# 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実装及び評価

折原　義一　　安井　浩之　　松山　実

武蔵工業大学

## 1　まえがき

情報コンセント環境が普及してきたことで，ネットワークの不正利用や端末を基点としたマルウェアの蔓延など，セキュリティ問題が多発してきている．

本報告では，すでに提案されている「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]の機能を利用し，DHCP 方式の隔離機能及びセキュリティを向上させた DHCP 認証ゲートウェイ方式検疫ネットワーク[2]の実装と評価について述べる．

## 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．

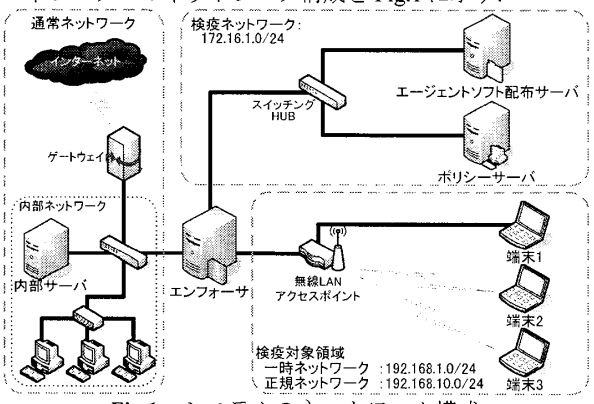


Fig.1　システムのネットワーク構成

本システムは認証ゲートウェイ及び DHCP サーバの役目を担うエンフォーサによってネットワークを物理的に 3 つの領域に分ける．通常ネットワークはインターネットや内部ネットワークなどの検疫対象外の領域，検疫ネットワークは検疫を行うために必要なサーバ群を設置する領域，検疫対象領域は検疫対象となる端末が接続するための領域である．

検疫ネットワークに設置するエージェントソフト配布サーバは，本システムを利用するため端末にインストールする必要があるエージェントソフトの配布を行う．また，ポリシーサーバは端末が管理者の定めたセキュリティポリシーを満たしているかポリシーチェックを行う．

検疫対象領域は論理的に IPv4 クラス C の 2 つのネットワークに分ける．1 つはポリシーチェックによりポリシーを満たしていると確認された端末(検疫済み端末)が接続する正規ネットワーク，もう 1 つはそれ以外の端末(未検疫端末)が接続する一時ネットワークである．

Implementation and Evaluation of DHCP Authentication Gateway Type Quarantine Network Using User Authentication System

Yoshikazu Orihara, Hiroyuki Yasui, Minoru Matsuyama
Musashi Institute of Technology

エージェントソフト導入済みの端末とエンフォーサ，ポリシーサーバ，そして内部サーバとの通信シーケンスは Fig.2 に示すように 4 つのフェーズからなる．

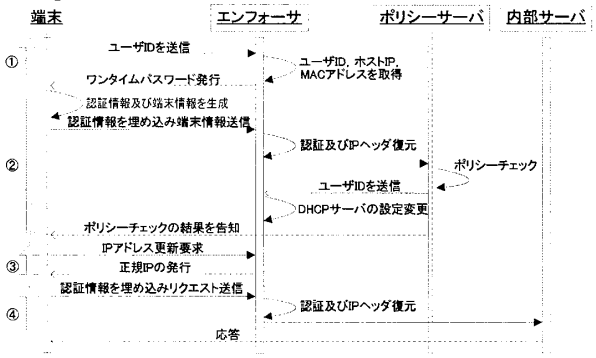


Fig.2　通信シーケンス

① 端末を検疫対象領域に接続するとエンフォーサから一時ネットワークの IP アドレス(一時 IP)が割り当てられる．端末のエージェントソフトからユーザ ID がエンフォーサに送信され(この動作を以下ファーストコンタクトと呼ぶ)，エンフォーサからワンタイムパスワードが端末に発行される．その際，エンフォーサは端末の MAC アドレスと IP アドレスのホスト部を取得し，ユーザ ID とユーザパスワード，ワンタイムパスワードを関連付ける．ワンタイムパスワードを受け取った端末は，②以降，ワンタイムパスワードとユーザパスワード，IP パケットのペイロード部から生成した認証情報を全ての IP パケットに埋め込み，送信する．

② エージェントソフトからパッチ適用状態などの端末情報がポリシーサーバに送信され，ポリシーサーバからポリシーチェックの結果が端末に返信される．その際，端末が管理者の定めたセキュリティポリシーを満たしていた時のみ，ポリシーサーバから端末のユーザ ID がエンフォーサに送信され，その情報を基にエンフォーサは DHCP サーバの設定を変更する．

③ 端末から IP 更新要求がエンフォーサに送信され，エンフォーサから端末に正規ネットワークの IP アドレス(正規 IP)が割り当てられる．

④ 正規 IP を割り当てられた端末は内部サーバに接続できるようになり，通常ネットワークが利用可能になる．

## 3　隔離機能の実装

本システムの隔離機能はエンフォーサと端末のエージェントソフトの 2 つにより実装されている．

エンフォーサの隔離機能はユーザモードで動作する検疫コントローラとカーネルモードで動作する IP 認証モジュールを連携動作させることによって実装した．検疫コントローラは UNIX や Linux システムで数多く用いられ

ている ISC DHCP サーバ[3]に付属する OMAPI(Object Management API)[4][5]を用いて任意の端末に指定した IP アドレスを割り当てることで，ネットワークの切り替えを実現している．IP 認証モジュールは Linux の標準的なファイアウォール機能である iptables で利用されている netfilter[6]を用いてカーネルモジュールとして実装しており，IP パケットを捕捉し，認証および IP ヘッダの復元を行っている．正規ネットワークに固定 IP を設定して接続した端末は，IP パケットに認証情報が含まれていないため，この IP 認証モジュールにより通信が破棄される．

端末のエージェントソフトはユーザモードで動作する検疫エージェントとカーネルモードで動作する IP 認証フィルタを連携動作させることによって実装した．検疫エージェントは端末情報の生成及びポリシーサーバへの送信を行う．IP 認証フィルタは送信される IP パケットに認証情報の埋め込みを行っており，Linux 版ではエンフォーサと同様に netfilter を用いてカーネルモジュールとして実装している．一方，Windows 版では TCP/IP 用のフィルタフックドライバ[7]として実装している．また，ファーストコンタクト後のワンタイムパスワード受信時にエンフォーサの IP アドレスのホスト部を取得し，同一ネットワーク内からの IP パケットは，送信元がエンフォーサ以外であれば破棄することで，同一ネットワーク内での端末間相互通信を抑制している．

## 4 検査・治療機能の実装

検査機能はエージェントソフトの検疫エージェントとポリシーサーバにより実装され，Windows は OS のパッチ適用状態，Linux はパッケージ管理ツールが管理しているパッケージの状態を中心にポリシーチェックを行う．

治療機能は認証が正常に行われている端末にのみ，Windows Update サーバやパッケージのリポジトリなどの管理者が許可した外部サーバに接続許可を与え，実施する．その他の外部接続はエンフォーサによって破棄される．なお，今回，治療機能は未実装である．

## 5 実験と評価

システムの基本機能を実装し，動作実験を行った．

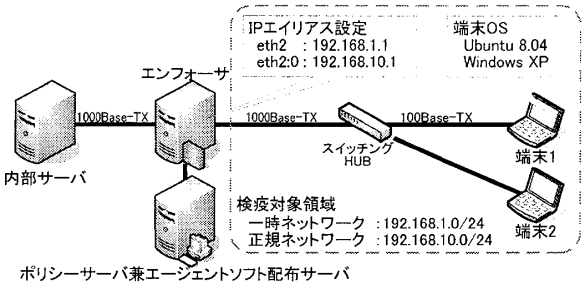


Fig.3 実験用ネットワーク構成

Table 1 各マシンのスペック

| マシン名 | CPU | メモリ | OS |
|---|---|---|---|
| 端末 1-2 | 2.0GHz | 1024MB | Fig.3 参照 |
| エンフォーサ | 900MHz | 256MB | Debian4.0 |
| ポリシーサーバ | 500MHz | 256MB | Debian4.0 |
| 内部サーバ | 2.2GHz | 2048MB | Debian4.0 |

DHCP サーバ : ISC DHCP ver3.1.1rc2

上記の構成において検疫ネットワークの基本動作の確認を行った結果，検疫対象領域に接続した端末に対してエンフォーサが一時 IP を割り当て，ポリシーチェック通過後，端末に正規 IP が割り当てられたことを確認した．

次に，AIPS の機能を利用することにより向上を図った隔離機能の確認のため，検疫対象領域での端末間相互通信範囲を確認した結果を Table2 に示す．なお，Table2 のエージェントソフト(AgentSoft)を導入していない正規 IP の端末は，固定 IP 設定で正規ネットワークに接続した端末である．この結果より，固定 IP 設定で正規ネットワークに接続した端末は，内部サーバに接続できないことを確認した．また，同一ネットワーク内での端末間相互通信範囲を大幅に狭めることができたことを確認した．

Table 2 検疫対象領域での端末間相互通信範囲

| | | | 送信側 | | | |
|---|---|---|---|---|---|---|
| | | | 一時 IP | | 正規 IP | |
| | | AgentSoft | 無 | 有 | 無 | 有 |
| 受信側 | 一時 IP | 無 | ○ | × | × | × |
| | | 有 | × | × | × | × |
| | 正規 IP | 無 | × | × | ○ | × |
| | | 有 | × | × | × | × |
| | 内部サーバ | | × | × | × | ○ |

## 6 まとめ

本検疫ネットワークを利用することで，従来の DHCP 方式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，同一ネットワーク内の端末間相互通信抑制，外部へ送信されるパケットの認証が可能であることを確認した．これにより，情報コンセント環境におけるネットワーク不正利用やネットワーク内でのマルウェア蔓延のリスクを抑えることができる．

今後の課題として，現在のシステムはファーストコンタクトや認証の失敗時に端末へ通知を行わないため，ユーザが通信を行えない原因を知ることができない．そのため，通知機能を実装する必要がある．また，1 つの情報コンセント環境に閉じたシステムであるため，ユーザパスワードを一元管理し，エンフォーサに通知するパスワード管理サーバを構築することが必要となる．さらに，今回，未実装である治療機能を実装する必要がある．

## 参考文献

[1] 安井浩之，松山実："IP パケット認証ゲートウェイシステム AIPS"，情報処理学会論文誌 Vol.49 No.7，2614-2622(July 2008)

[2] 折原義一，安井浩之，松山実："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"，FIT2008，講演論文集，pp.101-102

[3] ISC DHCP https://www.isc.org/sw/dhcp

[4] OMAPI(3) – Linux man page http://linux.die.net/man/3/omapi

[5] 趙昕，安井浩之，松山実："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 回全国大会講演論文集(3)，pp.359-360，2007

[6] The netfilter.org "iptables" project http://www.netfilter.org/projects/iptables/index.html

[7] Microsoft Tech net: TCP/IP パケット処理パス http://www.microsoft.com/japan/technet/community/columns/cableguy/cg0605.mspx