2003－DPS－113 (9)
2003／6／20

ユーザビリティを考慮した安全な無線 LAN システムの提案

古森 貞† 齋藤孝道††

無線 LAN 製品の普及に伴い，無線 LAN システムの安全性に対する注目が集まっている．とりわけ，IEEE802.11a，802.11b に準拠した製品にはセキュリティ上の問題を解決するため，より安全な無線 LAN システムの研究が盛んに行われている．しかしながら，これまで提案されているシステムでは，安全性もしくは通信効率を主に追求した結果，ユーザビリティの低下を招いてしまっている．そこで，本論文では，ユーザビリティの向上と安全な無線 LAN の構築を目指したシステムを提案する．提案システムでは SSL (Secure Socket Layer) によって無線区間の安全性を確保し，SSL のサーバ認証を利用する read only モードと，SSL の相互認証を利用する full access モードを用意する．read only モードは，ユーザの事前登録が不要で，匿名でサービスを享受できるモードであり，限られたサービスのみをユーザに提供することで，提案システムの安全性を確保する．full access モードでは，ユーザは，SSL の認証時にサービスを提供する主体に対して，ID のかわりに認証済みの権限を記述したチケットを提出することによって，匿名で相互認証をすることができ，安全にサービスを享受できる．そのため，提案システムは，匿名で気軽にサービスを受けたいユーザ側と安全にサービスを提供したいサーバ側の双方の要求を満たす仕様になっている．

A Secure Wireless LAN System for Supporting Usability

Tadashi KOMORI † and Takamichi SAITO††

A wireless LAN system, based on IEEE802.11a or 802.11b, has a lot of drawbacks for security. Some secure wireless systems have already been proposed. However, they are not convenient for a user to utilize thier systems, since the user has to register his / her ID or public key on their systems. In this paper, we propose a new secure wireless LAN system for supporting usability.

1. はじめに

近年，無線 LAN が急速に普及しつつある．以前は課金制で利用できた無線 LAN を，最近では無料で提供するところも出現してきた．無線 LAN の安全性に関しては，これまで様々な研究[1),2)]がされており，その脆弱性が問題視されている．

そのため，安全性を考慮した無線 LAN のシステム[3)~5)]が多く研究されている．それらのシステムはセキュリティを向上させるため，システムを利用するユーザに対してユーザ固有の情報 (ID (システム毎のユーザ識別子) やパスワード，ユーザの公開鍵・秘密鍵など．以降，**アカウント情報**と呼ぶ) を登録させ，相互認証を行う．このとき，ユーザの認証にアカウント情報を利用するため，常にユーザを特定することになる．ところが，昨今，個人情報の取り扱いに敏感な世相を反映して，アカウント情報を登録せずに匿名で利用できるサービスの要求が高まってきている．例えば，イベントの特設会場などで無線 LAN を提供する場合，ネットワークの利用を希望するユーザに対して，個々にアカウント情報を発行するのは大変な手間となる．また，例えば，ホットスポット☆において，ホームページなどの参照のみを希望するユーザに対して，アカウント情報を登録させるのは，そのユーザにとって負担である．さらに，あるユーザが，同一のシステムが導入された複数の異なるネットワークを利用する場合には，そのユーザはそれらのネットワークごとにアカウント情報を登録しなければならず，より一層敬遠されやすくなる．ユーザビリティとセキュリティはトレードオフではあるが，ユーザビリティを無視したセキュリティ機能はしばしば利用されない傾向にある．

そこで，本論文ではユーザビリティを重視した安全な無線 LAN システムの構築を目指す．すなわち，提案システムでは，匿名で気軽にサービスを受けたいユーザ側と安全にサービスを提供したいサーバ側の双方の要求を満たすシステムの構築を目標とし，read only モードと full access モードの 2 種類のモードを用意する．read only モードは，ユーザが予めユーザ個別のアカウント情報を登録するなどの煩わしい手続きを行わずに，利用方法を限定することで，安全に無線 LAN を利用できるモードである．すなわち，ユーザは，Web ブラウザを用いてホームページの参照のみを行いたいときに，このモードを利用する．ユーザには外部ネットワークへの接続プロトコルとして HTTP (Hypertext Transfer Protocol) と，通信相手と End-to-End にセキュリティを確保するプロトコル (例えば SSH (Secure SHell)) のみを提供する．一方，full access モードは，権限証明書 (後述) を用いたアクセス制御を行う公開鍵基盤である SPKI (Simple Public Key Infrastructure)[6),7)] を利用することで，チケット (後述) を持つユーザに，外部ネットワークへの無制限のアクセスを許可するモードである．筆者らのグループはすでに文献[8),9)]において，SPKI に SSL (Secure Socket Layer) を適用し，匿名アクセス制御を提供するシステムを提案した．当該モードは，このシステムを無線 LAN に適用したことによって，ユーザはチケットの有効期限内であれば，何度でも提案システムを利用できるようになる．さらに，提案システムを導入しているネットワークが複数存在し，互いに連携し合っている場合には，それらの全てのネットワークを利用することができるようになる．そのため，このモードはモビリティに優れたモードとなっている．

提案システムでは SSL を利用することで，無線区間のセキュリティを確保する．すなわち，read only モードでは SSL のサーバ認証モードで，full access モードでは SSL の相互認証モードでセキュリティを確保する．これまでの既存の無線 LAN のシステムでは，常にユーザの認証を求めることで安全性を確保していた．これに対し，本論文では，ユーザの特定をせずとも無線 LAN のシステムを安全に提供できることを示す．提案システムでは，read only モードで利用方法を限定することにより，SSL のサーバ認証モードでも十分な安全性を確保でき，さらに，full access モードにおいても，チケットを用いることによって，安全性を確保したモビリティシ

† 三菱電機株式会社 情報技術総合研究所
†† 東京工科大学

☆ 無線 LAN や Bluetooth などの Access Point を設置し，無線でのインターネット接続サービスを不特定多数の利用者に提供している空間のこと．

ステムを実現していることが，既存の方式との違いであることに注意されたい．それに加えて，ユーザはこの二つのモードのどちらを利用しても匿名でサービスを享受できることにも注意されたい．

本論文の構成は，2 節で無線 LAN に求められる要件を明らかにした後，3 節で提案システムについて説明し，4 節で提案システムに対する議論を行い，最後の 5 節でまとめを行う．

2. 無線 LAN の要件

まず，現状の無線 LAN の問題点と関連研究の問題点について述べた後，無線 LAN システムに求められる要件を明らかにする．

2.1 現状の無線 LAN の問題点

IEEE802.11a，802.11b と併用して利用される無線 LAN のセキュリティの技術として，SSID (Service Set Identifier) や WEP (Wired Equivalent Privacy)，MAC (Media Access Control) アドレスフィルタリングの三つが提案されており，既に多くの無線 LAN 製品で実装されている．しかしながら，これらの技術にはいくつかの脆弱性が発見されている[1),2)]．そのため，会社や大学，ネットカフェなどで利用できる無線 LAN システムにおいて，悪意有るユーザが簡単にそれらの無線 LAN システムを不正に利用できてしまい，そのユーザを追跡することも非常に困難になるという問題があるとされている．

2.2 関連研究の問題点

現状の無線 LAN の脆弱性を鑑みて，これまでに，無線 LAN のアクセス制御システムとして，SSH や SSL，もしくは独自のプロトコルなどを利用したシステム[3)~5)] が提案されている．次に，これらのシステムをセキュリティとユーザビリティの観点から見た問題点を考察する．

上記で示したシステム[3)~5)] は，ユーザとの間でユーザのアカウント情報を用いて相互認証を行うため，ユーザは安全に無線 LAN を利用できる．このとき，システム側はユーザのアカウント情報を管理する必要があり，ユーザ側は自身のアカウント情報の登録といった作業を必ず行わなければならない．確かに強固なセキュリティを確保するためにはユーザ認証が必要であるが，Web ブラウザでホームページを見るためだけに，わざわざ自身の情報を登録しなければならないユーザの立場から鑑みると，相互認証を常に求めるシステムは，ユーザビリティに欠ける．実際，パスワード利用者の 6 割から 7 割が面倒であると言う統計もあるため，導入すれば簡単に利用できるこれまでの無線 LAN システムの利用から比べると，多くのユーザには煩雑であるだろう．安全性に関しても通信の機密性が守られていないものがある[3)]．また，SSL のサーバ認証モード時にパスワード認証を利用すると，実装によっては，MITM (Man In The Middle) 攻撃が仕掛けられる可能性が報告されている[10)]．

2.3 無線 LAN のシステムに求められる要件

現状の無線 LAN の問題点や関連研究の問題点から得られた，「ユーザビリティを考慮した無線 LAN のシステム」に求めたい要件を以下に述べる：

(1) ユーザビリティの向上
(2) システム側の管理コストの削減
(3) 無線区間の通信の暗号化
(4) 相互認証 (full access モード)

(1) はユーザの利便性に関する要件であり，read only モードでユーザが自身のアカウント情報を生成・保持する必要がないことを意味する．それに加えて，full access モードでは，ユーザが複数の無線 LAN のシステムを利用する際のモビリティの向上をも目指す．

(2) は運用に関する要件であり，アクセス制御を行う主体が，ユーザを認証するためのアカウント情報や ACL (Access Control List) を管理しないことを指す．これはすなわち，同一のシステムが導入されている複数のネットワークを利用するユーザは，read only モードにおいては，アクセス制御を行う主体に自身のアカウント情報を登録せずにそれらのネットワークの利用が可能であることを意味する．一方，full access モードにおいては，チケットを発行するどこかの主体にアカウント情報を登録しておけば，提携している違う組織に再度アカウント情報の登録をせずとも，その組織からインターネットに接続できることを意味する．つまり，ユーザは両方のモードにおいて匿名でサービスを受けられることになる．

また，(3)，(4) はセキュリティに関する要件である．(3) は，両方のモードにおいて，他の無線端末からの盗聴を防ぐことを意味する．(4) は，full access モードのときのみの要件であり，安全な無線 LAN の提供と同時に，問題が生じた際に，提案システムを利用しているユーザを特定できることを指す．

3. 提案システム

この節では，前の節で示した無線 LAN のシステムに求められる要件を満たすシステムを提案する．

提案システムでは，ユーザビリティとセキュリティという相反する要件を満たすために，ユーザビリティを重視した read only モードと，セキュリティとモビリティを重視した full access モードの二つのモードを用意する．ユーザは，どちらか一方のモードを選択し，提案システムを利用する．

read only モードは，提案システムを利用するユーザに外部ネットワークへの参照のみを許可するモードであり，ユーザビリティを高めることを目的とする．当該モードを利用するユーザは，予めユーザ自身のアカウント情報の登録や提示といった，煩わしい手続きの必要がなくなる．さらに，当該モードでは SSL の認証時にサーバ認証のみを行い，ユーザ認証は行わない．そのため，外部ネットワークへアクセス可能なサービスを限定されてはいるが，ユーザは匿名で享受できるといった利点が得られる．

full access モードは，提案システムを利用するユーザに対して外部ネットワークへの接続を制限せずに全て許可するモードである．当該モードでは安全性を考慮し，提案システムと提案システムを利用するユーザとの間で SSL の相互認証を行う．ただし，当該モードでは，相互認証しているにも関わらず，ユーザには Gateway (後述) に対して匿名でサービスを享受できるという利点がある．また，提案システムが導入されたネットワークが複数存在し，互いに連携し合っている場合には，ユーザはチケットを使用することで，それらの全てのネットワークを利用することができる．そのため，当該モードはモビリティに優れたモードとなっている．

各モードにおいて，Gateway はユーザを認証するための ACL やアカウント情報を管理することなしに，ユーザのアクセス制御を行える．つまり，貴重なリソースを無駄に消費せずに済み，2.3 (2) の要件を満たす．また，各モードでは，Gateway と Mobile Node (後述) の間の通信路に，SSL で暗号化された通信路を利用するため，2.3 (3) の要件を満たす．

提案システムでは，無線区間の安全性の確保に SSL を利用するため，データリンク層などの下位層が変化した場合でも容易に対応することができる．また，SSL は WEP とは異なり，暗号アルゴリズムを選択できるため，常に強力な暗号アルゴリズムを利用できるという利点もある．それに加えて，SSL では IPsec のようにマシンを認証するのではなくユーザを認証するため，ユーザごとの認証が可能となる．

read only モードから full access モードへの移行に関しては，3.5 に記述する．以降，各モードについて説明をする．

3.1 システムの主体

各モードを構成する共通の主体を以下に示す．ただし，各モードで固有の機能や固有の主体はそれぞれの節で説明を付加する：

(1) **Mobile Node**：ユーザが使用する無線端末．
(2) **Mobile Node クライアント**：Gateway との間で暗号化通信路を確立するソフトウェアであり，Mobile Node から送信される全ての通報を OSI (Open Systems Interconnection) 参照モデルの TCP 層でフックし，その暗号化通信路に流す．
(3) **Gateway**：Mobile Node から受信した通報を解析し，ルーティングを行う主体．Mobile Node に IP アドレスを貸し出すために，DHCP (Dynamic Host Configuration Protocol) サーバを動作させる．また，DNS (Domain Name System) サーバも動作させる．
(4) **Access Point**：Mobile Node と Gateway との間の通信を中継する主体．IEEE802.11a もしくは 802.11b 規格の製品を利用する．
(5) **CA (Certificate Authority)**：X.509 ID 証明書 (後述) を発行する主体で，RFC 3280 で規定される主体を想定する．

3.2 利 用 前 提

各モードを利用する上での共通の前提を以下の通りとする：

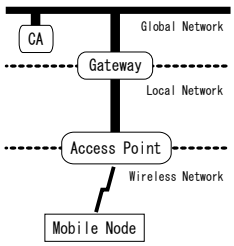

図 1 read only モードにおけるシステム構成

(1) Mobile Node クライアントが予め Mobile Node にインストールされている.
(2) 外部ネットワークとの通信は全て Gateway を経由する.
(3) Access Point では，SSID や WEP，MAC アドレスフィルタリングの機能を利用しない.
(4) Mobile Node はインフラストラクチャ・モード ☆で動作させる.
(5) 1 台の Mobile Node と Gateway との間の SSL のコネクションは高々 1 本しか開かない.
(6) ユーザは，正しく検証できない ID 証明書を受け取った場合，その ID 証明書を信頼しない.

3.3 read only モード

read only モードは，提案システムを利用するユーザに外部ネットワークへの参照のみを許可するモードである.

HTTP には複数のメソッド (GET や POST など) が定義されているが，メソッド POST のように，外部に対して情報を発信する行為が可能なメソッドの利用を，当該モードではフィルタリングする．これは，例えば掲示板などへの書き込みを匿名で行えなくするためである．すわなち，当該モードではメソッド GET のみを許可する．現在，一般的に利用されている検索エンジンの多くがメソッド GET でサービスを提供している☆☆.したがって，当該モードでは，検索エンジンにおける検索とその検索結果の参照，ブックマークなどからの直接のホームページ参照の利用が可能である．ただし，例外として，ユーザが通信相手と End-to-End にセキュリティを確保するプロトコル (SSH や IPsec など) を利用する場合には，その接続は許可する.

3.3.1 システムの構成

当該モードは，3.1 で示した五つの主体で構成される．ここでは，当該モードでの各主体の役割について説明を付加する．当該モードのシステム構成図は，図 1 を参照されたい：

(1) **Gateway**：当該モードを利用している Mobile Node から受信した通報が HTTP もしくは SSH や IPsec の通報の場合にのみ，外部ネットワークへのルーティングを行う.
(2) **CA**：Gateway の ID 証明書を発行する.

3.3.2 利 用 前 提

当該モードを利用する上での前提は，3.2 で示した前提に，さらに以下の二つの前提を付加したものとする：

(1) 当該モードが HTTP のメソッド GET のみを許可することを，ユーザは予め知っている.
(2) Gateway が信頼する CA の ID 証明書が trust-point ☆☆☆ として，予め Mobile Node に登録されている.

☆ 無線 LAN における通信方式の 1 つであり，各無線端末 (ノード) が無線 LAN の Access Point を経由してネットワークへ接続する．このとき，Access Point はネットワークと無線端末の接続を橋渡しする一種のハブのように機能する.
☆☆ 我々の調べでは，2002 年 11 月現在，Yahoo や Google，Goo，LYCOS，Excite に関しては，メソッド GET で検索のサービスを提供していることを確認している.
☆☆☆ ある主体が直接信頼する CA の ID 証明書

3.3.3 システムの動作

当該モードにおけるシステムの動作を以下に示す：

(1) ユーザは Mobile Node を利用し，提案システムの Access Point に接続する.
(2) Mobile Node は Gateway で動作している DHCP サーバからネットワーク設定情報 (貸し出された IP アドレスや Gateway の IP アドレスなど) を取得する.
(3) Mobile Node クライアントは，Gateway へ SSL を利用して接続し，サーバ認証を行う．ここで，Mobile Node クライアントは，自身に登録された trust-point をもとに，Gateway から提示された ID 証明書を検証し，Gateway が信頼できる主体であることを確認する．サーバ認証が成功後，Mobile Node クライアントと Gateway はこの SSL の暗号化通信路を保持する.
(4) Mobile Node は外部ネットワークへ向けて通報を送信する．このとき，送信される通報を TCP 層で Mobile Node クライアントがフックし，Gateway との間の SSL の暗号化通信路へ流す．Mobile Node からの通報は，Access Point を通して，Gateway へ転送される.
(5) Gateway は，受信した通報が HTTP (メソッド GET) の通報，もしくは外部ネットワークのホスト (外部ホスト) への SSH や IPsec の通報の場合のみ，その通報を外部ネットワークへルーティングし，外部ネットワークからの応答をユーザの Mobile Node へルーティングする．上記以外のプロトコルの通報である場合は，Gateway がその通報を破棄する.

3.4 full access モード

full access モードは，提案システムを利用するユーザに対して外部ネットワークへの接続を制限せずに全て許可するモードである.

当該モードでは，ユーザを認証するための ACL やアカウント情報は，Ticket Issuing Agent (後述) が管理する．当該モードを利用するユーザは，予めユーザ自身の公開鍵や秘密情報 (パスワードなど) をある Ticket Issuing Agent に登録しておくだけで，その Ticket Issunig Agent にチケット発行の権限委譲を行っている全ての Gateway で有効なチケットを取得でき，サービスを受けられる．なお，チケットの失効管理に関しては，文献[8] を参照されたい.

3.4.1 表 記 法

ここで，当該モードを通して用いる表記の説明をする．主体 X の ID と対応付けられた公開鍵，秘密鍵を P_X，P_X^{-1} と表す．X.509 証明書の内容を「⟨」と「⟩」でくくって表現し，その X.509 証明書 (後述) に秘密鍵 P_X^{-1} で電子署名が施されていることを，$\langle \ldots \rangle_{P_X^{-1}}$ と表現する．MD5 などのハッシュ関数 H によるデータ M のハッシュ値を $\mathrm{H}(M)$ と示す．また，n 枚の X.509 証明書から構成される証明書パスを $\{crt_1, crt_2, \ldots, crt_n\}$ と表現する．ここで，crt_1 は自己署名されたルート証明書であり，階層型の構造を持つ CA から構成される公開鍵基盤においては，ルート CA の ID 証明書に相当する．crt_n はこの証明書パスの利用者の ID 証明書となる．さらに，主体 X が，秘密鍵 P_X^{-1} を用いた署名によって「主体 Y の ID と公開鍵 P_Y との対応」を保証する有効期限 V の X.509 証明書を $Crt_{ID}Y = \langle X, Y, P_Y, V \rangle_{P_X^{-1}}$ のように表記し，Y の ID 証明書と呼ぶ.

また，あるセグメント X に導入する Ticket Issuing Agent，Gateway，Access Point を TIA_X，GW_X，AP_X とそれぞれ表記し，そのセグメント X を利用する Mobile Node を MN_X と表記する.

3.4.2 システムの構成

当該モードは，3.1 で示した五つの主体と，新しく導入する主体 Ticket Issuing Agent の計六つの主体で構成される．ここでは，当該モードでの各主体の役割について，説明を付加する．当該モードのシステム構成図は，図 2 を参照されたい：

(1) **Mobile Node クライアント**：ユーザはこの Mobile Node クライアントを使用して，Ticket Issuing Agent からチケットを取得し，そのチケットを SSL の相互認証モード時のユーザの ID 証明書として Gateway に提出することで，匿名で外部ネットワー

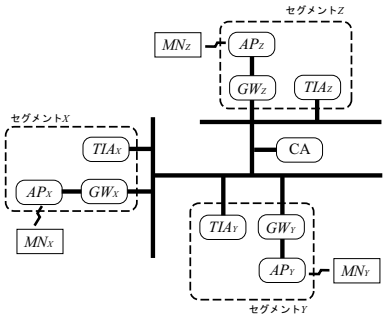

図 2 full access モードにおけるシステム構成

クへの接続サービスを享受する．

(2) **Gateway**：ユーザに対するチケットの発行権限を Ticket Issuing Agent に委譲する．SSL のクライアント認証時にユーザの ID 証明書としてユーザから提出されたチケットを検証し，そのユーザの外部ネットワークへの接続サービス利用の可否を決定する．正しいチケットを持つユーザの Mobile Node から通報を受信した場合には，全てのプロトコルを許可しルーティングを行う．ただし，Gateway はユーザの識別を行わず，チケットの正当性 (後述) が確認できればよい．Gateway は信頼する Ticket Issuing Agent を利用することで，不特定多数のユーザの ID による名前空間や個人情報などを管理する必要がなくなる．

(3) **Ticket Issuing Agent (以降，Ticket IA と表記する)**：Gateway からチケット発行権限の委託を受け，予め自身に登録されているユーザを認証し，ユーザにチケットを発行する主体．ユーザの認証には，ユーザのパスワード，もしくは，公開鍵を用いる．Ticket IA は特定のサービスを提供するための存在であり，公の存在である CA とは異なることに注意する．また，複数の Gateway からの委託を受ける可能性がある．

(4) **CA**：Gateway と Ticket IA の ID 証明書を発行する．

3.4.3 権限証明書について

ここでは，本論文で利用する権限証明書について述べる．権限証明書とは，公開鍵と権限の結び付きをその発行者に対する信頼の下で保証する公開鍵証明書 ☆ である．

提案システムでは，SSL における相互認証時にユーザが Gateway に提示するユーザの ID 証明書として，文献[8] に基づいた権限証明書を用いる．この権限証明書は以下の要素を格納した X.509 証明書に発行者の電子証明書 ☆☆を付加したものである：

Issuer：この権限証明書を発行した主体の持つ権限と対応する公開鍵のハッシュ値．

Subject：*Authority* と対応する公開鍵のハッシュ値．

PublicKey：*Authority* と対応する公開鍵．

Delegation：*Subject* によるさらなる権限の委譲の可否．

Authority：*Subject* が有する権限．

Validity：この権限証明書の有効期間．

例えば，権限 $Au1$ を持つ主体 X が，権限 $Au2$ に対する権限証明書を主体 Y に発行するとき，その権限証明書を以下のように表記する：

$$AuCrt_{X,Y}(Au2) = \langle \mathrm{H}(P_{Au1}), \mathrm{H}(P_{Au2}), P_{Au2}, D, Au2, V \rangle_{P_{Au1}^{-1}}$$

このとき，公開鍵 P_{Au1} がこの権限証明書を発行した主体の持つ権限 $Au1$ に対応し，公開鍵 P_{Au2} が権限 $Au2$ に対応している．この権限証明書は，秘密鍵 P_{Au1}^{-1} の保持者 X が，秘密鍵 P_{Au2}^{-1} に対して権限 $Au2$ を有効期限 V の間保証するものである．さらに，秘密鍵 P_{Au2}^{-1} の保持者 Y の権限委譲の可否は D で示される．

3.4.4 提案システムで利用する X.509 証明書

文献[8] に基づき，提案システムで利用する X.509 証明書を以下に示す：

- **CA CA が，ある主体 M に対して発行する ID 証明書**：
  $Crt_{ID}M = \langle CA, M, P_M, V_1 \rangle_{P_{CA}^{-1}}$
- **Gateway GW が自身に対して発行する権限証明書**．公開鍵 P_{Au1} に対する秘密鍵 P_{Au1}^{-1} は GW が保持する．このことから，権限 $Au1$ は GW が保持する権限を表す．なお，権限 $Au1$ は，チケットの発行を委譲する権限を意味する：
  $AuCrt_{GW,GW}(Au1) =$
  $\langle \mathrm{H}(P_{Au1}), \mathrm{H}(P_{Au1}), P_{Au1}, True, Au1, V_2 \rangle_{P_{Au1}^{-1}}$
- **Gateway GW がチケット発行の権限を委譲する Ticket IA TIA に発行する権限証明書**．公開鍵 P_{Au2} に対する秘密鍵 P_{Au2}^{-1} は TIA が保持する．このことから，権限 $Au2$ は TIA が保持する権限を表す．なお，権限 $Au2$ は，チケットを発行する権限を意味する：
  $AuCrt_{GW,TIA}(Au2) =$
  $\langle \mathrm{H}(P_{Au1}), \mathrm{H}(P_{Au2}), P_{Au2}, True, Au2, V_3 \rangle_{P_{Au1}^{-1}}$
- **Ticket IA TIA が ユーザ U に発行する権限証明書**．公開鍵 P_{Au3} に対する秘密鍵 P_{Au3}^{-1} は U が保持する．このことから，権限 $Au3$ は U が保持する権限を表す．なお，権限 $Au3$ は，チケットを行使する権限を意味する：
  $AuCrt_{TIA,U}(Au3) =$
  $\langle \mathrm{H}(P_{Au2}), \mathrm{H}(P_{Au3}), P_{Au3}, False, Au3, V_4 \rangle_{P_{Au2}^{-1}}$

3.4.5 チケットについて

本論文では，Ticket IA がユーザに発行する権限証明書群をチケットと定義する．n 個の異なる Gateway $GW_1, GW_2, \ldots, GW_n$ が，ある Ticket IA TIA_1 にチケット発行の権限を委譲している場合，ユーザ U が TIA_1 から取得するチケット $Ticket(TIA_1, U)$ の構成は以下のようになる：

$$Ticket(TIA_1, U) = \{AuCrt_{TIA_1,U}(Au3), AuCrt_{GW_1,GW_1}(Au1), \ldots, AuCrt_{GW_n,GW_n}(Au1), AuCrt_{GW_1,TIA_1}(Au2), \ldots, AuCrt_{GW_n,TIA_1}(Au2)\}$$

3.4.6 利 用 前 提

当該モードを利用する上での前提は，3.2 で示した前提に，さらに以下の四つの前提を付加したものとする：

(1) ユーザは，予め自身の公開鍵や秘密情報 (パスワードなど) を Ticket IA に登録済みである．

(2) Gateway，Ticket IA が信頼する CA の ID 証明書が，trust-point として予め Mobile Node に登録されている．

(3) Gateway と Ticket IA は互いの公開鍵を予め保持している．

(4) ユーザは，提案システムで取得したチケットを他人に譲渡しない．

3.4.7 システムの動作

当該モードにおけるシステムの動作を以下に示す：

(0) Gateway は Ticket IA との間で予め **発行権限委譲フェーズ** (後述) を経ているものとする．

(1) ユーザは Mobile Node を利用し，提案システムの Access Point に接続する．

(2) Mobile Node は DHCP サーバからネットワーク設定情報を取得する．

(3) もしユーザがチケットを取得していない場合には，**チケット発行フェーズ** (後述) に移り，チケットを取得する．

(4) **権限行使フェーズ** (後述) に移り，Gateway に SSL の接続を試みる．このとき，Gateway とユーザは相互に認証する．

(5) 権限行使フェーズを経た後，ユーザはこの SSL の暗号化通信路を利用して，外部ネットワークとの通信を行う．

3.4.8 発行権限委譲フェーズ

Gateway GW は予め取得している Ticket IA TIA の公開鍵を含めた権限証明書 $AuCrt_{GW,TIA}(Au2)$ を作成し，権限証明書

☆ 証明書利用者の本人性（Authenticity）を証明する証明書．

☆☆ 安全な社会的取引を行うにあたって，洗練された形式である「印鑑 (署名) 付きの封印文書 (すなわち証明文書) 」を媒介とする技術に支えられる紙の世界の証明文書を電子化したもの．

$AuCrt_{GW,GW}(Au1)$ と共に TIA に送信する．TIA は，予め取得している GW の公開鍵 P_{Au1} を用いて，それら二つの権限証明書を検証する．

3.4.9 チケット発行フェーズ

ユーザ U が Mobile Node クライアント MNC を通して，Ticket IA TIA からチケット $Ticket(TIA, U)$ を取得するフェーズである．ユーザがチケットをまだ取得していない場合や，取得したチケットの有効期限が切れた場合に，このフェーズに移る．このとき，ユーザは自身の公開鍵や秘密情報 (パスワードなど) が登録されている Ticket IA に接続する必要がある．例えば，ユーザが，はじめにセグメント X の Ticket IA TIA_X からチケットを取得し，その後セグメント Y へ移動後に再度チケットを取得する場合には，TIA_X へ接続することになる．以下，流れを述べる：

(1) U は MNC を通して，U の公開鍵もしくは秘密情報 (パスワード) を持つ TIA に SSH で接続を試みる．このとき，U と TIA は相互認証を行う．なお，TIA に U の秘密情報のみが登録されており，公開鍵が登録されていない場合，秘密情報で認証を行った後で，ユーザは公開鍵と秘密鍵のペアを生成し，その公開鍵を TIA に送信する．

(2) ユーザ認証が成功した場合，TIA は U を特定し，ACL から権限，すなわち，提案システムが導入されたネットワークの利用の可否を確認する．TIA は U の権限を確認すると，U の公開鍵を含む権限証明書 $AuCrt_{TIA,U}(Au3)$ を生成する．次に，$AuCrt_{TIA,U}(Au3)$ を含むチケット $Ticket(TIA, U)$ を生成し，MNC に送信する．MNC は，受信した $Ticket(TIA, U)$ を検証し，改竄などの問題がなければ自身のローカルファイルに保存する．

(3) MNC は，TIA との通信を終了させる．

3.4.10 権限行使フェーズ

ユーザ U が Mobile Node クライアント MNC を通して，Ticket IA TIA から取得したチケット $Ticket(TIA, U)$ を Gateway GW に提出し，提案システムの利用を開始するためのフェーズである．ただし，$Ticket(TIA, U)$ の有効期限が切れている場合，チケット発行フェーズで再度取得する必要がある．以下，流れを述べる：

(1) MNC は GW との間で SSL の相互認証の開始を要求する．

(2) SSL のサーバ認証時に，GW は自身の ID 証明書 $Crt_{ID}GW$ を MNC へ提示する．MNC は予め trust-point として登録されている CA の ID 証明書を用いて，$Crt_{ID}GW$ を検証し，GW が信頼できる主体であることを確認する．

(3) U が，チケット発行フェーズでユーザ認証が成功し，$Ticket(TIA, U)$ を取得している場合は，GW との SSL のユーザ認証時に，GW に $Ticket(TIA, U)$ を提示する．

(4) GW は MNC から取得した $Ticket(TIA, U)$ を検証し，改竄などの問題なければ，GW は MNC との間で SSL の暗号化通信路を保持する．

3.4.11 チケットの検証

権限行使フェーズで，Gateway がユーザから取得したチケットを検証する場合，以下の手順を行う (詳細は文献[8] を参照)：

(1) チケットに含まれている権限証明書から，自身が発行した権限証明書 $AuCrt_{GW,GW}(Au1)$ と $AuCrt_{GW,TIA}(Au2)$，および，TIA が作成した権限証明書 $AuCrt_{TIA,U}(Au3)$ を取り出す．

(2) 取り出した三つの権限証明書から証明書パス $\{AuCrt_{GW,GW}(Au1), AuCrt_{GW,TIA}(Au2), AuCrt_{TIA,U}(Au3)\}$ を作成し，RFC3280 に記述されている方式で検証する．

3.5 モードの移行

提案システムでは，read only モードを利用しているユーザが full access モードへ移行することも可能である．ただし，この場合，3.4.6 (1)，(2) で示した利用前提を満たしていなければならない．以下，移行手順を示す：

(1) ユーザは read only モードで提案システムを利用する．

(2) full access モードへ移行する際に，今まで Gateway との間で保持していた SSL の暗号化通信路を一旦閉じる．

(3) チケット発行フェーズ，権限行使フェーズを経て，full access モードの利用を開始する．なお，read only モードの利用時に，チケットを取得することもできる．

以上の移行手順により，ユーザは，どこかの Ticket IA に自分の情報を登録しておけば，例えば，違う組織の提携している Gateway から full access モードでインターネットに接続できる．

4. 議　　論

ここでは，提案システムにおける議論を行う．

4.1 HTTP のメソッド GET と POST

HTTP で定義されている GET は，POST と同様の動作を行うことができる．read only モードでは GET のみの通報を許可するため，悪意有るユーザが POST の要求を GET の要求に変換し，掲示板などへ匿名で書き込み (誹謗中傷など) ができてしまう．この問題は，サーバサイドではクライアントから受け取ったリクエストが GET なのか POST なのかを区別することができるにも関わらず，GET と POST の要求を同一の関数もしくはメソッドで処理するように実装することで発生する．そのため，サーバサイドの実装次第で，この問題は避けることができる．

4.2 SSL の利用について

SSL はネットワーク層以上のセキュリティを確保するプロトコルである．つまり，IPsec のようにマシンを認証するのではなくユーザを認証することで，ユーザごとの管理を行うことができる．さらに，提案システムのように一方の主体のみ認証したい場合に，SSL のサーバ認証は適しているプロトコルであると言える．特に，SSL はハードウェアに依存しないため，802.11a や 802.11b，802.11g などの OSI 参照モデルのデータリンク層以下の変化にも対応することが容易である．また，IPsec の利用において問題となる NAT (Network Address Translation) などへの対応も考慮しなくて良い．

4.3 提案システムのセキュリティ

IEEE802.11a，802.11b と併用して利用される WEP では，一つの SSID 内で利用できる暗号化通信路の鍵は一つである．そのため，同一 SSID 内の端末は，他の端末の通信を盗聴することができてしまう．

また，提案システムでは，SSL において通信を行う 2 者間で暗号アルゴリズムを決定するため，RC4 しか選択できない WEP よりも，常により強力な暗号アルゴリズムを利用でき，安全性を確保することができる．

提案システムでは，DHCP でユーザに IP アドレスを配布する．このとき，ユーザにローカル IP アドレスを貸し出し，Gateway で NAT を利用すれば，外部ネットワークから無線 LAN 内の個々の無線端末への攻撃を防ぐことができる．グローバル IP アドレスを貸し出す場合には，Gateway にファイアウォールの機能を持たせることでも外部ネットワークからの攻撃を防ぐことができる[11]．また，DHCP によって，悪意有るユーザも IP アドレスを取得できるが，Gateway でアクセス制御を行っているため，full access モードでは認証が成功せずに外部ネットワークとの通信はできない．read only モードでは利用できるサービスが限られており，外部ネットワークへの DoS (Denial of Service) 攻撃を行った場合でも，Snort などの IDS (Intrusion Detection System) を用いることによって，その行為をでき，Gateway を閉じるなどの対抗策を施すことができる．

悪意有るユーザが正規のユーザのなりすまし (IP アドレスや MAC アドレスの詐称) を行おうとしても，正規のユーザと Gateway 間で SSL の通信路を張っているため，外部ネットワークへの接続を Gateway で防ぐことができる．

ただし，提案システムでは，悪意有るユーザが同じセグメント内での正規のユーザに対して直接攻撃を行った場合や，無線 LAN 内部から Gateway に対して SSL セッション開始の DoS 攻撃を行った場合は防ぐことはできない．

4.4 関連研究との比較

文献[3)~5)] で述べられているシステムは，アカウント情報を用いて相互認証を行うため安全性が高いが，ユーザに対してアカウント情報の管理といった煩わしい手続きを強いることになる．これに対し，提案システムで

は，read only モードを利用することで，利用できるサービスは限定されているもののアカウント情報の登録などの手続きを必要とせずにネットワークを利用できる．さらに，full access モードにおいては，相互認証を行っているにも関わらず，ユーザはサービスを提供する主体に対して匿名でサービスを享受できるという利点が得られる．また，各 Access Point では，権限証明書の正当性をチェックするだけで良く，アカウント情報を管理する必要がなくなる．

アクセス制御の規格として IEEE802.1x や，チケットを利用した認証システムとして Kerberos[13] がある．IEEE802.1x では，認証サーバがアカウント情報を使ってユーザを認証するため，ユーザは常に特定されてしまう．さらに，無線区間での通信の暗号化に WEP を利用するため，WEP における問題を内包しており[2]，認証サーバ，Access Point，ユーザの端末が全て IEEE802.1x の規格に対応する必要がある．これに対し，提案システムでは SSL によって，匿名で安全なネットワークをユーザに提供できる．また，Kerberos と比較すると，提案システムは，匿名の権限制御や様々なドメインでのモビリティを重視したシステムとなっている．

4.5 read only モードの認証に関して

read only モードでは，サーバ認証のみを行い，ユーザ認証は行わない．ここでは，文献[12] に基づいて，認証プロトコルの観点から，SSL におけるサーバ認証が何を意味するのかを議論する．

SSL におけるサーバ認証とはその名のとおり，ユーザがサーバを認証することを意味する．SSL のサーバ認証のプロトコルを議論のために簡略化すると以下のようになる．なお，任意の通報 Msg を鍵 (共通鍵もしくは公開鍵) K で暗号化するとき，$\{Msg\}_K$ と表記する：

(手続き 1)　$S \rightarrow U : S$
(手続き 2)　$U \rightarrow S : \{Nc\}_{P_S}$
(手続き 3)　$S \rightarrow U : \{Ns\}_{Nc}$

ここで，手続き 1 において，サーバ S は，ユーザ U へ，サーバ自身を表すシンボル S を送信している．ゆえに，手続き 1 の通報を受け取ったユーザは，この通報が S からのものであると判断する．次に，ユーザは，ノンス ☆Nc (最終的にサーバとユーザとの間の共通鍵となる) を新しく生成し，S の公開鍵 P_S を用いて Nc を暗号化し，手続き 2 で S へ送信する．手続き 2 の通報を受信した S は，P_S に対する秘密鍵 P_S^{-1} でこの通報を復号する．この時点で，S と U は，互いに秘密の共通鍵 Nc を保持できる．さらに，手続き 3 では，S がノンス N_S (実際には，SSL ハンドシェイクプロトコル中にサーバとユーザがやり取りした全ての通信内容などを含むハッシュ値) を生成し，U に送信する．

このとき，手続き 2 と 手続き 3 でチャレンジレスポンスになるため，U は S を特定できている．しかし，注意しなければならないことは，S はユーザを特定できていないことである．なぜなら，サーバの観点から見ると，ユーザから送られてくる通報はサーバの公開鍵を用いて暗号化されるため，誰でも生成することが可能であるからである．ただし，ユーザの観点から見ると，公開鍵暗号の性質によって，ユーザが公開鍵で指定したサーバのみが，その通報を開示できることが保証されていることがわかる．

したがって，提案システムでは，read only モードで SSL のサーバ認証を利用することによって，提案システム側 (Gateway) はユーザを特定せずに外部ネットワークへの接続サービスを提供できることを意味し，ユーザ側からすると匿名でサービスを享受できることにつながる．ただし，ユーザが利用できるサービスを限定することで，外部ネットワークへの不正なアクセスを防いでいる．また，ユーザは，自身でパスワードや公開鍵，秘密鍵などを，生成もしくは保持する必要がなくなり，2.3 (1) の要件を満たす．

4.6 チケットについて

提案システムでは，文献[8] に基づいてチケットの「発行」と「サービス享受」を行っているので,「発行」における認証においてユーザを特定するが,「サービス享受」のチケットの利用においては匿名である．

提案システムで利用するチケットは，権限証明書，つまり，X.509 証明書で構成される．この X.509 証明書のデータサイズは，提案システムの利用では，一つの X.509 証明書あたりほぼ 800 bytes である．したがって，例えば，ある Ticket Issuing Agent $TicketIA$ が 100 個の異なる Gateway からチケット発行権限を委譲されていた場合，ユーザに対するチケットのデータサイズは，ほぼ 160 Kbytes になる．この程度であれば，現在のネットワークの通信速度をもってすれば，ユーザが提案システムを利用するときに，大幅な遅延が起きないと思われる．

なお，ある Ticket Issuing Agent $TicketIA$ にチケット発行の権限を委譲する Gateway の数がさらに膨大な場合には，チケットのデータサイズも比例して膨大になるため，LDAP (Lightweight Directory Access Protocol) などにチケットを登録しておくことも考えられる．このとき，ユーザは，チケットに対応する自身の秘密鍵のみを，自身が安全に保持していさえすればよい．チケットの改竄防止ができるという議論については，文献[8] を参照されたい．

5. おわりに

本論文では，ユーザビリティを重視した安全な無線 LAN システムを提案した．提案システムでは，read only モードと full access モードの二つのモードを用意し，ユーザビリティの向上と，セキュリティとモビリティを満たすシステムの実現を示した．また，SSL のサーバ認証モードと相互認証モードを利用しつつも，ユーザが匿名でサービスを享受できることも示した．それに加えて，提案システムでは，SSL を利用することで，データリンク層などの下位層の変化に容易に対応でき，さらに，WEP と比べ，より強力な暗号アルゴリズムの利用やユーザレベルの認証が可能となった．

今後の課題としては，プロトタイプの評価や内部から内部への攻撃の対処などが挙げられる．

参考文献

1) William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan : Your 802.11 Wireless Network has No Clothes (March 30, 2001).
2) ISAAC : Security of the WEP algorithm, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html
3) 後藤英昭, 満保雅浩, 静谷啓樹 : 廉価なスイッチと Secure Shell を利用した安全な情報コンセントの構成方法, 電子情報通信学会論文誌, Vol.J84-DI, No.10, pp1502-1505 (2001).
4) 石橋勇人, 山井成良, 森下英夫, 森 俊明, 安倍広多, 松浦敏雄 : 無線 LAN における利用者認証機構, 情報処理学会研究報告, DSM-21 (2001).
5) 藤川 賢治, 中野 博樹, 太田 昌孝, 平原 正樹, 真野 浩, 池田 克夫 : 無線インターネットサービスに必要なセキュリティを提供する高速認証システム, 情報処理学会研究報告, DPS-107 (2001).
6) C. Ellison : SPKI Requirements, RFC2692 (September 1999).
7) C.Ellison, B.Frantz, B.Lampson, R.Rivest, B.Thomas, T.Ylonen : SPKI Certificate Theory, RFC2693 (September 1999).
8) 梅澤健太郎, 齋藤孝道, 奥乃博 : 権限証明書と SSL 相互認証による匿名アクセス制御方式, 情報処理学会論文誌, Vol.43, No.08, pp.2562-2572 (August 2002).
9) 齋藤孝道, 梅澤健太郎, 奥乃博 : プライバシーを重視するアクセス制御システムの一方式, 電子情報通信学会 論文誌 (D-I), Vol. J84-D-I, No.11, pp.1553-1562 (2001).
10) 鬼頭利之, 齋藤孝道 : SSL (Secure Socket Layer) のシステムとしての安全性の考察, 情報セキュリティ研究会 (July 2002).
11) 齋藤孝道, 古森貞, 溝口文雄 : ユーザ認証付き DHCP (UA-DHCP) の提案と実装, 情報処理学会論文誌, Vol.43, No.08, pp.2587-2597 (August 2002).
12) 齋藤 孝道 : 認証プロトコルの機能と構成, コンピュータソフトウエア (日本ソフトウエア科学会 論文誌), Vol. 19, No.5, pp.60-73 (2002).
13) J. Kohl, C. Neuman : The Kerberos Network Authentication Service (V5), RFC1510 (1993).

☆ 理想的にはそれ以前に存在しないはずの文字列で，実装上は乱数である．ノンスは，長ければ長いほど安全上望ましいが，通信する上では短い方が良い．