# 無線LAN環境における二重暗号化回避による通信効率の改善手法

岡山聖彦[†1] 山井成良[†1] 河野圭太[†1]

現在最も普及している無線 LAN の規格である IEEE802.11a/b/g では，通信内容の漏洩やネットワークの不正利用を防ぐために WEP（Wire Equivalent Privacy）や WPA（Wi-Fi Protected Access）が用いられている．しかし，これらと end-to-end の暗号化とを併用する場合には，無線区間が二重に暗号化されることになるため，通信効率が必要以上に低下するという問題がある．この問題点を解決するため，本論文は end-to-end 暗号化の有無に応じて，無線区間ではパケット全体の暗号化とパケット認証を切り替えることができるような手法を提案する．end-to-end の暗号化が行われている場合には，無線区間では暗号化の代わりにパケット認証のみを適用することにより，不正アクセスを防止しながら二重暗号化の回避による通信効率の改善が期待できる．

# An Improvement Method of Communication Efficiency with Avoidance of Duplicated Encryption on Wireless LAN Environment

Kiyohiko Okayama,[†1] Nariyoshi Yamai[†1] and Keita Kawano[†1]

On IEEE 802.11a/b/g, the most popular standards of wireless LAN networks, encryption functions called WEP (Wire Equivalent Privacy) or WPA (Wi-Fi Protected Access) are used for preventing malicious users from both eavesdropping and unauthorized access. However, along with end-to-end encryption, WEP and WPA have large overhead due to duplicated encryption. In this paper, we propose a method to reduce this drawback. On this method, a wireless client can choose packet encryption or packet authentication in its wireless LAN automatically depending on whether end-to-end encryption is performed or not. With packet authentication in case that end-to-end encryption is performed, we can improve the communication speed on the wireless environment while preventing invalid access.

## 1. はじめに

無線 LAN は，電波の届く範囲であれば容易にネットワークへのアクセスが可能であるという利便性の面から，近年注目されている．最近では，無線 LAN 製品の低価格化や無線 LAN 内蔵端末（ノート PC など）の普及にともない，利用者の端末から無線 LAN を利用してネットワークにアクセスできるような環境が多くの組織で提供されるようになってきた．

一方，無線 LAN は有線 LAN と比較すると通信速度およびセキュリティの面で問題がある．

まず，通信速度の面では，無線 LAN は比較的低速である点が問題である．現在では，IEEE802.11b[1] よりも高速な規格である IEEE802.11a[2] や 802.11g[3] が普及しており，これらの規格上の最大通信速度は 54 Mbps である．しかし，無線 LAN は有線 LAN と比較するとオーバヘッドが大きく，実質的な通信速度はたかだか二十数 Mbps 程度しかない．

また，セキュリティの面では，第三者への通信内容の漏洩や利用資格がない者によるネットワークの不正利用の危険性があることが問題である．この問題への対策のため，従来は WEP（Wire Equivalent Privacy）[4] と呼ばれる暗号化技術が用いられてきたが，脆弱性を有することが知られており[5),6)]，最近では WPA（Wi-Fi Protected Access）[7] が急速に普及している．

ところで，上記の暗号化技術はいずれも無線区間，すなわち，無線 LAN 端末とアクセスポイント間のセキュリティを確保するためのものである．このため，無線 LAN 端末がアクセスポイントよりも外部のネットワーク上にあるホストなどと安全に通信を行うためには，SSL[8] や SSH[9] などによる end-to-end の暗

†1 岡山大学総合情報基盤センター
Information Technology Center, Okayama University

号化が併用されることが多い．ところが，無線区間の暗号化と end-to-end の暗号化を併用すると，無線区間では二重に暗号化が行われることになるため，無線 LAN の実質的な通信速度がさらに低下するという問題が発生する．

そこで本論文では，無線 LAN 区間で暗号化の代わりにパケット認証を行うことにより，無線 LAN の不正利用を防止しつつ二重暗号化による通信速度低下を回避する手法を提案する．提案手法は，end-to-end 暗号化の有無に応じて無線区間の暗号化とパケット認証を切り替えるものであり，end-to-end の暗号化が行われる場合には，無線区間では暗号化の代わりに処理効率の高いパケット認証を適用することにより，不正アクセスを防止しつつ通信速度を改善することが可能である．

以下，2 章では，パケット認証の必要性について述べる．3 章で試作システムの設計と実装について述べ，4 章では提案手法の有効性を検証するための，実際の無線 LAN 環境で実施した性能評価実験について述べる．5 章では考察と今後の課題を述べ，6 章で本論文をまとめる．

## 2. パケット認証による通信効率の改善手法

1 章で述べたように，無線 LAN 端末が他のホストとの間で end-to-end の暗号化を行うと，**図 1** に示すように，無線区間では二重に暗号化が行われることになる．

これを回避する最も単純な方法は，無線区間の暗号化を放棄し，end-to-end の暗号化のみに頼ることである．しかし，無線 LAN の暗号化機能（WEP および WPA）は，通信内容の漏洩防止だけでなく，不正アクセスの防止も兼ねているため，これを放棄すると二重暗号化による通信速度の低下がなくなる代わりに，任意の第三者によるアクセスポイントへのアクセスを許してしまうことになる．そこで本論文では，不正アクセス防止機能を付与するために，WEP や WPA に代わる機能としてパケット認証を導入し，上述した end-to-end の暗号化機能と併用して，通信性能低下を回避する．

パケット認証は，不正アクセスの防止と通信データの改竄を検出する機能である．具体的には，**図 2** に示すように，送信側がパケットの内容に応じた認証情報を付加し，それを受信側で検証することにより，送信者が正規利用者であると確認できる．認証情報は送信者が持つ秘密情報に基づいて計算されるため，第三者が認証情報を偽造することは困難であり，ネットワークの不正利用を防止することができる．

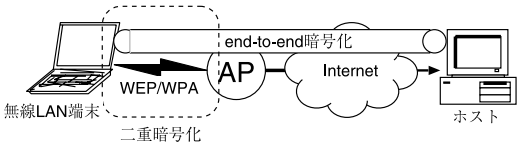


**図 1** 無線区間における二重暗号化
Fig. 1 Duplicated encryption in the wireless network.

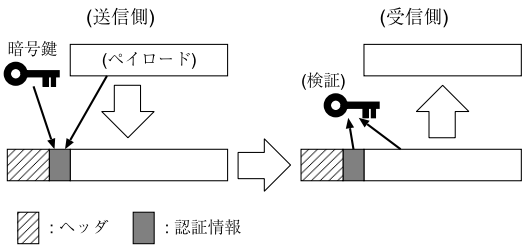


**図 2** パケット認証の処理手順
Fig. 2 An example procedure of packet authentication.

一般に，パケット認証は認証情報の生成時にハッシュ関数を用いるので，認証情報は比較的小さくなる．たとえば，暗号化ライブラリとして広く普及している OpenSSL [10] では，パケット認証のために MD5 [11] あるいは SHA1 [12] を選択可能である．認証情報の大きさはそれぞれ 16 および 20 オクテットであり，しかも，パケットのペイロード部分に対して行われるのは読み出しのみである．一方，WEP や WPA の場合はパケットのペイロード全体が暗号化により書き換えられるため，特に MTU サイズのパケットが送受信されるファイル転送などのように，スループットが重視されるバルク型通信においては，暗号化よりもパケット認証の方が効率が良いと考えられる．

以上のような理由から，end-to-end の暗号化が行われている場合には，WEP や WPA の代わりにパケット認証機能を適用することで，通信性能の改善が期待できる．

## 3. 試作システムの設計と実装

### 3.1 アクセスポイントに必要な機能

提案手法を実現するには，既存のアクセスポイントと無線 LAN 端末に以下の機能を追加する必要がある．

- パケット認証機能
- end-to-end の暗号化検出機能
- （無線区間における）暗号化通信およびパケット認証の切替え機能

これらの機能のうち，パケット認証機能については，SSL などで使われている既存のパケット認証方式が流

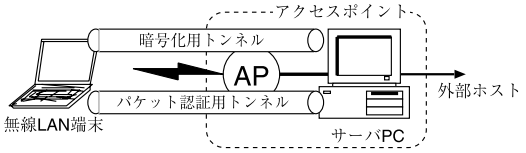


**図 3** システム構成
Fig. 3 The system structure of the proposed method.

用可能であると考えられる．一方，end-to-end の暗号化検出機能と，暗号化通信およびパケット認証の切替え機能については，トランスポート層プロトコルのポート番号や，より上位層で行われる暗号化通信に関するネゴシエーションを監視する必要がある．一部のアクセスポイント製品には，パケットフィルタリング機能を備えているものもあるため，ポート番号単位での切替えは比較的容易に実現できると考えられ，セッション層以上で行われるネゴシエーションを監視するには，IDS などの通信監視技術が応用可能であると考えられる．

しかし，既存のアクセスポイント製品では，機能の追加にハードウェアやファームウェアの変更をともなうため，新たな機能を実装するのは容易ではない．このため，本研究では既存のアクセスポイント製品には変更を加えず，上述した機能を PC で実現するシステムを試作した．以下，試作システムの構成について述べた後，無線区間における暗号化とパケット認証の選択方法と，これに基づく試作システムの実装について述べる．

### 3.2 システム構成

試作システムの構成を**図 3** に示す．図中の “AP” は無線 LAN のアクセスポイントである．3.1 節で述べたように，既存のアクセスポイント製品にパケット認証機能を実装するのは困難であるため，有線 LAN を用いてアクセスポイントにサーバ PC を直結し，アクセスポイントとサーバ PC をまとめて仮想的なアクセスポイントと見なす．以下，アクセスポイントに直結されたサーバ PC を単にサーバといい，サーバよりも外側に位置するホストを外部ホストという．

図 3 の構成において，無線区間の暗号化およびパケット認証は，無線 LAN 端末–アクセスポイント間ではなく無線 LAN 端末–サーバ間で行う．したがって，アクセスポイントは無線 LAN 端末に対してデータリンク層レベルの接続を提供するのみであり，WEP や WPA といった暗号化機能はいっさい利用しない．

一方，サーバが無線 LAN 端末に対して暗号化機能およびパケット認証機能を提供するため，無線 LAN 端末–サーバ間ではあらかじめ 2 つのトンネル用コネクションを確立するものとする．無線 LAN 端末はこれらのコネクションをトンネルとして利用することにより，外部ホストにアクセスすることができる．このとき，一方のトンネル（以下，暗号化用トンネルという）ではパケットの暗号化とパケット認証の両方を行い，他方のトンネル（以下，パケット認証用トンネルという）ではパケット認証のみを行うものとする．無線 LAN 端末は，end-to-end の暗号化を行う場合や，通信内容を秘匿する必要がない場合にはパケット認証用トンネル，それ以外の通信には暗号化用トンネルを経由することにより，二重暗号化を回避することが可能になる．また，これらのトンネルを確立する際に利用者認証を行うことにより，アクセスポイントの不正利用防止だけでなく，ユーザ単位の認証やアクセス制御も実現できる．

### 3.3 無線区間における暗号化とパケット認証の選択方法

前節で述べた 2 つのトンネルを用いることにより，無線 LAN 端末は無線区間においてパケット認証と暗号化のいずれかを選択することが可能であるが，どの通信に対してどのトンネルを経由させるかを決定する仕組みが必要となる．厳密には，end-to-end での暗号化通信に関するネゴシエーションを監視するなどして，その結果に応じて適切なトンネルを選択する必要があるが，より簡便な方法として，試作システムではトランスポート層プロトコルのポート番号に基づいた選択を行う．

たとえば，SSH（22/TCP）や HTTPS（443/TCP）のように，end-to-end の暗号化通信を前提とするサービスや，DNS（53/UDP）のように通信内容の秘匿があまり重要視されないサービスの場合には，パケット認証用トンネルを経由させることにより，二重暗号化を回避することができる．一方，それ以外のサービスについては，暗号化用トンネルを経由させることにより，無線区間における通信内容の秘匿を実現する．

### 3.4 実　　装

試作システムの内部構成を**図 4** に示す．アクセスポイントは暗号化をいっさい行わず，無線 LAN 端末とサーバを接続する HUB と等価であるため，図からは割愛している．

3.2 節で述べたサーバを実装するにあたり，OS として FreeBSD を採用した．その理由は，標準のファイアウォール機能である ipfw [13] を利用すれば，パケットを改変することなく指定したインタフェースに転送することができるためである．

一方，暗号化用トンネルおよびパケット認証用トン

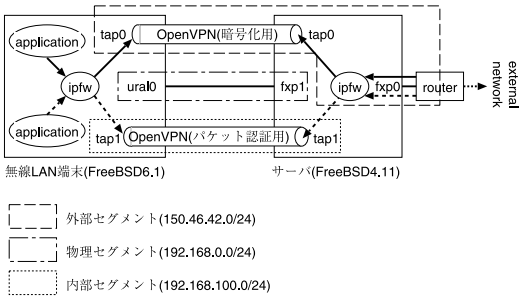


**図 4** 試作システムの内部構成
Fig. 4 Block diagram of the experimental system.

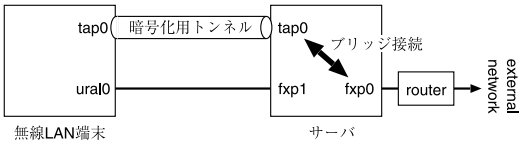


**図 5** 試作システムにおける暗号化用トンネルの構成
Fig. 5 A tunnel for encryption in the experiment system.

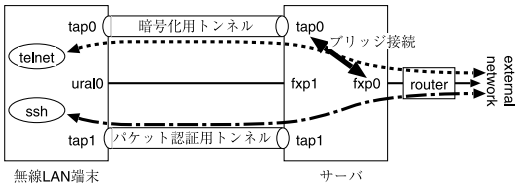


**図 6** 試作システムにおけるパケット認証用トンネルの構成
Fig. 6 A tunnel for packet authentication in the experiment system.

ネルの作成にはフリーの VPN ソフトウェアである OpenVPN [14] を用いた．その理由は，トンネル用コネクションに適用する暗号化通信方式およびパケット認証方式の有無とその種類を個別に指定できるためである．さらに，OpenVPN クライアントでは，各トンネルのエンドポイントは仮想インタフェースとして実現されるため，トンネルの選択が容易であるという利点もある．

以下，暗号化用トンネルの実現方法について述べた後，パケット認証用トンネルの選択方法について詳述する．

なお，図 4 の “ural0” および “fxpX” は，無線 LAN 端末およびサーバの実インタフェースであり，“tapX” は OpenVPN が作成する仮想インタフェースである．以降では，研究室などのネットワークにアクセスポイントを設置するような一般的な運用方法を想定し，サーバが直接接続する外部ネットワーク（暗号化用トンネルを含む）を外部セグメント，無線 LAN 端末およびサーバの実インタフェースを物理セグメント，パケット認証用トンネルを内部セグメントという．

### 3.4.1 暗号化用トンネル

**図 5** に暗号化用トンネルの構成例を示す．一般的な無線 LAN の運用方法では，アクセスポイントを外部セグメントに接続し，アクセスポイントに接続する無線 LAN 端末を外部セグメントの一部として扱う（すなわち，外部セグメントのネットワークアドレスを無線 LAN 端末も共有する）ことが多い．これに対し，試作システムでは，物理セグメントは無線 LAN 端末–サーバ間でのみ通信が行えればよく，end-to-end で暗号化する必要のない通信はすべて暗号化トンネルを経由させればよい．このため，物理セグメントには無線 LAN 端末およびサーバで使用されていない任意のプライベートネットワークアドレスを割り当てるとともに，無線 LAN 端末の仮想インタフェース（tap0）に外部セグメントの IP アドレスを割り当てる．このとき，サーバの仮想インタフェースに外部セグメントの IP アドレスを割り当てると，実インタフェース（fxp0）に割り当てる IP アドレスとネットワークアドレスが競合するため，FreeBSD の bridge 機能[15] を使ってこれらのインタフェースをブリッジ接続する．これにより，サーバの仮想インタフェース（tap0）には IP アドレスを割り当てる必要がなく，暗号化用トンネルをデータリンク層レベルで外部セグメントに直結させることができる．

また，OpenVPN では，トンネル用コネクションの確立および切断時に任意のスクリプトを実行することができる．そこで，無線 LAN 端末では，デフォルト経路を図 5 のルータに設定するようなスクリプトをあらかじめ作成し，暗号化用トンネル確立時に自動的に実行させることにより，無線 LAN 端末から送出される（自分自身以外への）パケットがすべて暗号化用トンネルを経由するようになる．なお，サーバでは仮想インタフェースと実インタフェースをブリッジ接続しているため，（外部セグメントを含む）外部から無線 LAN 端末宛のパケットは暗号化用トンネルを経由することになる．

### 3.4.2 パケット認証用トンネルの選択方法

次に，パケット認証用トンネルの実現方法と，特定のパケットに対してパケット認証用トンネルを経由させる方法を示す．

**図 6** は図 5 にパケット認証用トンネルを追加した例である．内部セグメントであるパケット認証用トンネルでは，無線 LAN 端末–サーバ間でのみ通信できればよいため，物理セグメントと同様に任意のプライベートネットワークアドレスを割り当てればよい（た

```
(a) 無線 LAN 端末
01000 fwd 192.168.100.S tcp from 150.46.42.C1 to any dst-port 22

(b) サーバ
01000 fwd 192.168.100.C2 tcp from any 22 to 150.46.42.C1
```

**図 7** ipfw ルールの例
Fig. 7 Examples of ipfw rules.

だし，物理セグメントとは異なるネットワークアドレスを選択する必要がある）．

図 6 の構成において，end-to-end で暗号化が行われる通信のパケットのみパケット認証用トンネルを経由させるために，ipfw の forward 機能を用いる．これは，特定の条件にマッチしたパケットを，改変することなく指定したポートやインタフェースに転送する機能である．たとえば，無線 LAN 端末から外部ホストに向けての SSH（22/TCP）通信に適用するためには，無線 LAN 端末には**図 7** (a) のような ipfw ルールを設定する．

“192.168.100.S” はサーバの tap1 に付与された IP アドレス，“150.46.42.C1” は無線 LAN 端末の tap0 に付与された IP アドレスである（“01000” は ipfw のルール番号，“fwd” は forward 機能を意味するキーワードである）．このルールは，「送信元が 150.46.42.C1 であり，かつ，任意の IP アドレス（any）の TCP22 番ポート宛てのパケットは，192.168.100.S に転送する」ことを意味する．したがって，無線 LAN 端末から外部に送出されるパケットのうち，宛先ポート番号が 22/TCP のものについては，パケット認証用トンネルを経由するようになる．パケットは改変されることなくサーバに届くため，サーバでは通常の経路制御により外部に転送される．

一方，サーバでは図 7 (b) のようなルールを設定する．“192.168.100.C2” は，無線 LAN 端末の tap1 に付与された IP アドレスである．このルールは，「任意の送信元の TCP22 番ポートから送出されたクライアント宛てのパケットは，192.168.100.C2 に転送する」ことを意味する．したがって，外部ホストから無線 LAN 端末に返される SSH の応答パケットもパケット認証用トンネルを経由するようになる．

ただし，実装の過程において，ipfw の仕様により，ブリッジ接続されたインタフェースに対しては forward 機能が適用されないことが判明した．これは，オリジナルのカーネルを使用する場合は，サーバ側で上述した ipfw ルールを設定しても無視され，外部ホストから無線 LAN 端末への応答パケットが暗号化トンネルを経由してしまうことを意味する．

この問題を解決するため，サーバに対して，FreeBSD のメーリングリストで公開された非公式パッチ[16] を適用した（サーバで使用する FreeBSD のバージョンが無線 LAN 端末よりも古いのは，本パッチが FreeBSD のバージョンに依存するためである）．これにより，ブリッジ接続されたインタフェースに対しても ipfw の forward 機能が適用され，無線 LAN 端末から見て往路だけでなく復路のパケットもパケット認証用トンネルを経由させることが可能となった．

なお，OpenVPN は FreeBSD だけでなく，Windows や Linux など数多くの OS をサポートしている．このため，bridge 機能や ipfw の forward 機能と同等の機能をサポートする OS であれば，サーバを容易に実装することが可能であると考えられる．

## 4. 性能評価

提案手法によって通信性能がどの程度改善されるかを確認するため，試作システムを利用して，無線区間の暗号化と end-to-end の暗号化およびパケット認証のオーバヘッドを実際のネットワーク上で測定し，比較検討を行った．

### 4.1 実験環境

実験環境を**図 8** に示す．無線 LAN 端末とサーバの間にアクセスポイントを配置し，無線 LAN 端末–アクセスポイント間は IEEE802.11g で接続し，アクセスポイント–サーバ間は 100Base-TX の Ethernet で接続した．無線 LAN 端末（Pentium4-3.0 GHz，メモリ 1 GB）は FreeBSD 6.1-RELEASE，サーバ（Pentium4-3.2 GHz，メモリ 512 MB）は FreeBSD 4.11-RELEASE を搭載している．アクセスポイントは Planex 社製 GW-AP54SAG，無線 LAN 端末に装着する無線 LAN アダプタは，BUFFALO 社製 WLI-U2-KG54 である．今回の実験に用いた無線 LAN アダプタは，仕様上，IEEE802.11g と IEEE802.1b のみをサポートすることから，IEEE802.11g を選定した．

無線 LAN 端末およびサーバには，OpenVPN を導入することにより，無線 LAN 端末–サーバ間の暗号

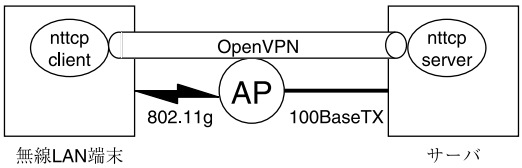


**図 8** 実験環境
Fig. 8 The experiment network.

化とパケット認証の有無が制御可能となり，無線区間における暗号化の有無と組み合わせることにより様々な場合の通信性能が測定できる．図 8 の実験環境において，通信のボトルネックになるのはアクセスポイント–サーバ間ではなく無線 LAN 端末–アクセスポイント間であるため，OpenVPN による暗号化を end-to-end の暗号化，OpenVPN によるパケット認証を無線区間のパケット認証と見なした．さらに，無線 LAN 端末およびサーバにはスループット測定ソフトウェアである nttcp[17] を導入した．nttcp は指定した大きさのデータを nttcp クライアントから nttcp サーバに対して（逆方向も可能）送信するソフトウェアであり，ハードディスクへのアクセスをまったく行わないため，ftp などのファイル転送ソフトウェアよりもスループットを精確に測定することが可能である．

### 4.2 実験方法

二重暗号化による通信性能の低下とパケット認証の有効性を検証するため，無線区間のパケット認証および暗号化について，以下の 6 通りを設けた．

(1) パケット認証および暗号化なし
(2) パケット認証のみ
(3) 64 ビット WEP（以下，WEP64）
(4) 128 ビット WEP（以下，WEP128）
(5) WPA の AES[18] モード（以下，WPA-AES）
(6) WPA の TKIP モード（以下，WPA-TKIP）

いずれの場合も，end-to-end の暗号化，すなわち OpenVPN による暗号化を有効にしている．なお，OpenVPN は暗号化通信時の暗号方式やパケット認証に使用するハッシュ関数を複数サポートするが，予備実験を行ったところ，暗号方式およびハッシュ関数をそれぞれ変更してもスループットに大きな変化はなかったため，暗号方式として AES，ハッシュ関数として MD5 を使用した．

本実験では，上記の場合それぞれにおいて，nttcp クライアントから nttcp サーバに 8 MB のデータを 5 回送信し，その平均スループットを算出した．

### 4.3 実験結果と考察

実験結果を**表 1** に示す．まず，無線区間の暗号化に注目すると，WEP64，WEP128，WPA-AES はいずれもスループットの低下が同程度（10〜13%）であるのに対し，WPA-TKIP の場合は約 27%もの低下が見られる．これは，WEP および WPA-AES はアクセスポイントにおける暗号化および復号をハードウェアで処理しているのに対し，WPA-TKIP は既存の機器に対する互換性重視のため，暗号処理の一部をソフトウェアで実現していることが原因[⋆1]であると推測される．

**表 1** 実験結果
Table 1 The result of the experiment.

| 無線区間の暗号化 | パケット認証 | スループット（Mbps） |
|---|---|---|
| なし | なし | 18.81 |
| なし | あり | 18.47 |
| WEP64 | なし | 16.44 |
| WEP128 | なし | 16.66 |
| WPA-AES | なし | 17.02 |
| WPA-TKIP | なし | 13.71 |

一方，パケット認証によるスループット低下は 2%未満であり，2 章で述べたように，パケットのペイロード全体を書き換える暗号化に比して，小さな認証情報を付加するだけでよいパケット認証のオーバヘッドが小さいことが確認された．

今回の実験環境において，パケット認証により二重暗号化を回避した場合の性能向上は，WEP および WPA-AES の場合が約 9〜12%，WPA-TKIP の場合は約 35%である．厳密には PC やアクセスポイントのハードウェア性能に依存するが，end-to-end 暗号化時には無線区間にオーバヘッドの小さなパケット認証を適用することにより，通信性能が大きく改善される可能性があるといえる．

また，上述した性能評価では，パケット認証処理を PC で行っているのに対し，無線区間の暗号化処理はアクセスポイント製品で行っているため，ハードウェアの性能が異なる．このため，図 8 の無線 LAN 端末において OpenSSL の暗号ベンチマーク機能[⋆2]を実行し，同一ハードウェア上での処理速度を計測した．

計測結果を**表 2** に示す．“MD5” はパケット認証のハッシュ関数として MD5 を用いた場合の処理速度であり，“RC4” は WEP や WPA-TKIP で使用される暗号アルゴリズム，“AES” は WPA-AES で使用される暗号アルゴリズム（鍵長 256 ビット）である．この表から，MD5 は RC4 に対して 1.16〜1.5 倍，AES に

⋆1 WPA-TKIP で使用される暗号アルゴリズムは WEP と同様の RC4 であるため，既存の製品のドライバあるいはファームウェアを変更すれば対応可能である．
⋆2 “openssl speed” コマンドにより実行可能である．

**表 2** openssl の暗号ベンチマーク結果
Table 2 The result of the openssl benchmark.

| データサイズ (bytes) | 処理速度 (MB/s) | | |
|---|---|---|---|
| | MD5 | RC4 | AES256 |
| 1,024 | 130.28 | 112.30 | 41.09 |
| 8,192 | 168.85 | 112.20 | 40.92 |

対して 3〜4 倍の処理速度を持つことが分かる．RC4 は AES よりも MD5 に対する性能差が小さいが，文献 5)，6) で指摘されているように，使用法によっては脆弱性が問題となるため，安全性の面からは AES の利用が望ましいといえる．

表 2 は特定の PC における計測結果であり，実際には，プロトコル処理のオーバヘッドやハードウェア性能の差異により，絶対的な数値を議論することはできない．しかし，同一のハードウェアであれば，パケット認証で使用されるハッシュアルゴリズムと，暗号化で使用されるアルゴリズムとの間には，相対的に表 2 と同程度の性能差があると考えられる．

## 5. 考察と今後の課題

最後に，提案手法に対する性能評価以外の考察と，今後の課題を以下にまとめる．

(1) **提案手法の有用性**

提案手法は，無線区間および end-to-end の二重暗号化を回避するためのものである．しかし，インターネット全体のトラフィック量に対する end-to-end 暗号化通信の割合が不明であるため，この観点から定量的に有用性を議論することは困難である．

一方，最近では，インターネットを介して組織のネットワークに安全にアクセスするための手段として，VPN の利用が増加しており，様々な VPN 構築手法が提案されている．これにより，組織外のホットスポットなどに持ち出した無線 LAN 端末を，仮想的に自組織ネットワークに直接接続しているかのように見せかけることが可能であるが，無線 LAN 端末は暗号化された VPN トンネルを介して自組織の VPN ルータに接続するため，無線区間に WEP や WPA を適用すればほぼすべての通信が二重暗号化されることになる．

したがって，end-to-end の暗号化が行われる通信のうち，特に VPN を利用する場合には，提案手法による二重暗号化の回避が非常に有用であるといえる．

(2) **アクセスポイント製品への組み込み**

無線 LAN のアクセスポイント製品は低価格化が進んでおり，一般家庭向けの製品は 1 万円前後で購入可能である．一方，最近では PC も比較的安価になってきているが，アクセスポイント製品との価格差は依然として大きい．このため，試作システムのようにアクセスポイントとサーバを組み合わせると場合によってはコストの問題が発生し，企業や大学など，ネットワーク環境に比較的コストがかけられる組織に適用範囲が限定される恐れがある．また，一般家庭で普及しているブロードバンド回線（ADSL や FTTH など）では，ブロードバンドルータがアクセスポイント機能を持つものがあり，仮想アクセスポイントのサーバを設置することが困難な場合もある．提案手法を一般家庭などに広く普及させるためには，3.1 節で述べた機能をアクセスポイント製品自体に組み込む方法を検討する必要がある．

(3) **MTU 問題**

図 2 で示したように，パケット認証ではペイロード部分に基づいて計算された値を認証情報としてパケットに付加するため，MTU 超過によるパケットの破損あるいは破棄（MTU 問題）が懸念される．これに対し，試作システムでは，パケット認証処理後のパケットは OpenVPN，すなわちトランスポート層レベルのトンネルを流れるため，MTU 問題は発生しないと考えられる．

一方，提案手法を無線 LAN アクセスポイント製品に組み込む場合には，MTU 問題の発生はパケット認証機能の実装方法に依存する．しかし，無線 LAN の規格である 802.11 の最大ペイロード長は 2,304 バイトであり，Ethernet の 1,500 バイトよりも大きいため，MTU 問題が発生する可能性は低いといえる．

(4) **フラグメントへの対応**

IP データグラムが MTU の異なるリンクを経由する場合，通過するルータにおいてデータグラムの断片化（フラグメント）が行われる場合がある．このとき，トランスポート層のポート番号は先頭フラグメントにのみ含まれるため，end-to-end 暗号化が行われる通信について考えると，試作システムでは，先頭フラグメントはパケット認証用トンネル，後続のすべてのフラグメントは暗号化用トンネルを経由することになる．したがって，通信が阻害される可能性は低いものの，二重暗号化の回避による性能向上が最大限に行われないことが予想される．

対策としては，IP ヘッダの識別子フィールドやフラグメントビットを監視するなどして，同一の IP データグラムに属するフラグメントはパケット認証用トンネルを経由させるといった方法が考えられるが，現在の実装における動作検証やさらなる性能評

価も含め，今後の検討が必要である．

(5) **ヘッダの暗号化**

一般に，end-to-end の暗号化はパケットのペイロードに適用されるため，OpenVPN をパケット認証用トンネルとして利用する場合，カプセル化前のパケットヘッダは平文のままトンネルを流れることになる．通信によってはヘッダ部分の情報（送信元/宛先 IP アドレスなど）も秘匿したい場合があるが，このような通信については暗号化用トンネルを経由させる必要がある（暗号化用トンネルでは，カプセル化前のパケット全体が暗号化される）．

(6) **トンネル選択方法の改良**

3.3 節で述べたポート番号に基づくトンネル選択方法は，実装が容易であるという利点を持つ反面，VoIP の代表的な規格である SIP [19] などのようにポート番号が固定されていないサービスや，STARTTLS [20] のように暗号化通信がセッションの途中から始まるサービスへの対応が困難である．現在の実装では，種類が不明なサービスについてはつねに暗号化用トンネルを経由させるような運用を行えば安全性は確保できる．しかし，安全性と効率を両立させるためには，今後はトランスポート層よりも上位のレイヤにおけるネゴシエーションを監視して end-to-end 暗号化の有無を判定するなど，トンネル選択手法の高度化を検討する必要がある．

また，今回の実装では，パケット認証用トンネルを経由させるための設定を無線 LAN 端末とサーバの両方に施さなければならないため，トンネル選択ポリシの実質的な決定権はサーバ管理者にあるといえる．しかし，通信の安全性に対する要求はユーザごとに異なる場合も考えられるため，無線 LAN 端末のユーザがトンネル選択ポリシを決定できるような方法もあわせて検討したい．

## 6. おわりに

本論文では，無線 LAN での暗号化と end-to-end での暗号化の併用による通信の非効率性を改善するため，end-to-end における暗号化の有無に応じて無線区間での暗号化とパケット認証を切り替えることができるシステムを試作した．また，実際の無線 LAN 環境で性能評価実験を行うことにより，WEP や WPA のオーバヘッドがかなり大きいことを明らかにし，提案手法により通信効率を改善できる可能性を示した．

今後の課題として，暗号化用トンネルとパケット認証用トンネルの選択基準をユーザごとに設ける方法の検討や，無線 LAN アクセスポイント製品への提案手法の組み込みなどがあげられる．

**謝辞** 本研究の一部は，総務省・戦略的情報通信研究開発推進制度（特定領域重点型研究開発プログラム，課題番号 041108001）の補助を受けている．ここに記して感謝の意を表する．

## 参考文献

1) IEEE: 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, IEEE (1999).
2) IEEE: IEEE 802.11a-1999 (8802-11:1999/Amd 1:2000(E)), IEEE Standard for information technology – Telecommunications and Information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Contorol (MAC) and Physical Layer (PHY) specifications – Amendment 1: High-speed Physical Layer in the 5 GHz band, IEEE (1999).
3) IEEE: IEEE 802.11g-2003 IEEE Standard for Information technology – Telecommunications and information exchage between systems – Local and metropolitan area networks – Specific requirements – Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications – Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, IEEE (2003).
4) L.M.S.C. of the IEEE Computer Society: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, IEEE Std 802.11 (1999).
5) Borisov, N., Goldberg, I. and Wagner, D.: Security of the WEP algorithum (2001). http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
6) Fluhrer, S., Mantin, I. and Shamir, A.: Weaknesses in the Key Scheduling Algorithm of RC4. http://www.drizzle.com/˜aboba/IEEE/rc4_ksaproc.pdf
7) IEEE: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i (2004).
8) Netscape Corporation: The SSL Protocol version 3.0 (1996). http://wp.netscape.com/eng/ssl3/draft302.txt
9) Ylonen, T. and Lonvick, C.: The Secure Shell (SSH) Protocol Architecture, RFC4251 (2006).
10) The OpenSSL Project: OpenSSL. http://www.openssl.org/

11) Rivest, R.: The MD5 Message-Digest Algorithm, RFC1321 (1992).
12) NIST: Secure Hash Standard, FIPS PUB 180-1, (1995).
13) Antsilevich, U., Kamp, P., Nash, A., Cobbs, A., Rizzo, L.: ipfw – IP firewall and traffic shaper control program. http://www.FreeBSD.org/cgi/man.cgi
14) Yonan, J.: OpenVPN. http://openvpn.sourceforge.net/index.html
15) Wright, J.: bridge – Bridging support. http://www.FreeBSD.org/cgi/man.cgi
16) ipfw の非公式パッチ. http://lists.freebsd.org/pipermail/freebsd-ipfw/2003-September/000526.html, http://lists.freebsd.org/pipermail/freebsd-ipfw/2003-October/000546.html
17) Bartel, E.: nttcp: New TTCP Program. http://www.leo.org/~elmar/nttcp
18) US National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197 (2001).
19) Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E.: SIP: Session Initiation Protocol, RFC3261 (2002).
20) Hoffman, P.: SMTP Service Extension for Secure SMTP over Transport Layer Security, RFC3207 (2002).

(平成 19 年 6 月 7 日受付)
(平成 19 年 12 月 4 日採録)

**岡山 聖彦**（正会員）

平成 2 年大阪大学基礎工学部情報工学科卒業．平成 4 年同大学大学院基礎工学研究科博士前期課程修了．同年同大学院基礎工学研究科博士後期課程を退学し，同大学工学部助手．平成 6 年奈良先端科学技術大学院大学情報科学研究科助手．平成 10 年岡山大学工学部助手．平成 17 年同大学総合情報基盤センター助手．平成 19 年同助教．博士（工学）．インタネットアーキテクチャ，ネットワーク管理，ネットワークセキュリティの研究に従事．電子情報通信学会会員．

**山井 成良**（正会員）

昭和 59 年大阪大学工学部電子工学科卒業．昭和 61 年同大学大学院博士前期課程修了．昭和 63 年同大学院基礎工学研究科（物理系専攻情報工学分野）博士後期課程退学．同年奈良工業高等専門学校情報工学科助手．同講師，大阪大学情報処理教育センター助手，同大学大型計算機センター講師，岡山大学総合情報処理センター（現，総合情報基盤センター）助教授を経て，平成 18 年より同教授．分散システム，マルチメディアシステム，マルチメディアネットワークの研究に従事．IEEE，電子情報通信学会各会員．博士（工学）．

**河野 圭太**（正会員）

平成 12 年大阪大学工学部電子情報エネルギー工学科卒業．平成 14 年同大学大学院工学研究科（情報システム工学専攻）修士課程修了．平成 16 年同大学院情報科学研究科（情報ネットワーク学専攻）博士課程修了．同年岡山大学総合情報基盤センター助手．平成 19 年同助教．モバイルネットワーク，分散システムの研究に従事．IEEE，電子情報通信学会各会員．博士（情報科学）．