分散システム／インターネット運用技術 21－3
（2001．5．25）

無線LANにおける利用者認証機構

石橋勇人[1]　山井成良[2]　森下英夫[3]　森 俊明[3]　安倍広多[1]　松浦敏雄[1]
[1]大阪市立大学 学術情報総合センター
[2]岡山大学 総合情報処理センター
[3]（株）ステラクラフト

概　要

IEEE 802.11b[1] 準拠の無線 LAN では，不正な利用者によるアクセスを防止するために ESS ID や MAC アドレスによる制限が行われる．しかし，これらの値は電波を傍受することによって容易に判明するため，あまり有効ではない．また，WEP による暗号化を行ったとしても，正規の利用者による別の利用者へのなりすましに対しては効力がない．我々は，文献 [2] において，特定多数の利用者が自己の計算機を接続して使用する情報コンセントにおける MAC アドレス等の事前登録を必要としない利用者認証機構の実現方法を明らかにしたが，本研究では，暗号化通信路を用いることによって同機構を無線 LAN 環境へと応用し，無線 LAN 環境における利用者認証機構が実現できることを示す．また，システムの試作によりその有効性を確かめている．

An Authentication System for Secure Wireless Communication

Hayato Ishibashi[1], Nariyoshi Yamai[2], Hideo Morishita[3], Toshiaki Mori[3],
Kota Abe[1] and Toshio Matsuura[1]
[1]Media Center, Osaka City University
[2]Computer Center, Okayama University
[3]Stellar Craft, Inc.

Abstract

In wireless LAN systems based on IEEE 802.11b, access restriction by an ESS ID and/or MAC addresses is used to prevent unauthorized network access. However, these are easily obtained by interception. Though WEP is one countermeasure for interception, it is not able to prevent false statement of source addresses by legal users. In [2], we have revealed a method to implement an authentication mechanism for LAN sockets where only approved users are able to use and MAC addresses are not required to register in advance. In this paper, we propose an authentication mechanism for wireless LAN systems that is based on the method above. In order to apply the method, encrypted connections are introduced for identifying each client. Also, we describe the prototype system we have implemented.

1 はじめに

昨今の無線 LAN 製品の普及にともなって，利用者の計算機から無線を利用してネットワークアクセスを行うニーズが高まっている．IEEE 802.11b[1] のような無線 LAN システムでは，キャリヤとして電波を使用しているところから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．これは大きな長所でもあるが，同時に悪意を持った人間によるネットワークへの不正アクセスを容易なものとする．悪意を持った，あるいは悪意はなくとも利用資格がない者によるネットワークアクセスを防止するためには，何らかの認証機構が必要である．

無線 LAN においてネットワークアクセス可能な計算機を限定する手段として，ESS ID によるアクセス制限やアクセス可能な MAC アドレスを登録したもののみに制限することが行われる．この場合，ESS ID や MAC アドレスが認証キーの役割を果たすことになるが，ESS ID や MAC アドレスは電波を傍受するだけで内容が判読可能であるため，これらの方策はあまり安全とは言えない．

そこで，WEP （Wired Equivalent Privacy）と呼ばれる暗号化方式が用いられるが，WEP は共有鍵方式であるために鍵の配布方法が問題となる．また，特定のアクセスポイントに接続するすべてのクライアントは同一の鍵を共有するため，のべ利用者数が非常に多い大学のような環境では，鍵の値を秘匿することは実質的に困難である．

ところで，ネットワークアクセスに対する認証機構が有効性を発揮するためには，認証を受けていない利用者の計算機から発信されたパケットを排除できることが必要であり，そのためには個々のパケットの送信元の識別が重要である．

しかし，通常の無線 LAN システムでは，(WEP の如何にかかわらず) 100BaseTX でリピータハブに接続されたネットワークと同様に，各クライアント計算機が送信したパケットがどの計算機から送信されたものであるかをデータリンク層以上から区別する手段は存在しない．一般には IP アドレスや MAC アドレスが送信元計算機の識別に用いられるが，これらの値は利用者側の設定によって詐称することが可能であり，確実な識別手段ではない．

我々は，このような無線 LAN 環境において確実に認証とアクセス制御を実現する認証機構を開発し，システムを試作した．本システムは，(1) 不正アクセスの防止，(2) 利用者ごとのアクセス制御，(3) 電波傍受による通信内容の露見防止，を実現することができる．このうち，(1) には，(1a) 利用資格のない利用者によるアクセスの防止，(1b) 送信元を詐称したアクセスの防止，の 2 つを含んでいる．また，(3) は暗号化技術によって実現しているが，秘密鍵の事前配布は不要である．

本システムの利用にあたっては，利用者の ID とパスワードを登録する必要があるが，通常は既存の情報が利用できると考えられる．また，それ以外に利用者の計算機の MAC アドレスをシステムに登録したり利用者に対して IP アドレスを固定的に割り当てたりする必要はなく，管理が容易である．

以下では，この認証機構とその実現について述べる．

2 提案する利用者認証機構

我々は，文献 [2] において，特定多数の利用者が自己の計算機を接続して使用する情報コンセントにおいては，利用者の計算機の IP アドレス，MAC アドレスだけでなく情報コンセントの接続ポートという不変の識別子を含めて利用者を管理することによって，IP アドレスや MAC アドレスの偽造にも耐えることができる安全な情報コンセントシステムの構築が可能であることを示した（このシステムを LANA システムと呼ぶ）．LANA システムでは，利用者ごとにアクセス可能なホストやサービスを限定するなどのアクセス制御も実現している．そこで，同システムを無線 LAN 環境に応用することによって，利用者認証とアクセス制御を実現することが考えられる．

ところが，無線 LAN システムにおいては，物理的な “ポート” が存在しないために個々のクライアント計算機を確実に識別する手段がない．このため，クライアント計算機 A から発せられたあるパケットが，間違いなく A のものである（A のものであるかのごとく偽造されていない）ことを確認することは困難である．

本稿において提案する利用者認証機構は，文献 [2] の方式を無線 LAN においても適用できるよう拡張したものである．このためには，無線 LAN における個々のクライアント計算機から送信されるパケットの送信者を確実に識別できる必要がある．すなわち，有線 LAN における物理的な “ポート” に代わ

る一意な（しかも利用者自身が変更できない）識別子を何らかの形で用意しなければならない．

そこで，本稿において提案する認証機構では，利用者の計算機と外部ネットワークとのゲートウェイとなる計算機との間に張った論理的な“コネクション”を用いて利用者の計算機を識別する．

具体的には，認証システムと各クライアント計算機の間に暗号化された TCP コネクションを張り，外部ネットワークへアクセスしようとするクライアント計算機はそのコネクションを通してパケットを送受信する．コネクションの確立に先だって利用者の認証を行うので，そのパケットを送信した利用者は特定可能であり，パケットの送信元アドレスが偽造されていないことを確認することができる．また，暗号化コネクションをハイジャックすることは極めて困難であるため，他の利用者がそのコネクションを利用して認証された利用者になりすますことも防止できる．

3 システムの概要

本方式の概要を図 1 に示す．クライアント計算機は無線 LAN によってアクセスポイント（AP）経由で認証システムに接続される．認証システムは，利用者の認証機能を持つとともに，クライアント計算機と外部のネットワークとの間でパケットを中継し，同時にアクセス制御を行う．アクセス制御には，不正アクセスの防止と利用者ごとのアクセス範囲の制限を含んでいる．

利用者の計算機を接続するにあたって，システムは次のように動作する．

1. 利用者がクライアント計算機を無線 LAN に接続する（電源を入れる，インタフェースカードを挿入する等）．
2. IP アドレス割り当てサーバはクライアント計算機に IP アドレスを割り当てる．
3. クライアントは認証システムに対して暗号化コネクションを張る（たとえば，SSL によるコネクション）．
4. 暗号化コネクション上で（ユーザ名/パスワード等により）利用者を認証する．
5. 認証に成功すると，認証システムはそれ以降対応する暗号化コネクションを通して送られてきたパケットを外部ネットワークへ中継する．

4 システムの実装

4.1 試作システムの構成

提案する方式に基づく試作システムの構成を図 2 に示す．大きな機能ブロックとして，(有線) LANA システムと同様に LANA フィルタ，LANA サーバ，DHCP サーバ，RADIUS サーバから構成されている．以下では，本システムを WILL（Wireless LANA）システムと呼ぶことにする．

無線 LAN への対応にあたって，試作システムの実装では，暗号化コネクションとして SSL コネクションを，クライアント計算機と外部ネットワークの通信のために SSL 上の PPP コネクションを使用している．そこで，今回 LANA フィルタのサブシステムとして SSL サーバおよび PPP サーバを導入した．また，クライアント計算機上では WILL クライアントを動作させる．

次に，各構成要素について順に述べる．

4.1.1 LANA フィルタ

フィルタ部 LANA フィルタは，クライアント計算機と WILL システムの各サーバや外部ネットワークの間の通信を中継し，必要なアクセス制御を行う．アクセス制御には，次のようなものがある．

1. DHCP サーバとクライアント計算機の間の DHCP による通信は常に中継する（図 2 の a）．
2. クライアント計算機と LANA フィルタの SSL サーバ部との間の SSL コネクションは常に中継する（図 2 の b）．
3. SSL コネクションを経由した LANA サーバとの認証情報のやり取りは常に中継する（図 2 の c）．
4. クライアント計算機の認証に成功した後は，PPP コネクションを通して送られてきたパケットを外部ネットワークへ中継する．この際，送信元アドレスのチェックと，利用者に応

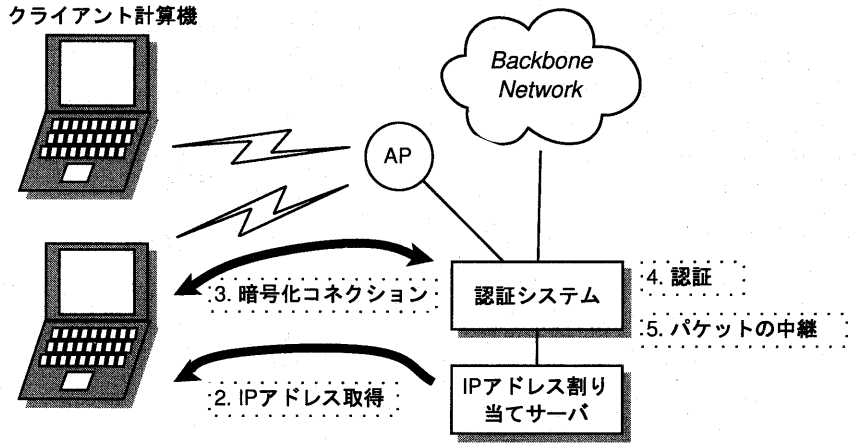

図 1: 動作の概要

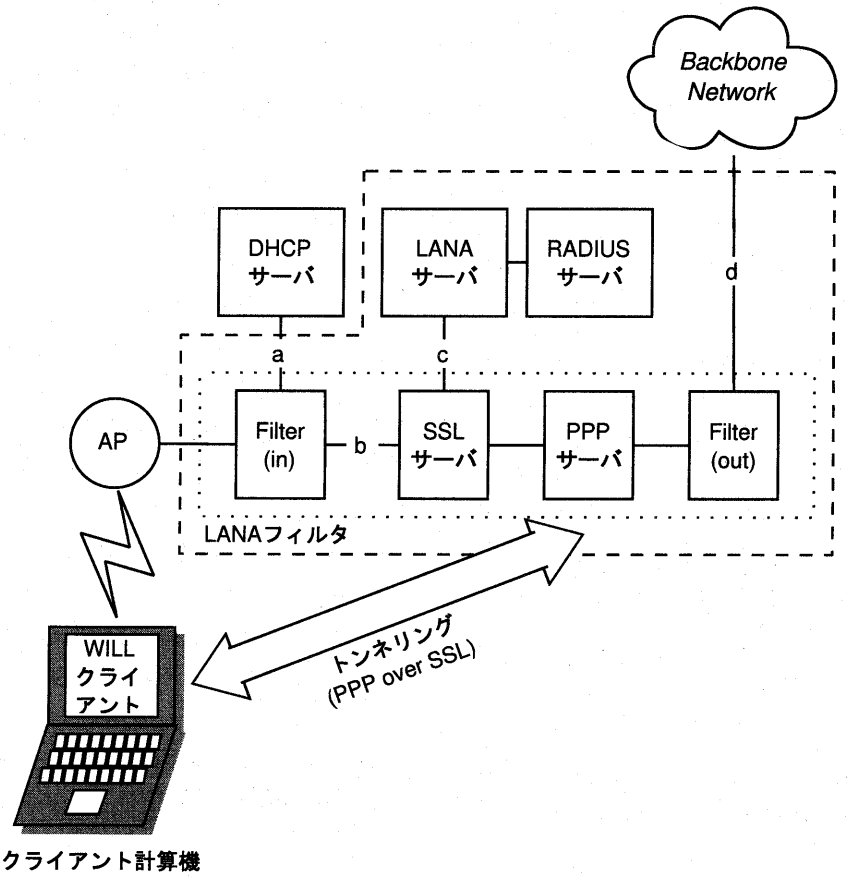

図 2: システム構成

じて定義されたアクセス制御を行う（図2のd）.

1〜3は入力フィルタ（図2におけるFilter(in)），4は出力フィルタ（図2におけるFilter(out)）において行う処理である.

SSLサーバ部 クライアント計算機からの接続を待ち，接続があればLANAサーバへ中継する．LANAサーバにおいて認証に成功すると，以降の通信をPPPサーバへと中継する.

PPPサーバ部 WILLクライアントとの間のSSLセション上でPPPコネクションを確立する.

4.1.2 LANAサーバ

RAIDUSサーバと連携した利用者の認証やその後の利用者管理（ログイン，ログアウトの情報），LANAフィルタに対するアクセス制御の指示を行う．従来のLANAシステムではクライアント計算機の（IPアドレス，MACアドレス，IEEE 802.1Q VLAN ID）と利用者IDを対応づけて管理していたが，WILLでは（IPアドレス，MACアドレス，PPPコネクション）と利用者IDを対応づけて管理する.

4.1.3 WILLクライアント

起動時にLANAフィルタに対してSSLコネクションを確立する．その後LANAサーバからの要求に応じて利用者から認証情報を獲得し，送信する．認証に成功した場合はSSLコネクション上でPPPコネクションを確立し，以降の通信をPPPコネクション経由で行うようにする.

4.1.4 DHCPサーバ

無線LAN上でIPアドレスを割り当てるDHCPサーバには，一般に広く配布されているISC DHCP[3]サーバを利用しているが，特に制限はない.

4.1.5 RADIUSサーバ

利用者の認証とアカウンティングを行うRADIUSサーバも，やはり一般に配布されているDTC RADIUS[4]を利用している.

4.1.6 無線LANアクセスポイント

IEEE 802.11b準拠の無線LANシステムを使用している．無線による通信と有線のEthernetとの間でMACブリッジとして動作するものである.

4.2 動作の詳細

WILLシステムの具体的な接続シーケンスを図3に示す．図3の詳細は次の通りである.

1. DHCPによるIPアドレスの割り当て

   クライアント計算機は無線LANのアクセスポイントを経由し，DHCPサーバにIPアドレスを要求する．このIPアドレスはSSLによる通信のためにだけ使用される．したがって，ここで取得したIPアドレスからは，LANAフィルタのSSL用ポート番号にのみアクセスできるよう制限しておく.

2. SSLコネクションの確立

   WILLクライアントはLANAフィルタのSSLサーバ部とSSLコネクションを確立し，SSLコネクション経由でLANAサーバと接続する．LANAサーバはクライアントに利用者の認証情報を要求し，クライアントは利用者にユーザ情報（ユーザ名とパスワードなど）の入力を促す．このセションは暗号化されているので，この際には平文のパスワードを送信しても問題はない．得られたユーザ情報はLANAサーバへ送られ，LANAサーバはRADIUSサーバを用いて認証を行う．成功すれば次のフェーズに移行するが，認証に失敗した場合はコネクションを切断する．認証に成功した場合にはRADIUSのアカウンティングが開始される（ログインの記録）.

3. PPPコネクションの確立

   次に，LANAフィルタは，SSLコネクションをPPPサーバへと接続する．クライアント側でも同様にSSLコネクションをPPPクライアントへ接続する.

4. PPPによるIPアドレスの割り当て

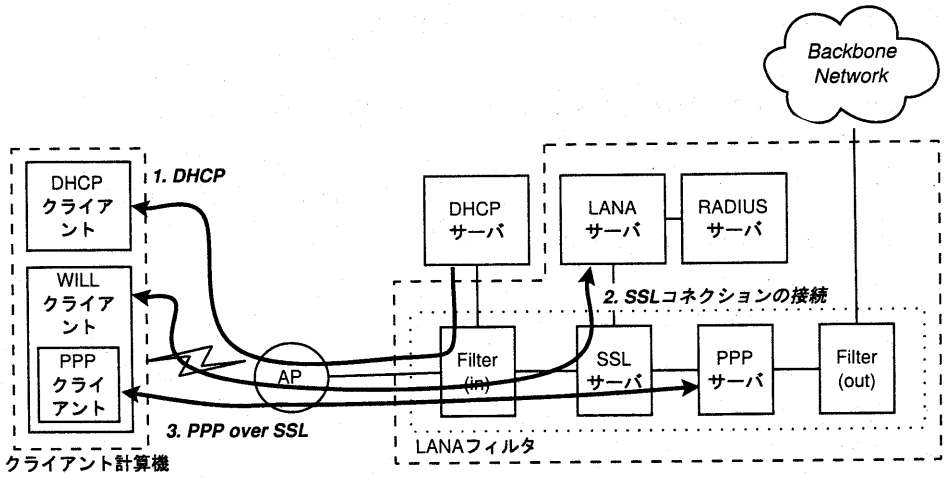

図 3: 接続シーケンス

PPP セションが開始されると，クライアントは IPCP[5] によって IP アドレスを取得する．外部ネットワークとの接続時に NAT を利用しない場合には，この IP アドレスが実際に外部と通信する際に使用されることになる．

5. ルーティングテーブルの変更

   クライアント側ではデフォルトルートを PPP コネクションへと向けることによって，外部ネットワークへの到達性を確保する．これによって，クライアントからの通信は暗号化された PPP コネクションを通して安全に行われることになる．

   PPP コネクションを通して LANA フィルタへと流れてきたパケットは，利用者ごとのアクセス制御を行うフィルタを経由して外部ネットワークへと中継される．この際，送信元 IP アドレスのチェックも行う．

6. クライアントの終了

   クライアント側が PPP コネクションを切断するか，あるいは，一定時間パケットの送信がない場合には，LANA サーバは RADIUS サーバにアカウンティングの終了を告げ（ログアウトの記録），PPP および SSL のセッションを終了する．LANA フィルタはクライアントのフィルタリング情報を削除する．

5 おわりに

本稿では，既存の無線 LAN 環境において認証とアクセス制御を可能とする機構を提案し，その実装である WILL システムについて述べた．本システムによって，多数の利用者が入れ替わり利用するような環境でも確実に利用者を認証し，不正アクセスを防止することができる．

参考文献

[1] IEEE: *Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*, IEEE (1999).

[2] 石橋勇人, 山井成良, 安倍広多, 阪本晃, 松浦敏雄: 利用者ごとのアクセス制御を実現する情報コンセント不正利用防止方式, 情報処理学会論文誌, Vol. 42, No. 1, pp. 79–88 (2001).

[3] Internet Software Consortium: ISC DHCP, `http://www.isc.org/dhcp.html`.

[4] デジタルテクノロジー (株): DTC Radius 2.03, `http://www.dtc.co.jp/Radius2.0/`.

[5] McGregor, G.: The PPP Internet Protocol Control Protocol (IPCP), RFC 1332 (1992).