

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 —

中西 康夫 安井 浩之 松山 実†

武蔵工業大学‡

1. はじめに

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][2][3]。本報告では改善したシステムの実験と測定、評価について述べる。

2. システム概要

本認証システムは IPv4 のクラス C で構成された情報コンセントを対象とし、許可されていないユーザの IP パケットをネットワーク外部に送信させないことを目的としている。利用者の識別情報は携帯端末から送信されるパケットに埋め込むこととし、情報コンセントのゲートウェイで認証を行うという形をとる。

IPv4 で構成されたネットワークであることから、IP ヘッダの送信元 IP アドレスの上位 24 ビットはそのクラス C ネットワーク内部で同一であり、冗長であるといえる。これを利用し、認証情報を埋め込む (Fig. 1)

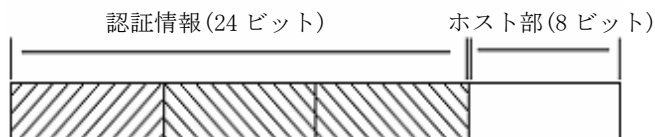


Fig.1 本認証システムの IP ヘッダ (送信元アドレス部)

本システム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ソフトウェア

アと、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ソフトウェアによって認証を行う。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。

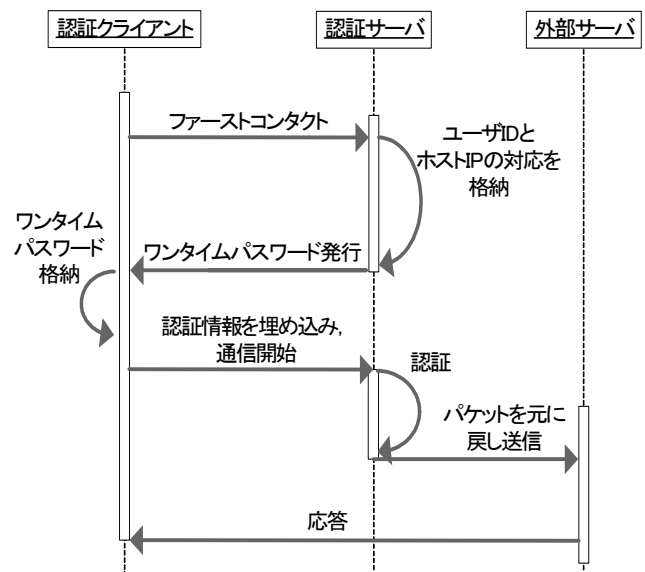


Fig.2 認証シーケンス

個人の携帯端末 (認証クライアント) が DHCP サーバによって IP を割り振られた後、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する (この動作を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し、認証クライアントに対しワンタイムパスワードを発行する。

その後、認証クライアントは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、さらに IP パケットペイロード部から認証情報を生成し IP ヘッダに埋め込み、通信を行う。

なお、情報コンセント環境の特性より外部からのパケットはすべて内部からの要求のレスポンスとみなし、認証サーバでは認証を行わないこととする。これにより認証処理によるオーバーヘッドが軽減できる。

Construction of Authentication system with user-authentication-field embedded into IP-header

- Experiment and Evaluation -

† Yasuo Nakanishi, Hiroyuki Yasui, Minoru Matsuyama

‡ Musashi Institute of Technology

3. パフォーマンス測定

認証処理の負荷によるパフォーマンスへの影響を測定するため、FTP による転送速度の測定を行った。

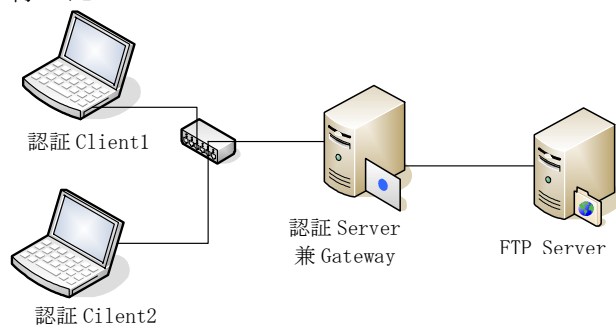


Fig. 3 実験ネットワーク構成

Table 1. 各マシンのスペック

マシン名	CPU	メモリ	OS
認証 client1	800MHz	256MB	Windows 2000
認証 client2	1GHz	256MB	Windows XP
認証 Server	733MHz	512MB	Debian/GNU Linux 3.0
FTP Server	366MHz	96MB	Debian/GNU Linux 3.1

ネットワーク：Ethernet 100BASE-TX

実装方法：

Windows 認証クライアント：フィルタドライバによる認証情報埋め込み

Linux 認証サーバ：pcap ライブラリを利用した認証情報チェック／IP ヘッダ復元

使用 FTP ソフトウェア：

クライアント：Windows の FTP コマンド

サーバ：proftpd 1.2.10-15 (Debian Package)

上記の構成において、認証あり・なしの状態で 5M バイトのファイルを転送し、PUT と GET の速度を計測（10 回の平均値）する。

4. 結果と考察

実験の結果を Table 2, Table 3 に示す。また改善前システムとの比較を Table 4 に示す。

Table 2. 認証クライアント 1 台での結果

	認証なし	認証あり	低下率
GET の転送速度 [KB/S]	11261.8	10552.1	7%
PUT の転送速度 [KB/S]	6935.57	6800.10	2%

Table 3. 認証クライアント 2 台での結果

	認証なし	認証あり	低下率
GET の転送速度 [KB/S]	6629.91	6015.39	10%
PUT の転送速度 [KB/S]	3056.37	3021.11	2%

Table 4. 改善前システム^[2]との比較
(認証クライアント 1 台での結果)

	改善前システム	改善後システム
GET の低下率	7%	7%
PUT の低下率	47%	2%

改善前 Windows 認証クライアントの実装方法：

pcap ライブラリを利用した認証情報の埋め込み

改善前 Windows 認証クライアントは pcap ライブラリを用いた実装をしており、パケットのコピーと認証情報の埋め込みをしていた。このため二重のパケット送信をして、サーバの負荷が高かった。改善後の実装方法はフィルタドライバによる IP ヘッダの直接操作をしており、無駄なトラフィックを生ずることがなくなった。

各結果より改善後の認証システムの PUT の転送速度に大幅なパフォーマンスの向上が見られた。

5. おわりに

本報告では IP ヘッダへの認証情報埋め込みによるパフォーマンス測定について述べ、改善システムではパフォーマンスが向上したことが示された。

現在の認証情報生成アルゴリズムは実験のため、強度より速度を優先しているため認証情報が簡単に見破られる可能性がある。

今後の課題として、パケットコピーによるサーバ負荷の軽減と、認証情報生成アルゴリズムの強化を行う必要がある。これらの課題を克服し、パフォーマンスとセキュリティを向上させ、更なるシステムの改善を目指す。

参考文献

- [1] 川内, 安井, 松山: “IPヘッダへの利用者認証フィールド埋め込みによる認証システム”, 情報処理学会 第 64 回 (平成 14 年) 全国大会公演論文集(3) pp.539-540
- [2] 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
- [3] 中西, 安井, 松山: “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”, 情報処理学会 FIT2005 第 4 回情報科学技術フォーラム論文集 pp.221-222