6Z-3

IPv6/IPv4 混在環境におけるユーザ認証システムの開発

永井 勢一† 安井 浩之† 吉野 邦生†
東京都市大学‡

1. はじめに

2011年2月にIANAのIPv4アドレス在庫が枯渇し，この問題の解決策として，IPv6の導入が進められている．IPv6の導入方式としては，現在多くのネットワークで用いられているIPv4と共存可能なデュアルスタック方式が主流になっていくと考えられる．

また，インターネットがさまざまな公共機関において使用できるようになり，そのような場所では不正利用を防止するためにユーザ認証システムが利用されている．しかし，上述したようなデュアルスタック向けのユーザ認証システムは少ないのが現状である．そこで本研究では，デュアルスタック環境向けのユーザ認証システムの開発を行う．

2. 関連研究

2.1. Opengate [1]

Opengateは，デュアルスタック環境に対応したユーザ認証システムである．ネットワーク上に設置されたOpengateが，通信の制御を行う．新しくユーザが接続した際に，IDとパスワードによる認証を行い，通信路を開放する．デュアルスタック環境では，一つの端末が複数のIPアドレスを持つことがある．そのため，MACアドレスを用いることで，以前に認証が成功した端末に対しては，新たに認証処理を行うことなく通信路を開放する．しかし， MACアドレス偽装に対して対策は取られていない．

2.2. AIPS [2]

AIPSは特定多数のユーザが利用する情報コンセント環境を想定し，IPv4 のクラスC規模を対象としたユーザ認証システムである．

このシステムは，ユーザの端末で動作する認証クライアントプログラムとネットワーク上のゲートウェイで動作する認証サーバプログラムよって認証を実現している．

このシステムの特徴は，認証クライアントプログラムが端末の送信するIPパケットのヘッダに認証情報を埋め込み，それを認証サーバプログラムで検証することにより認証を実現する点である．クラスCネットワークにおいて，IPヘッダの送信元アドレスの上位24bitは冗長であるため，その部分を利用して認証情報を埋め込んでいる．

しかし，IPv4 パケットヘッダ特有の領域を用いているため，ヘッダのフォーマットが異なるIPv6 には応用しづらく，また認証情報のサイズを大きくとることができない問題がある．

3. 本システム

3.1. 概要

本システムは，デュアルスタック環境向けのユーザ認証システムである．デュアルスタック環境では，同一端末で複数のIPアドレスを利用することが考えられるため，MACアドレスベースの認証システムとする．

ただし，MACアドレスは容易に変更可能であり，悪意のある者が正規ユーザのMACアドレスを詐称することで認証をくぐり抜ける可能性があるため，ユーザが送信する各IPパケットに認証情報を埋めこむことによりそれを回避する．

3.2. 構成

本システムの構成を図1に示す．

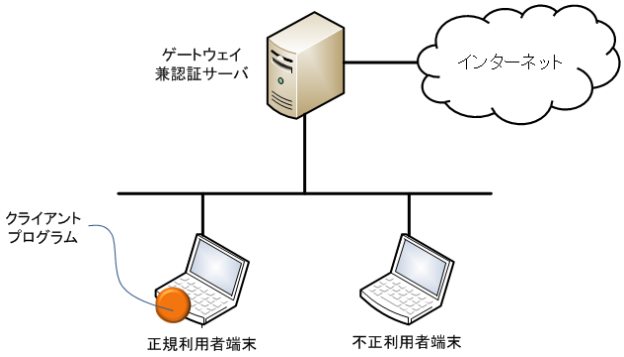

図1 システム構成

本システムは，ネットワーク上に設置するゲートウェイ兼認証サーバと，正規ユーザの端末にインストールして動作するクライアントプログラムによって構成される．また，チャレンジレスポンス方式を採用し，直接的なパスワードのやり取りは行わない．

Development of a user authentication system in a dual-stack environment
†Seiichi Nagai,Hiroyuki Yasui,Kunio Yoshino
‡Tokyo City University

クライアントプログラムでは，端末が送信するIPパケットをキャプチャし，ヘッダ部分に認証情報を埋め込み送信する．

ゲートウェイ兼認証サーバでは，クライアントプログラムによって送信された IP パケットをキャプチャし，認証情報を照合する．認証情報が正しくない場合や，クライアントプログラムがインストールされていない端末からの IP パケットである場合は破棄する．認証情報が正しく正規のユーザによる通信である場合は，ヘッダから認証情報を削除して外部のネットワークに送信する．

3.3. 認証情報

本システムにおいて用いる認証情報は，パスワード，チャレンジ，端末のシステム起動時間，IPパケットのペイロード部をハッシュ化することにより生成する．

パスワードは，事前にネットワーク管理者がユーザIDとともに発行したものである．チャレンジは，ゲートウェイ兼認証サーバにより256bitの乱数として発行される．端末のシステム起動時間は，端末によって重複が起こりにくく，もしも流出したとしても端末を再起動することにより再度設定される利点がある．また，IPパケットのペイロード部を用いることで，IPパケットごとに異なる認証情報を生成することができる．

これらをSHA256でハッシュ化し，IPv4であればオプションヘッダ，IPv6であれば拡張ヘッダに埋め込む．

3.4. システム動作

本システムの動作を図2に示す．

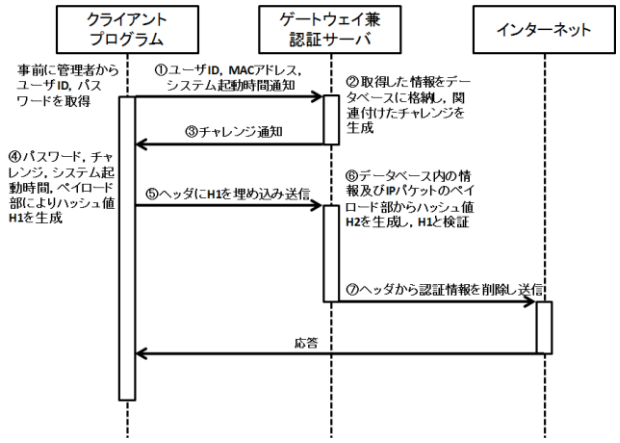

図2 システムの動作

①クライアントプログラムは，ユーザIDと端末のシステム起動時間，MACアドレスをゲートウェイ兼認証サーバに通知する．

②ゲートウェイ兼認証サーバは，それらの情報をサーバ内のデータベース格納し，それらに関連付けたチャレンジを生成する．

③ゲートウェイ兼認証サーバは，生成したチャレンジをクライアントプログラムに通知する．

④クライアントプログラムは，端末が送信するIPパケットをキャプチャし，パスワード，チャレンジ，端末のシステム起動時間，IPパケットのペイロード部から認証情報となるハッシュ値H1を生成する．

⑤クライアントプログラムは，H1をIPパケットのヘッダに埋め込み送信する．

⑥ゲートウェイ兼認証サーバは，通過するIPパケットのキャプチャを行う．登録されていないMACアドレスからのIPパケットや，認証情報が埋め込まれていないIPパケットは破棄する．埋め込まれている場合は，データベース内にあるパスワード，チャレンジ，システム起動時間とキャプチャしたIPパケットのペイロード部からハッシュ値H2を生成する．H1とH2を照合することによって認証情報を検証する．

⑦認証情報の検証が正しければ，認証情報を削除してIPパケットを外部のインターネットに送信する．正しくない場合は破棄する．

4. まとめ

本報告では，デュアルスタック環境におけるユーザ認証システムについて示した．本システムを用いることで，複数の IP アドレスが利用される環境においても，MAC アドレスにより端末単位で認証されるため，利用者の負担は少ないといえる．また，IP パケットに認証情報を埋め込むことにより，MAC アドレス偽装を検知することを可能にした．

今後の課題として，本システムは現在実装作業中であり，実証実験が行われていない．よって実装が終わり次第，デュアルスタック環境において実運用を行い，スループット等の評価をしていく必要がある．

参考文献

[1] 大谷誠，江口勝彦，渡辺健次“IPv4/IPv6 デュアルスタックネットワークに対応したネットワーク利用者認証システムの開発”情報処理学会論文誌 Vol.47 No.4 1146-1156 (2006)

[2] 加藤央，安井浩之，吉野邦生“IP ヘッダへの利用者認証フィールド埋め込み型認証システムの改良”情報処理学会論文誌 Vol.74 No.3 3651-3652 (2012)