)が接続する検疫済みネットワークである．

端末には AIPS で認証を実現するためのプログラムを本システム向けに改良したものをインストールする．その端末のプログラムと認証ゲートウェイ上で動作する認証サーバプログラム，検査サーバ上で動作する検査サーバプログラムによって認証機能，検査機能，隔離機能を実装する．認証機能を使用するため，ユーザはあらかじめ認証ゲートウェイにユーザ名と接続用パスワードを登録しておく必要がある．未検疫端末からの通信は認証ゲートウェイによるフィルタリングで，HTTP は端末の専用プログラムを配布するプログラム配布サーバへ誘導され，その他の外部サーバへの通信は破棄される．

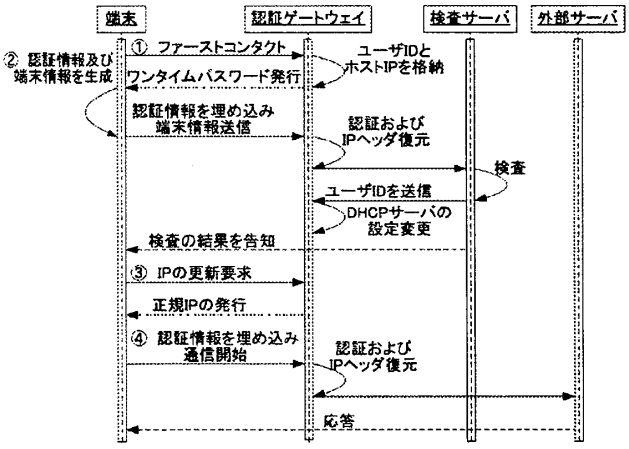

Fig.2　シーケンス図

検疫の流れは Fig.2 のシーケンス図に示すように 4 つのフェーズからなる．

① 未検疫端末は DHCP サーバによって未検疫ネットワークの IP アドレス(一時 IP)が割り振られた後，ユーザ ID と IP アドレスのホスト部を認証ゲートウェイに送信する(この動作を以

† 武蔵工業大学
Musashi Institute of Technology

下ファーストコンタクトと呼ぶ). ファーストコンタクトを受けた認証ゲートウェイはユーザ ID と一時 IP のホスト部を格納し，未検疫端末に対してワンタイムパスワードを発行する．その後，未検疫端末は送信する全てのパケットに対しワンタイムパスワードと接続用パスワードから生成した認証情報を IP ヘッダに埋め込み，通信を行う．

② ワンタイムパスワードを受け取った未検疫端末は，端末の情報を収集し，検査サーバへ送信する．端末の情報を受け取った検査サーバは端末にセキュリティ上の問題がないか検査を行う．検査によって端末にセキュリティ上の問題がないと判断すると，検査に合格した未検疫端末のユーザ ID を認証ゲートウェイへ送信後，未検疫端末に検査の結果を返す．

③ 検査に合格した未検疫端末のユーザ ID を受け取った認証ゲートウェイは，そのユーザ ID を元に DHCP サーバの設定を変更する．一方，検査結果を受け取った未検疫端末は IP 更新要求を行うことで，外部へ接続できる検疫済みネットワークの IP アドレス(正規 IP)が DHCP サーバから割り振られ，未検疫端末の IP アドレスは一時 IP から正規 IP に変わる．

④ その後，正規 IP を割り振られた検疫済み端末は外部サーバと通信できるようになる．

3. 検疫ネットワークによる隔離機能

UNIX や Linux システムで多く用いられている ISC DHCP サーバ[3]に付属する OMAPI(Object Management API)[4][5]を用いることで DHCP 方式検疫ネットワークの隔離機能を実装する．

DHCP サーバの設定は検疫対象領域に端末が接続した場合，一時 IP が割り振られるようになっているため，正規 IP を端末に割り振るには，DHCP サーバの設定を変更しなければならない．そのため，正規 IP を割り振る端末の MAC アドレスと検疫済みネットワークで使用されていない IP アドレスを指定し，OMAPI を通して DHCP サーバの設定を動的に変更することで，正規 IP を特定の端末に割り振る．端末の MAC アドレスはファーストコンタクト時に取得し，割り振られる正規 IP は認証ゲートウェイのプログラムによって管理されている端末情報を元に決められる．DHCP サーバの設定変更後，端末が IP 更新要求を行うことによって端末に正規 IP が割り振られる．これにより，端末が未検疫ネットワークから検疫済みネットワークへ移行し，未検疫端末との隔離が行われる．

4. AIPS による隔離機能

本システムでは ISC DHCP サーバと IPv4 のクラス C で構成されているネットワークを対象とした認証システムである AIPS を連係動作させることで DHCP 方式検疫ネットワークの隔離機能向上を図る．DHCP サーバと AIPS の連携は OMAPI を用いることで実現している．

AIPS は送信元 IP アドレスのネットワーク部に認証情報を埋め込み，認証ゲートウェイで認証およびパケットの復元を行っている．この機能によってパケットの送信元 IP アドレスが異なるため，同じネットワークに接続している端末同士での相互通信を抑制することができる．また，認証ゲートウェイにより外部サーバとの通信を監視し，フィルタリングを行うことで，不正端末からの外部サーバへの通信を遮断する．これにより，固定 IP アドレスを設定した端末からの通信も遮断し，固定 IP による接続問題を解消する．

なお，従来の AIPS は複数のネットワークには対応していないため，今回は IP ヘッダの ECN フィールドをネットワーク識別子として使用することで，論理的に分けられた 2 つのネットワークで AIPS の機能を利用することを可能とした．

5. まとめと今後の課題

本システムを用いてセキュリティに問題のある端末の通信を制限し，同じネットワーク内での相互通信を抑制することで，たとえワームに感染した端末がネットワーク内に持ち込まれても，被害を最小限に抑えることができる．また，従来の DHCP 型検疫ネットワークが対応できない固定 IP による接続問題の解消によって隔離機能を向上することができ，よりセキュアなネットワークを構築することができると思われる．

今後の課題は，現時点での端末専用プログラムは Linux のみ対応のため Windows への移植と不正端末のネットワーク接続に対する対処方法の検討，運用試験と検証を行うことである．

参考文献

[1] 倉内，安井，松山：“IP ヘッダへの利用者情報埋め込み型認証システムの構築”，情報処理学会　第 66 回(平成 16 年)全国大会講演論文集(3) pp.485-486

[2]中西，安井，松山：“IP ヘッダへの利用者情報埋め込み型認証システムの構築　—実験と評価—”，情報処理学会　第 68 回(平成 18 年)全国大会講演論文集(3)pp.689-690

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

[4]OMAPI(3) - Linux man page
http://www.die.net/doc/linux/man/man3/omapi.3.html

[5]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及び評価”，情報処理学会　第 69 回(平成 19 年)全国大会講演論文集(3)pp.359-360