無線 LAN 向けセキュリティプロトコルの一検討

渋谷 尚久　滝 大輔　後藤 真孝　高木 雅裕
株式会社東芝　研究開発センター
{naohisa.shibuya, daisuke.taki, masataka2.goto, masahiro3.takagi}@toshiba.co.jp

IEEE02.11-1999 に従う無線 LAN のセキュリティ機能である WEP (Wired Equivalent Privacy) の脆弱性が指摘され，問題になっている．そこで，セキュリティの強化，スケーラビリティの確保，設定の単純性，既存無線 LAN への適用性の実現を目標として，既存無線 LAN のセキュリティを強化するためのプロトコル (TWSec: TOSHIBA Wireless Security) を設計・試作したので，その概要を報告する．TWSec プロトコルは，主に認証・鍵配布およびレイヤー 2 フレームの機密保護の機能を持つ．また，IEEE802.11 無線 LAN 上での性能評価では，試作した本プロトコル実装が若干のスループットの低下で動作することが可能なことを確認した．

A Study on the Security Enhancement for the Wireless LAN

Naohisa Shibuya　Daisuke Taki　Masataka Goto　Masahiro Takagi
Corporate R&D Center, TOSHIBA CORPORATION

Security issues on the IEEE802.11-1999 wireless LAN standard was disclosed. The WEP, Wired Equivalent Privacy, function have some weakness in its algorithm. Therefore, we propose the new security protocol, TOSHIBA Wireless Security protocol, for the wireless LAN, which realize security enhancement, scalability, easy configuration and easy installation in the existing wireless LAN system. TWSec protocol consist of three main functions, authentication, key derivery and protection of layer 2 frames. We also confirmed that our implementation of the protocol work well on the IEEE802.11 wireless LAN in a little throughput degradation.

1　はじめに

無線 LAN (IEEE802.11) 製品の低価格化や相互接続性の向上によって，家庭やオフィス・公衆スポットエリアといった様々な場所で無線 LAN が使われるようになってきた．一方，IEEE802.11-1999[1] のセキュリティ機能の中核をなす WEP (Wired Equivalent Privacy) の脆弱性がいくつか指摘されており [2]，特に FMS attack[3] では IEEE802.11 のトラフィックを数分〜数十分間程度傍受し，多少の計算をするだけで，傍受者が WEP 鍵そのものを知ることができる．さらに，この方式を実装したソフトウエアがインターネット上で配布されるなど事態は深刻であり，無線 LAN の使用を禁止する企業がでるなど，無線 LAN のさらなる普及を阻害する原因のひとつとなっている．

そこで，筆者等は，

- 強固なセキュリティ
- オフィスや事業所で使える程度のスケーラビリティ
- 管理者・ユーザによる設定の単純性
- 既存無線 LAN システムへの適用の容易性

の実現を目標として，既存無線 LAN のセキュリティを強化するためのプロトコル (TWSec: TOSHIBA Wireless Security) を設計・試作し，その性能評価を行ったので報告する．

2　無線 LAN セキュリティの現状

2.1　IEEE802.11

IEEE802.11 では，認証およびデータフレームの機密保護の機能が規定されている．認証に関しては Open System 認証と Shared Key 認証のふたつの方式があり，前者は実質認証なし，後者は WEP をベースとした Challenge-Response 方式の認証となっている．また，データフレームの機密保護のために WEP による暗号化が行われる．しかし，WEP には既に述べたような脆弱性が存在するため，WEP を用いてもセキュリティを確保したことにはならない．さらに，WEP で使用する鍵の配布方法が規定されておらず，すべての無線 LAN 基地局と端末に WEP の鍵を設定する必要があり，無線 LAN の基地局や端末の数が増大すると鍵の管理が困難になるという運用・管理上の問題も存在する．また，すべての端末に対して同一の WEP 鍵を使用する無線 LAN 基地局の実装が多く，このこともセキュリティのレベルを低下させる原因のひとつとなっている．

2.2　IEEE802.1X

上記のような認証および鍵管理の問題を解決するために，IEEE802.1X[4] の IEEE802.11 への適用が検討されている．これによってより安全な認証および鍵管理が実現されることになるが，データフレームの暗号化はこれまでと同様に WEP により行われるため，この点に関しては根本的な問題の解決には至らない．また，端末を認証するのに EAP-TLS[5] 等の公開鍵暗号を用いることや RADIUS[6] に対応した認証サーバを用意する必要があることなどが導入・管理コストを増大させ，またマルチベンダー間での相互接続性が確立されていない等の理由で，まだ本格的な普及には至っていない．

2.3　IEEE802.11i

現在，IEEE802.11 WG の 11i Task Group では，IEEE802.11 における無線 LAN セキュリティの強化を目的に，新たなセキュリティ機能の標準化を進めている．こ

の中で，レガシーハードウエア，すなわち WEP をベースとした既存無線 LAN 機器で動作可能な TKIP (Temporal Key Integrity Protocol) と，新たなハードウエアの追加が必要となるがより強固な秘匿を実現できる AES (Advanced Encryption Standard) [7] のふたつのデータフレームの暗号化方式が検討されている．同様に，認証や鍵管理に関しても IEEE802.1X をベースとして検討が進められている．しかし，これらの標準化が完了するまでにはまだしばらくの時間を要するため，それまでの間無線 LAN のセキュリティの問題を解決するためのソリューションが必要となる．

3 TWSec プロトコル

1. で述べた目標のもと設計された TWSec プロトコルは，主に以下の機能から構成される．

- 認証・鍵配布
- レイヤ 2 フレームの機密保護

また，図 1 に示すように，TWSec 端末・ブリッジ・認証サーバから構成され，3 者間で認証および鍵配布が行われ，TWSec 端末・ブリッジ間のトラフィックに対して機密保護の機能が実行される．機密保護の機能は，鍵配布で配布された SA (Security Association) をもとに送信すべきデータフレームの暗号化および MIC (Message Integrity Code) の生成・付加が行われる (またその逆)．

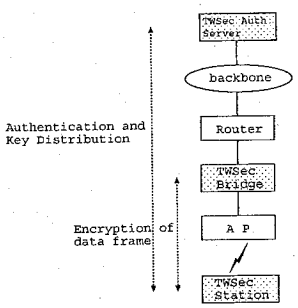

図 1：全体構成

3.1 レイヤ構成

図 3 に TWSec を用いた場合のレイヤ構成を示す．MAC1 = Ethernet, MAC2 = IEEE802.11 とした場合，Ethernet フレーム (図 4(a)) を入力として TWSec レイヤにより機密保護の機能が実行され，IEEE802.11/IEEE802.2/TWSec ヘッダを付加したフレーム (図 4(b)) としてネットワークインタフェースから送信される．よって，元の Ethernet フレームは図 4(b) のフレームの TWSec data payload にカプセル化された形で送信され，元の Ethernet フレームの送信元・宛先アドレス (IEEE802.3 Address) は隠蔽される．また，変換後のフレームの IEEE802.2 ヘッダには LLC/SNAP SAP が含まれ，ベンダー拡張として TWSec プロトコルを挿入する．

TWSec プロトコルで送受信するフレームのヘッダフォーマットは図 2 の通りで，認証・鍵交換で使用されるコントロールフレームおよび機密保護がなされるデータフレームのそれぞれで使用される．Ver には TWSec のバージョン番号が，Typ にはフレーム種別が含まれる．その他のフィールドに関しては後述する．

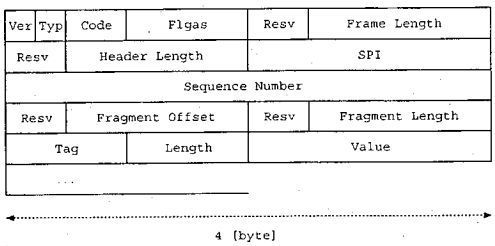

図 2：TWSec Header

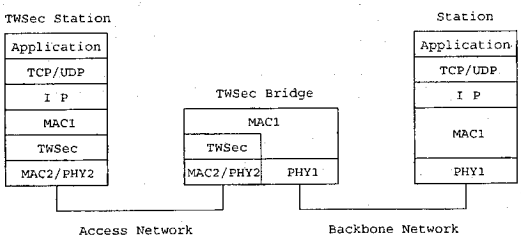

図 3：レイヤ構成

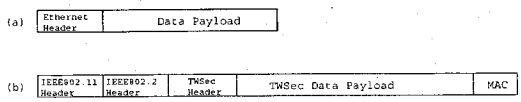

図 4：TWSec フレームへの変換

3.2 認証・鍵配布

認証・鍵配布の機能は一連のコントロールシーケンスで実行され，端末とネットワークの相互認証とデータ交換フェーズで必要となる SA の確立を行う．なお，実装上 SA は手動で設定することも可能であり，その場合は認証・鍵配布のシーケンスは起動されない．本方式では，

1. TWSec 端末毎に異なるユニキャスト通信用 SA を TWSec ブリッジとの間で認証された形で共有
2. TWSec ブリッジ毎に異なるブロードキャスト/マルチキャスト通信用 SA を配下のすべての TWSec 端末間で共有
3. 不正な端末がネットワークにアクセスすることを防止
4. TWSec 端末は不正なネットワークに接続されることを回避
5. 管理に必要な情報および計算の負荷を軽減

の要求条件を満たすことを目的に，Amended Needham Schroeder Protocol[8] をベースとした共通鍵方式の認証・鍵配布プロトコルとなっている．

3.2.1 メッセージシーケンス

図 5 に，認証・鍵交換のメッセージシーケンスを示す．図中のそれぞれの記号は，

A, B: A, B の識別子
Na, Nb: A, B が生成する Nonce
Kas, Kbs: A-S 間，B-S 間で予め共有しているマスター鍵
Kab: A-B 間のセッション鍵
E(Kij: X): Kij により X を暗号化したデータ

を示す．A・B は S を信頼し，それぞれ S と秘密鍵 (マスター鍵) を共有していることが前提となる．また，一連のシーケンスが成功した時点で，A・B は新しい Kab を認証された形で共有する．TWSec プロトコルでは Kab は SA そのものであり，鍵以外の情報も含まれる．また，TWSec 端末からセッションを開始する場合は図 5 に示す NULL フレーム (TWSec ヘッダだけを持つ TWSec プロトコルのコントロールフレーム) を最初に送信し，一方 TWSec ブリッジからセッションを開始する場合は自身の識別子 (ブリッジの IEEE802.3 Address) を含むコントロールフレームを最初に送信する．

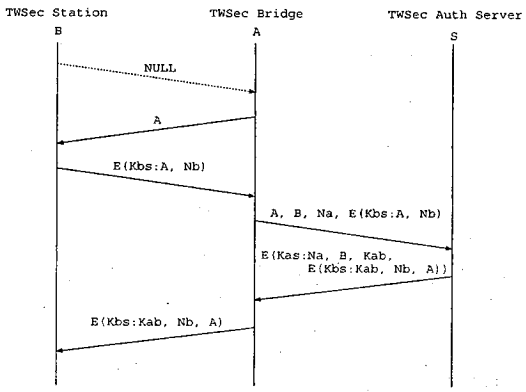

図 5 : 認証・鍵交換のシーケンス

3.3 Security Association

認証・鍵交換では，TWSec 端末毎にユニキャスト通信用およびブロードキャスト通信用それぞれに対して，TWSec 端末から TWSec ブリッジ方向 (上り)，またその逆方向 (下り) のための SA として計 4 種類の SA が配布される (図 6)．下りブロードキャスト通信用の鍵はすべての端末で共有するが，上りブロードキャストおよびユニキャスト通信用の鍵はすべての端末で同一のものである必要はないため，端末毎に異なる鍵を含む個別の SA が配布される．SA には以下の情報が含まれる．

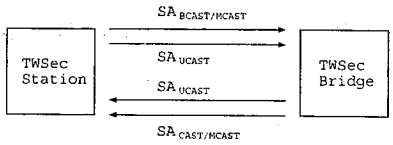

図 6 : Security Association

= IEEE802.3 Destination Address
= IEEE802.3 Source Address
= Security Parameter Index
= Algorithm Set ID
= Authentication Key
= Encryption Key
= Sequence Number
= Sequence Number Bitmap
= Sequence Number Window Size
= Soft Limit (Time, Sequence Number)
= Hard Limit (Time, Sequence Number)
= Start Time

IEEE802.3 Destination/Source Address は TWSec 端末または TWSec ブリッジの IEEE 802.3 Address のいずれかである．Security Parameter Index (SPI) は IEEE802.3 Address と共に SA を一意に示すためのインデックス値である．Algorithm Set ID で使用する認証 (MIC 生成)・暗号化の方式を示し，Authentication/Encryption Key がそこで使用されるセッション鍵である．また，Sequence Number 関連のフィールドは後述の Replay Protection で使用される．Soft/Hard Limit は再認証・鍵配布のための有効期限を示し，Start Time は SA が有効化された時刻を保持する．

3.4 データフレームの交換

3.4.1 送信手順

TWSec データフレームの送信手順に関して述べる．ここでは，TWSec レイヤへの入力は Ethernet フレームであることを前提とし，入力となる Ethernet フレーム全体が TWSec による暗号化の対象 (以後 TWSec plain payload data と呼ぶ) となる．

SA の検索

TWSec 端末・ブリッジでは，送信すべき Ethernet フレームがある場合，宛先となる TWSec 端末またはブリッジの IEEE802.3 Address をキーとして SA データベースから使用可能な SA を検索する．使用可能な SA を検索できなかった場合は，当該フレームを破棄し，再度認証・鍵配布のシーケンスを起動する．

暗号化

検索された SA が示すアルゴリズムを用いて TWSec plain payload data の暗号化を行う．SA が示すデフォルトの暗号アルゴリズムは AES CBC 128 bit であるが，この場合 TWSec plain payload data の先頭に IV (Initialization Vector) を付加し，さらに TWSec plain payload data のサイズが 16 [byte] の整数倍長になるようにパディングを行う．

フラグメント

IEEE802.2 Header + TWSec Header + TWSec data payload + MIC を含むフレーム長が下位レイヤの最大転送サイズを超えた場合に，最大転送サイズ単位にフラグメント処理を行う．実際には，TWSec data payload (IV + 暗号化された TWSec plain payload data + Padding) 以降をフラグメントの対象とする．また，フラグメント後の各フレームにも IEEE802.2 Header と TWSec Header を付加する．

TWSec ヘッダの生成

TWSec Header に関しては以下の通り設定する．

フラグメントが必要であれば，Flags フィールドのフラグメントビットを，Fragment Offset にフラグメント処理後のフラグメントの最初のフレームの TWSec data payload の先頭から当該フレームの TWSec Data Payload の先頭までの長さを，Fragment Length にフラグメント処理後の当該フレームの長さを設定し，逆にフラグメントを行わない場合はこれらのフィールドは 0 に設定する．

Frame Length にはフラグメントする前のヘッダの先頭から MIC の最後のオクテットまでの長さを設定し，Header Length には Ver から最後の TLV 形式のヘッダフィールドまでのヘッダ長を，SPI には使用する SA の SPI の値を，Sequence Number は SA 設定時の初期値 1 から始め，フラグメント前のフレーム毎に 1 ずつ増加させた値を設定する (同一フレームをフラグメントしたフレームは同じ値となる．)．その他の Reserved フィールドは 0 に設定する．

MIC の生成

次に，MIC を計算する．MIC の計算方式と必要な鍵は既に検索した SA により指定される．計算の対象は MIC を除いた全体である．フラグメントが必要な場合は，フラグメントする前のフレームに対して計算し，フラグメント最後のフレームにのみ MIC を付加する．MIC 生成のデフォルトのアルゴリズムとして，HMAC-MD5 [10] を使用する．

フレーミング

TWSec データフレーム を IEEE802.2 の LLC + TWSec SNAP SAP でカプセル化し，更に下位層 (e.g. IEEE802.11) のヘッダを適切に付加して，ネットワークインタフェースから送信する．

3.4.2 受信手順

TWSec データフレームの受信手順に関して述べる．

リアセンブル

受信したフレームの TWSec ヘッダの Flags フィールドにフラグメントビットが立っている場合，MAC レイヤのヘッダに含まれる IEEE802.3 Soruce Address, Destination Address, TWSec ヘッダに含まれる SPI, Sequence Number が全て同じ値を持つフレームを収集する．Frame Length, Fragment Offset, Fragment Length をもとにリアセンブルに必要なフレームがすべて揃ったと判断された場合は，適切な順序に並べかえた後，元のフレームにリアセンブルする．

SA の検索

IEEE802.3 Source Address および TWSec ヘッダの SPI の値をキーとして，SA データベースから使用可能な SA を検索する．SA が検索されなかった場合は，当該フレームを廃棄する．

MIC の検証

検索された SA が示す認証アルゴリズムと認証鍵を用いて MIC を計算する．計算した MIC と受信したフレームに付属する MIC とを比較し，それらが異なる場合には，当該フレームを廃棄する．

Replay Protection

MIC により正当性が検証された TWSec フレームは，更に Replay Protection のための処理を行う．以下のいづれかが成立する場合，Replay されたフレームではないと判断する．

- フレームの Sequence Number がこれまでに受信した最大の Sequence Number よりも大きい．この場合，対応する SA の Sequence Number を更新する．
- フレームの Sequence Number が Sequence Number Bitmap に照らしてこれまでに受信していないものであり，かつ Sequence Number Window Size から計算してウインドウ内に収まっている．

Replay でないと判断された場合は当該フレームの Sequence Number に対応した Sequence Number Bitmap のフラグを立て，逆に Replay であると判断された場合は当該フレームを廃棄する．

復号化

Replay Protection の処理を通過したフレームは，SA で指定されるアルゴリズムと鍵を用いて復号化を行う．AES CBC 128 bit の場合，IV とパディングを取り除いて TWSec plain payload data を取り出す．

フレーミング

TWSec 端末の場合，平文になった TWSec plain payload data に IEEE802.3 Destination Address と Source Address を付けて，Ethernet フレームとして上位レイヤへ渡す．

TWSec ブリッジの場合，ブリッジングすべきポートを検索し，宛先となる端末が接続するポートが TWSec 対応でなければ Ethernet フレームとして，また宛先が他

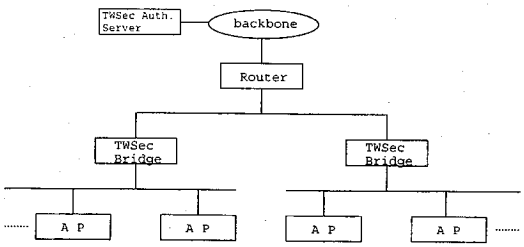

図 7：ネットワーク構成 3

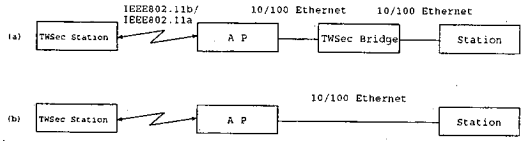

図 8：実験ネットワーク構成

の TWSec 端末であれば再度 TWSec の送信手順を通して TWSec 形式のフレームとして送信する．

3.5 TWSec の導入形態

TWSec プロトコルは無線 LAN 基地局自身に実装することも可能であるが，既存の無線 LAN システムへの適用を考慮すると，図 7 のネットワーク構成のような有線上の MAC ブリッジとしての利用が考えられる．これにより，既存の無線 LAN 基地局に関しては何ら影響を与えることなく，導入することが可能となる．

図 7 は比較的規模が大きなネットワーク構成で，例えばオフィスの各フロアの無線 LAN システム毎に TWSec ブリッジを設置し，TWSec の認証サーバだけ別ノードとして設置する形態である．この場合は，各フロアの無線 LAN セグメントを各一台の TWSec ブリッジの導入で効率的にセキュリティの強化をはかれると共に，各 TWSec ブリッジが利用する認証サーバも一台に集約することで認証情報の管理を一元化することが可能となる．ただし，TWSec 端末がフロアを移動して異なる TWSec ブリッジの配下に移動した場合には，再度新たな TWSec ブリッジを経由して認証を行う必要がある．また，比較的小規模なネットワーク構成において全体として TWSec ブリッジを一台だけ設置するような場合には，TWSec ブリッジと認証サーバとを同一のノードで兼用することも可能である．

4 性能評価

既存の 無線 LAN カードでは，WEP の機能は無線 LAN カードの中でハードウエアまたはソフトウエア (ファームウエア) で実現されているため，使用するホスト PC 環境 (CPU) に依存するところは少ない．一方，本実装は PC の CPU を用いて動作するソフトウエアとして実装しているため，少なからず CPU リソースを消費する．そこで，本章では WEP と比較した場合の TWSec 使用時の処理遅延とスループットに関する評価を行う．

4.1 実験ネットワーク構成

図 8 に示すネットワークにおいて実験を行った．無線区間は IEEE802.11 a/b，有線区間は 10/100 [Mbps] 対応の Ethernet である．(a) が TWSec を用いた場合，(b) が TWSec を用いない場合のネットワーク構成である．無線 LAN 基地局と TWSec 端末間の距離は，見通しで約 1 メートルで，無線のチャネルは周囲で使用されていないものを使用した．

使用機器一覧を表 1 に示す．表中の ORiNOCO 製品が IEEE802.11b 対応機器，ICOM 製品が IEEE802.11a 対応機器となる．

表 1：使用機器一覧

ノード名	OS	使用機材
TWSec 端末	FreeBSD 4.4S	TOSHIBA SS3440 ORiNOCO Silver
	Windwos XP	TOSHIBA Portege 4010 ICOM SL-50
無線 LAN 基地局	—	ORiNOCO AP-1000 ORiNOCO Silver
	—	ICOM SR21-BB ICOM SL-50
TWSec ブリッジ	RedHat 7.2	組み立て PC (PIII-866)
対抗端末	FreeBSD 4.5R	TOSHIBA Portege 2000

4.2 測定項目

図 8 に示すネットワーク上の TWSec 端末・相手端末間で，

- ping によるラウンドトリップタイム
- netperf [1] による TCP バルクデータ伝送時のスループット

の測定を行った．前者は IEEE802.11b 上でのみ，後者は IEEE802.11a/b のそれぞれの無線 LAN 上で測定を行った．TWSec 使用時は WEP を無効に，また現状の無線 LAN 機器は 40/104 [bit] の複数のビット長の WEP に対応したものが多いが，測定は 40 [bit] の場合のみ行った．

4.3 ラウンドトリップタイムの測定

TWSec 端末・対抗端末間で，ping によるラウンドトリップタイムの測定を行った．ping 送信時の ICMP データサイズをそれぞれ 64, 128, 256, 512, 1024, 1472 [byte] [2] と変化させ，10 [msec] 間隔で 100 個の ICMP パケットの送受信を行った．

測定結果を図 9 に示す．暗号化なし/TWSec/WEP のいづれの場合も，データサイズが大きくなるにつれラウンドトリップタイムが大きくなっているが，それぞれの間で差はほとんど見られない．また，TWSec/WEP はデータサイズが大きくなるにつれラウンドリップタイムが線形に増加しているが，暗号化を行わない場合に 512 [byte] で多少線形性が崩れている．以上の結果より，TWSec を用いた場合に大きな遅延が入ることはないことが確認された．

[1] http://www.netperf.org/

[2] Ethernet 上を流れるデータはこれに ICMP ヘッダ 8 [byte], IP ヘッダ 20 [byte], Ethernet ヘッダ 14 [byte] の計 42 [byte] が付加される．

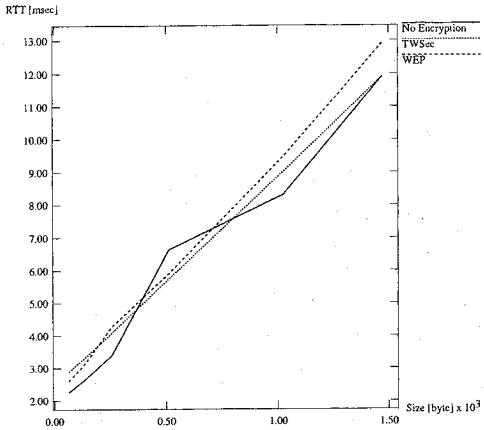

図 9：ラウンドトリップタイム

4.4 スループットの測定

TWSec 端末・対抗端末間で，netperf による 30 秒間の TCP バルクデータ伝送を各 10 回行った．データの伝送方向は，TWSec 端末から対抗端末へ，またその逆方向の 2 通りである．それぞれの端末の TCP の各種パラメータは OS のデフォルトの状態である．

4.4.1 IEEE802.11b

IEEE802.11b を用いた場合のスループット測定結果を，表 2 に示す．暗号化なし/TWSec/WEP のいづれの場合も，データの送受信方向によるスループットの顕著な差は見られない．また，暗号化の処理を行わない場合と比べて，TWSec または WEP のいづれかを使用した場合に元の 70 〜 80 [%] 程度のスループットに劣化することが確認された．これは，今回用いた IEEE802.11b 無線 LAN 機器が TWSec の場合と同様にソフトウエアにより処理されているためであると考えられる．

表 2：平均スループット [Mbps] — **IEEE802.11b**

送信方向	暗号化なし	TWSec	WEP 40bit
上り	4.69	3.33	3.46
下り	4.41	3.33	3.71

4.4.2 IEEE802.11a

IEEE802.11a を用いた場合のスループット測定結果を，表 3 に示す．暗号化なし/WEP の場合は，上りに比べて下り方向のスループットが若干高いが，TWSec を用いた場合は方向によらず同程度のスループットとなっている．また，WEP を用いた場合は暗号化を行わない場合と同程度のスループットを維持できているが，TWSec を用いると元の 80 [%] 弱程度のスループットに劣化することが確認された．これは，今回用いた IEEE802.11a 無線 LAN 機器がハードウエアにより WEP を処理しているのに対して，TWSec の場合はすべてソフトウエア処理しているためであると考えられる．

表 3：平均スループット [Mbps] — **IEEE802.11a**

送信方向	暗号化なし	TWSec	WEP 40bit
上り	20.67	16.71	20.61
下り	22.56	16.25	22.14

5 まとめ

今回，IEEE802.11-1999 の無線 LAN のセキュリティの問題を解決する新たなセキュリティプロトコル (TWSec: TOSHIBA Wirelss Security) を提案し，その有効性を検証した．その結果，試作した本プロトコル実装を用いることにより，実用的なスループットを維持したまま大幅にセキュリティの強化をはかれることを確認した．また，本プロトコルは既存の無線 LAN システムを変更することなく容易に導入することが可能等，様々な特徴を持つことも述べた．

今後は，本プロトコルの安全性等さらなる評価とともに，実装上または機能的な問題点等を明らかにし，さらなる改善を計っていく．

参考文献

[1] “Wireless LAN Medium Access Control (MAC) and Physical (PHY) Specifications”, ANSI/IEEE Std. 802.11 1999 Edition, August 1999

[2] N.Borisov et al, “Intercepting Mobile Communications: The Insecurity of 802.11”, MobiCom2001, July 2001

[3] S.Fluhrer et al, “Weakness in the Key Scheduling Algorithme of RC4”, 8th Annual Workshop on Selected Areas of Cryptography, August 2001

[4] “IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control”, IEEE-SA Standards Board, June 14, 2001.

[5] Aboba, B. and D. Simon, “PPP EAP TLS Authentication Protocol”, RFC 2716, IETF, October 1999.

[6] C. Rigney, et al, “Remote Authentication Dial In User Service (RADIUS)”, RFC2865, IETF, June 2000

[7] “Specification for the Advanced Encryption Standard (AES)”, FIPS0197, November 2001

[8] R.M.Needham and M.D.Schroeder, “Authentication Revisited”, Operating Systems Review, Vol21, No.1, P.7, January 1987

[9] R. Rivest, “MD5 Digest Algorithm”, RFC1321, IETF, April 1992

[10] H. Krawczyk, M. Bellare and R. Canetti, “HMAC: Keyed-Hashing for Message Authentication ”, RFC2104, IETF, February 1997