M-003

情報コンセントにおけるユーザ認証システムの構築と改良

－認証情報の強化とトラフィック量の低減－

Development of Authentication System on Information Wall Socket

- Enhancement of Authentication Information and Reduction in Network Traffic -

中西 康夫† 安井 浩之† 松山 実†
Yasuo Nakanishi Hiroyuki Yasui Minoru Matsuyama

1. まえがき

近年インターネットの普及に伴い，個人の携帯端末で手軽に情報ネットワークへ接続できるホットスポットなどの情報コンセント環境が普及してきている．便利になる反面，情報コンセントの使用を許可されていない第三者がそのネットワークを悪用する危険性も増えている．

そこで，情報コンセントを利用するユーザの認証を行うため 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を提案してきた[1]．本報告では従来システムで課題となっていた埋め込まれた認証情報の強化とネットワークのトラフィック量の低減について述べる．

2. システム概要

本認証システムでは情報コンセントに接続する携帯端末上で動作する認証クライアントと，情報コンセントのゲートウェイ上で動作する認証サーバによって認証を行う．本認証システムのネットワーク構成を Fig.1 に示す．

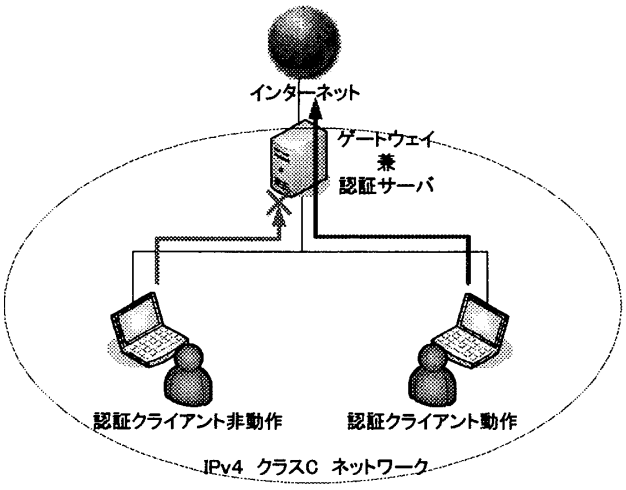

Fig.1 本認証システムのネットワーク構成

† 武蔵工業大学

ユーザはあらかじめ認証サーバにユーザ名と接続用パスワードを登録されている必要がある．以下に認証の流れを示す．

まず，個人の携帯端末（認証クライアント）は DHCP サーバによって IP が割り振られる．次に認証クライアントはユーザ ID と IP アドレスのホスト部を認証サーバに送信し，認証サーバはユーザ ID と IP アドレスのホスト部の対応を格納する（この動作を以下ファーストコンタクトと呼ぶ）．

本システムは IPv4 のクラス C で構成された情報コンセントを対象としていることから，ホストアドレス部は 8 ビットである．認証情報は認証サーバにより復元可能な（ネットワーク共通である）送信元 IP アドレスのネットワーク部（上位 24 ビット）に埋め込まれる．IP アドレスのネットワーク部の上位 8 ビットに送信パケット本来のプロトコル番号を保持し，IP ヘッダのプロトコル番号は本システムのためのプロトコル番号に変更する．これにより，認証クライアントが動作していないクライアントからのパケットをゲートウェイのフィルタリング機能で破棄することができ，認証サーバの負荷を軽減することができる．

認証ハッシュ値部（残り 16 ビット）が実際の認証に使用される部分で，パスワードとパケットのデータをハッシュ化して生成する．Fig.2 に認証情報が埋め込まれた IP ヘッダを例示する．

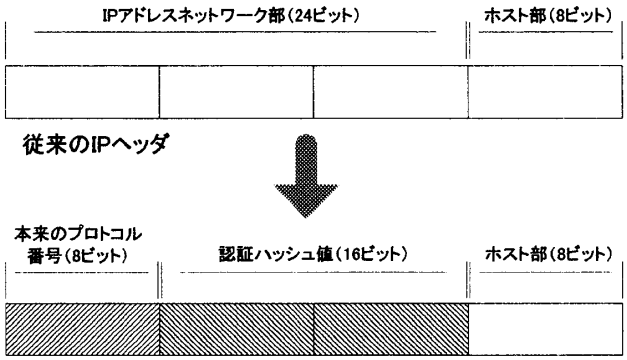

Fig.2 従来の IP ヘッダと本システムの IP ヘッダの発信元 IP アドレス部

ファーストコンタクト以降，個人端末から外部に向けて送信されるパケットは認証クライアントプログラムにより認証情報を埋め込まれ，送信される．

認証サーバはパケットに埋め込まれた認証情報により認証を行い，正規ユーザと判断された場合のみ IP ヘッダのプロトコル番号と IP アドレスのネットワーク部を復元し，外部に向けて送信する．

一方，外部からのパケットに関して認証サーバは認証情報の埋め込みを行わず，ゲートウェイを通過させ，クライアントに送信する．これは情報コンセント環境での外部からのパケットは主に内部からの要求によるものであると考えられるからである．

3. 認証情報の強化

前年度までの認証システムでは悪意あるユーザが正規ユーザの送信するデータをキャプチャし，正規ユーザがログアウトした後にキャプチャしたデータを再送信することで，正規ユーザに偽装することができてしまう．そこで，一定時間しか使用できないパスワード（以下，ワンタイムパスワードと呼ぶ）を認証サーバが発行することでこの問題を回避することにした．

システム概要で述べたファーストコンタクト時のレスポンスにサーバはクライアントにワンタイムパスワードを発行し，クライアントはこのワンタイムパスワードと接続用パスワード，さらにパケットデータから認証情報を生成し，IP ヘッダに埋め込むことでよりセキュアな認証を実現する．

Fig.3 に DHCP による IP が割り振られた後の流れを示す．

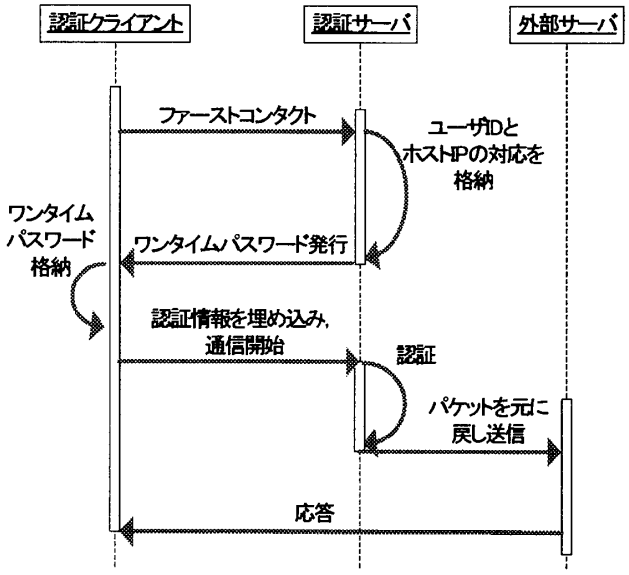

Fig.3 本認証システムのシーケンス図

4 ネットワークトラフィック量の低減

また，前年度のシステムにおいて Windows の認証クライアントプログラムの実現には試験的にパケットキャプチャライブラリを用いており，パケットをコピーし IP ヘッダへ認証情報の埋め込みを行っていた．このため二重のパケットが送信されており，無駄なトラフィックが発生していた．これを改善するため，デバイスドライバの一種であるフィルタドライバを開発し，直にパケットを操作することでネットワークトラフィックを半減した．

また Windows 認証クライアントプログラムにフィルタドライバを用いることより，今後よりセキュアな認証クライアントプログラムに発展することができると思われる．何らかのウィルスに感染している Windows クライアントに対し，認証サーバが通信停止命令を出すことで，ウィルス感染したクライアントのフィルタドライバによりデータ送信を不能にすることが可能である．これより，ウィルス発信の根源を停止することができ，被害拡大を防止することができると思われる．

5 まとめ

本認証システムを用いることで第三者の不正利用を阻止することができる．この認証システムの特徴である IP ヘッダに認証情報を埋め込むことで，TCP/IP モデルにおける IP 層以外の層のプロトコルに影響を与えることなく，送信情報への認証を行うことができる．これより認証機能を持った DHCP と組み合わせることもでき，よりセキュアな情報コンセントを実現することができると思われる．

今後は，Windows 認証クライアントにおいてユーザが操作しやすいインタフェースの実現と，Unix 系 OS などその他クライアントへの認証プログラムの移植，実際環境での運用試験と検証を行うことが課題である．

6 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）全国大会公演論文集(3) pp.485-486