遠隔機器制御プロトコルRACPを用いた無線LAN認証システム

野村 嘉洋† 秋成 秀紀† 田島 浩一‡
西村 浩二‡ 相原 玲二‡
†広島大学大学院 工学研究科
‡広島大学 情報メディア教育研究センター

概 要

IEEE 802.11b 無線 LAN 製品の普及に伴い，無線 LAN でネットワークサービスを提供する大学や公共施設が多くなってきた．利用者認証に基づくアクセス制御を行なう情報コンセントシステムが研究・開発されているが，有線/無線 LAN が混在する環境で使用でき，かつそれらの制御・管理を統一して行なうものは少ない．筆者らは既に情報コンセントシステムの機能をモデル化し，そのモデルに対する制御インターフェースを共通化するために，遠隔機器制御プロトコル RACP の枠組みに基づいた情報コンセントシステム PortGuard を提案し，有線 LAN での実装を行なっている．本稿では，PortGuard の無線 LAN への拡張について紹介し，さらにシステムの評価実験を通して，PortGuard が実用に耐える十分な性能を有することを示す．

User Authentication system for wireless LAN using Remote Appliance Control Protocol (RACP)

Yoshihiro Nomura† Hidenori Akinari† Kouichi Tashima‡
Kouji Nishimura‡ Reiji Aibara‡
† Graduate School of Engineering, Hiroshima University
‡ Information Media Center, Hiroshima University

Abstract

The universities and public facilities which provide the network service on wireless LAN are increasing caused by the popularization of IEEE 802.11b wireless LAN products. Several information outlet systems with user authentication are researched and developed. However, there are few systems which can be used in the environment which wired and wireless LAN were intermingled and which can be controled and managed with the standardized protocol. We have already modeled the function of the system, and proposed the system, named PortGuard, based on the concept of Remote Appliance Control Protocol (RACP). PortGuard was proposed to unify a control interface for that model, and it was already implemented by using the wired LAN. In this paper, we show about the extension to wireless LAN of PortGuard. Also, we show that PortGuard has the enough performance for practical use from the results of our evaluation experiments.

1 はじめに

近年の通信技術と携帯端末の普及により，いつでもどこでもネットワークサービスが受けられる環境の構築を望む声が高まってきている．このような要望に応じて，大学や公共施設では，図書館など不特定多数の利用者が出入りするオープンスペースに情報コンセントを設置し，利用者が携帯端末 (以下，利用者端末と呼ぶ) を接続できる環境を構築する組織が増えつつある．このような環境では，ネットワークの不正利用を防止するため，利用者の利用資格の有無に応じたアクセス制御を行うことが必要となる．

このような要求に対して，利用者認証に基づくアクセス制御を行う情報コンセントシステムの研究が行われており，いくつかシステムが提案されている [1]〜[9]．

また，近年の携帯端末の小型化・軽量化により，携帯端末におけるネットワークサービスの接続形態は，いままでの有線で繋がれた LAN だけでなく，IEEE 802.11b に準拠した無線 LAN によるネットワーク接続形態が急速に普及しつつある．また，無線 LAN ネットワークの構築は，設置場所のレイアウトに依存しないため，既存の施設でも容易に設置することか可能であり，簡単に行うことができる．

このように，無線ネットワーク接続形態の普及により，有線 LAN のみだけではなく，設置する場所や目的に応じて，有線 LAN や無線 LAN，あるいはそれらが混在する環境で使用できる情報コンセントシ

ステムの開発が必要となってきている．また，有線LAN・無線LANが混在するネットワーク環境でも，それらの制御を統一して行えることが重要である．しかし，提案されている多くの情報コンセントシステムは，このような点について十分に検討を行っているとは言えない．筆者らは，情報コンセントシステムにおけるアクセス制御のための機能をモデル化し，そのモデルに対する制御インターフェースを共通化するために，遠隔機器制御プロトコルRACP(Remote Appliance Control Protocol)[10] を提案し，その枠組みに基づいて情報コンセントシステムPortGuardの設計を行い，有線LAN用にVLAN機能を持ったSW-HUBを用いて実装し，実際に運用を行なっている．本稿では，PortGuardを無線LAN環境に対応できるように拡張した機能について紹介し，さらにシステムの評価実験を通してPortGuardが実用に耐える十分な性能を有することを示す．

2 情報コンセントシステムPortGuard

2.1 想定する環境

本システムでは，大学のように数千，数万人の利用対象者がいる環境において，無線LANカードのMACアドレス等の事前登録を必要としない利用者自身の持ちこんだ携帯端末及び無線LANカードが利用可能な無線ネットワークサービスの提供を想定している．

2.2 利用者端末のセキュリティ

無線LANネットワークの場合，利用者端末は互いに通信可能であり盗聴などが行なわれる可能性がある．そこで，無線LANアクセスポイントによっては，WEP(Wired Equvalent Privacy)と呼ばれる暗号方式を用いることにより，外部からの盗聴に対してセキュリティを確保するできる．しかし，WEPは共通鍵暗号方式であるため，想定する環境では，鍵の配布や漏洩を防ぐことが非常に困難である．また，鍵を共有している利用者端末間では，WEPを使用していない場合と同様に通信内容を盗聴することが可能となるため，利用者端末間の通信に関しては無力である．

また，あらかじめ利用者の無線LANカードのMACアドレスを無線LANアクセスポイントに登録することにより，登録を行なっていない無線LANカードからのパケット進入を拒むことができる．しかし，登録できるMACアドレスの数には制限があり，想定している環境で使用するには少ないものとなっている．将来的に上限が増えたとしても，全ての無線LANアクセスポイントに対してMACアドレスを登録することは非常に手間で，非現実的であるといえる．MACアドレスの登録により，パケット進入を拒むことは可能であるが，無線LANアクセスポイントから出て行くパケットの盗聴については防ぐことは不可能である．さらに，正規利用者のMACアドレスはパケットを盗聴することにより簡単に解読することが可能であり，このようにして奪われたMACアドレスを用いた偽造については無力である．

このように，WEPやMACアドレス登録によるMACアドレスフィルタリングでは利用者端末間の盗聴を防ぐことは本質的に不可能であるため，VPN(Virtual Private Network)を用いる方法 [7] やSSL(Secure Socket Layer)を用いる方法 [8]，PPPoE(PPP over Ethernet)を用いる方法 [9] により盗聴を防ぐ方法が提案されているが，通信路の安全が確保されるのは利用者端末から中継ノードまでで，中継ノード以降では盗聴される可能性があり，本質的な解決にはなっていない．また，これらのシステムは中継ノードで使用しているホストの負荷が高く，対応できる利用者端末はせいぜい20〜30台が限界であり，想定している環境での使用には向いていない．これらから分かるように，情報コンセントの機能として盗聴を完全に防ぐことは非常に困難であり，PortGuardでは盗聴防止機能については対象とせず，各利用者自身が盗聴される可能性を認識し，各自がエンドツーエンドでセキュリティを確保するように注意を促すようにしている．また，IP/MACアドレス偽造防止については，アプリケーションレベルで可能な範囲で対策しているが，IP/MACアドレスの両方を既に認証済の利用者端末のものに偽造された場合については，検出することは困難である．

2.3 システム構成

PortGuardのシステム構成を図1に示す．各構成要素の機能は以下のようになっている．

2.3.1 PortGuardサーバ

利用者端末からの認証要求を受付け，RADIUS(Remote Access Dialup User Service)サーバを用いて利用者認証を行なう．その認証結果に基づき，利用者端末の接続環境に応じてSW-HUBコン

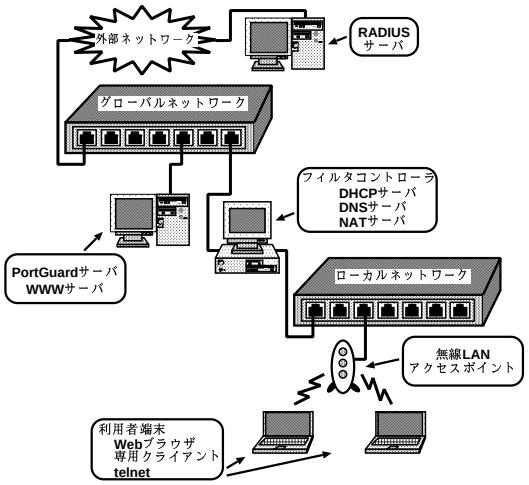

図 1: PortGuard のシステム構成

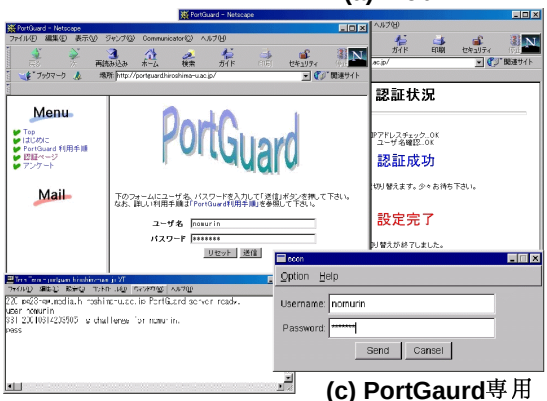

図 2: ユーザインターフェース

トローラ (有線 LAN) または，フィルタコントローラ (無線 LAN) に対して RACP コマンドを発行することにより，利用者端末のアクセス制御を行なう．また，利用者のアクセス記録をとっている．利用者端末から送られてくる認証情報の暗号/復号化には OpenSSL 0.9.6 を使用した．

2.3.2 フィルタコントローラ

PortGuard サーバからの RACP コマンドに従ってフィルタを制御する．無線 LAN 利用者端末の IP アドレスは，ここを通過するときに 1 対 1 NAT(Network Address Translation) によりプライベートアドレスとグローバルアドレスのアドレス変換が行なわれる．パケットフィルタリングおよび NAT には，Linux iptables 1.2 を使用した．

2.3.3 WWW(World Wide Web) サーバ

利用者が Web ブラウザを用いて認証を行なう際，認証情報は CGI(Common Gateway Interface) プログラムを通じて PortGuard サーバに伝えられる．利用者端末と WWW サーバ間では，認証情報を安全にやり取りできるように SSL を用いて通信を行なっている．実装には，Apache 1.3.14 + SSL 1.42 を使用した．

2.3.4 RADIUS サーバ

利用者の認証情報を管理し，PortGuard サーバからの認証要求に対する認証結果を応答する．実装には，DTC Radius 2.03p8 を使用した．

2.3.5 DHCP サーバ

DHCP(Dynamic Host Configuration Protocol) により，利用者端末に IP アドレスを割り当てるサーバ．無線 LAN 利用者端末にはプライベート IP アドレスを割り当てる．実装には，ISC DHCP 3.0b1pl16 を使用した．

2.3.6 DNS サーバ

どこでも同一の URL(Uniform Resource Locator) で利用者認証ページにアクセスできるように設置された，WWW サーバの属するドメインのプライマリドメインサーバ．実装には，ISC BIND 9.1.1rc3 を使用した．

2.3.7 無線 LAN アクセスポイント

無線ネットワークと有線ネットワーク間のネットワーク接続機器．本研究ではメルコ社製 AirStation を使用したが，IEEE 802.11b 準拠の製品であれば問題はない．実際には，フィルタコントローラを使用する場合は，使用するネットワーク機器の種類や方式を問わない．

2.4 ユーザインターフェース

PortGuard では，利用者認証時に用いるクライアントユーザインターフェースには，Web，telnet，PortGuard 専用クライアントの 3 つを用意し，幅広いユーザのニーズに答えることができるようにした．各クライアントソフト使用時の認証の様子を図 2 に示す．Web ブラウザによる利用者認証は，解り易いインターフェースを提供でき，telnet は，汎用のソフトが利用可能であり，PortGuard 専用クライアントは，認証以外の機能を提供しやすいといった特徴を持っている．また，各クライアントソフトは PortGuard サーバに認証情報を伝える際に，PortGuard サーバの公開鍵による利用者パスワードの暗号化を自動的に行う (telnet の場合は，暗号化を行なう専用レスポンス計算機が別途必要)．

2.5 利用者認証の流れ

PortGuard における利用者認証処理は図 3 の流れで行なわれる．まず，最初に PortGuard サーバは

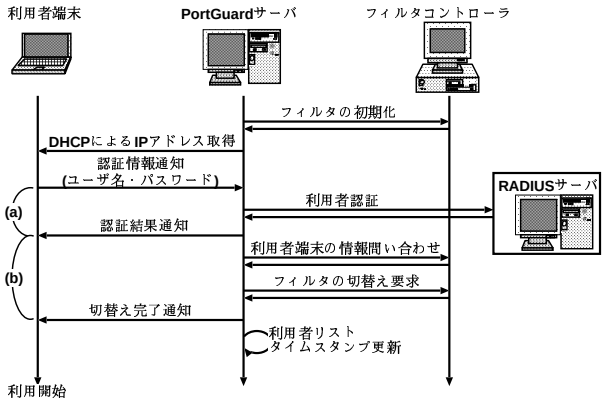

図 3: 利用者認証の流れ

フィルタコントローラを制御して，利用者端末が各種サーバホスト以外のホストと通信できないようにフィルタの設定を行なう．次に，利用者端末の認証では，Web ブラウザ等を介して，PortGuard サーバに認証情報を通知する．利用者認証に成功すると，該当する利用者端末の IP アドレスを基に，サーバホスト以外の外部ネットワークへもアクセスできるようにフィルタの切替えが行なわれる．

2.6 利用終了の検出

フィルタコントローラは常にネットワークを利用中の利用者端末の利用状況を監視しており，一定時間以上利用者端末に到達不能となったとき，該当する利用者端末の利用が終了したとみなす．利用者端末への到達性の確認には，ICMP ECHO_REQUEST を用いて，定期的に応答確認を行ない，一定回数以上連続して応答が無い利用者端末は利用が終了したと判断し，該当する利用者端末のフィルタ設定を，各種サーバホスト以外へアクセス不可となるように設定する．また，利用期間を設定することができ，利用期間が満了となると，サービスを終了するようになっている．利用者は，設定された利用期間以降も継続してネットワークを利用したい場合は，再度認証を行なうことにより，利用期間が更新される．利用期間が満了となった後で再度利用したくなった場合は，再び認証を行なうことにより利用できるようになる．

3 PortGuard の評価

3.1 測定環境

PortGuard の有効性を評価するために，以下の項目について評価実験を行なった．

測定 1 フィルタ・NAT のルール数及び適用順序による転送速度への影響

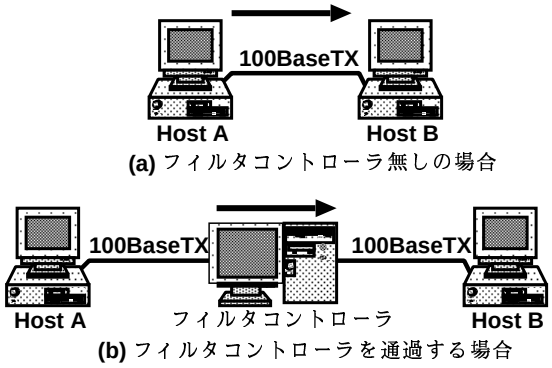

図 4: 測定環境 (測定 1)

表 2: フィルタ /NAT ルールによる転送速度への影響

条件		転送速度
フィルタルール	NATルール	(Mbps)
無し		93.21
1個	1個	93.48
	10000個の先頭	93.88
	10000個の末尾	92.78
10000個の先頭	1個	94.04
	10000個の先頭	93.96
	10000個の末尾	93.97
10000個の末尾	1個	4.32
	10000個の先頭	4.33
	10000個の末尾	4.33

測定 2 利用者認証の一斉要求に対する耐性及び認証に要する時間

測定に使用した，サーバとホストのスペックを表 1 に示す．

3.2 測定結果

3.2.1 測定 1

無線 LAN 環境の利用者端末が送受信する全パケットは，フィルタコントローラを通過する際に検査されるため，このフィルタコントローラのパケット処理能力がシステム全体の性能に大きな影響を与える．そこで，図 4 の測定環境の下で，フィルタルールと NAT ルールが表 2 に示す条件のときの，対応する利用者端末の転送速度にどの程度影響が出るかを測定した．測定には netperf 2.1pl3 を使用し，Host A から Host B の方向に，TCP，メッセージサイズ 1024 バイトで行なった．フィルタコントローラには，Server B を使用した．

表 2 の結果から，転送速度は NAT ルールの数や適用順序，およびフィルタルール数には無関係で，フィルタルールの適用順序からのみ影響を受けることが分かる．

表 1: サーバ/ホスト スペック

	RADIUSサーバ	Server A	Server B	Host A	Host B
CPU	Ultra SPARC-IIi 333MHz	AMD K6-2 300MHz	Pentium III 750MHz	AMD K6-2 300MHz	Pentium II 450MHz
Memory	128MB	128MB	256MB	128MB	128MB
OS	Sun OS 5.7	Linux 2.4.0	Linux 2.4.2	Linux 2.2.18	Linux 2.2.18

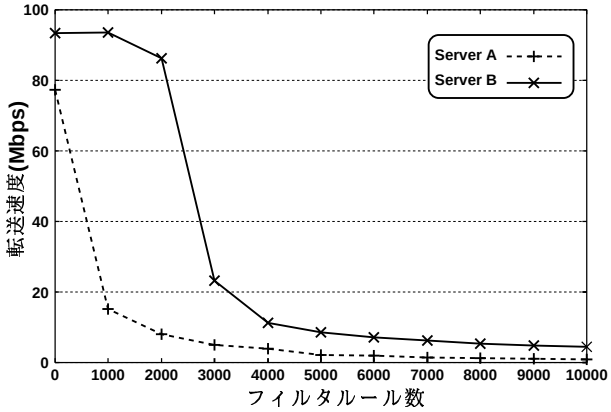

図 5: フィルタルール数による転送速度への影響

そこで，次に図 4 の測定環境で，フィルタルール数が 1,1000,2000,3000,...,10000 個の場合で，Host A に対応するフィルタルールをそれぞれの末尾に登録た場合の転送速度を測定した．測定には，先程と同様に netperf 2.1pl3 を使用し，Host A から Host B の方向に，TCP，メッセージサイズ 1024 バイトで行なった．フィルタコントローラが動作するホストの仕様は，Server A，Server B の場合でそれぞれ測定した．

結果を図 5 に示す．フィルタコントローラに Server B を使用した場合，フィルタルールが 1000 個までは転送速度にはまったく影響は現れていないが，Server A を使用した場合は，転送速度が急激に低下しているのが分かる．しかし，無線 LAN で使用する場合は，フィルタコントローラの動作するホストの仕様に Server A，Server B のどちらを選択した場合でも，フィルタルールが 1000 個程度であれば，無線 LAN の転送速度 (11Mbps) の制約が支配的となるため，Server A のような低スペックのホストでも問題ないと考えられる．実際に PortGuard では，1 台の利用者端末に対して 1 つのフィルタルールが設定されるので，実用上使用する範囲では，フィルタ・NAT のルールによる利用者端末の転送速度への影響は無いと考えられる．

3.2.2 測定 2

無線 LAN では，有線 LAN のポート数のように物理的な制約が無いため PortGuard で同時に利用することができる利用者端末の台数の限界値を見積もるために，複数の利用者端末が一斉に利用者認証要求を行なった場合の利用者認証に要する時間を測定した．測定は，図 6 に示す環境の下で，利用者端末は有線で繋がれた端末を使用し，以下に示す条件の元で行なった．(1)RADIUS サーバを除く各種サーバは，同一ホストで動作している．(2) 全ての利用者端末は NTP(Network Time Protocol) で時間を同期している．(3) 全ての利用者端末は Unix の at コマンドにより，同時刻に一斉に認証要求を行なう．(4) 利用者端末は，10 台から 60 台使用．(5) 測定を 3 回行ない，利用者認証要求を行なってからネットワークが利用できるようになるまでの平均時間，最長時間を計測．

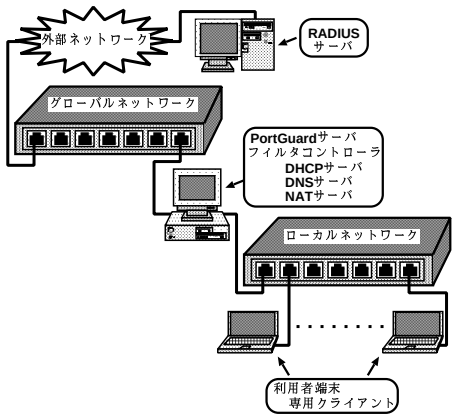

図 6: 測定環境 (測定 2)

PortGuard サーバ及びフィルタコントローラが動作するホストに表 1 の Server A を使用したときの結果を図 7 に，Server B を使用したときの結果を図 8 にそれぞれ示す．図 7，8 中で，平均認証時間は利用者端末が認証情報を PortGuard サーバに通知してから認証結果の通知を受け取るまでの時間 (図 3(a)) を表し，平均切替時間は認証結果通知を受け取ってからネットワーク切替設定の完了通知までの時間 (図 3(b)) を表している．

測定結果より，平均時間は利用者端末台数の増加に従い線形に増加しているのが分かる．また，PortGuard サーバ及びフィルタコントローラが動作しているホストのスペックを Server A から Server B に変更することにより，平均時間は 1/3 に，最長時間は 1/2 に短縮された．これらの結果から，無線 LAN 対応 PortGuard は，100 人程度の利用者端末に対応できる十分な性能を有しているといえる．

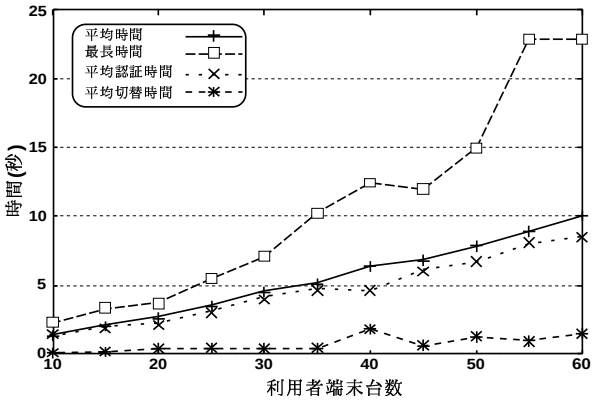

図 7: 一斉認証要求時に要する時間 (Server A 使用)

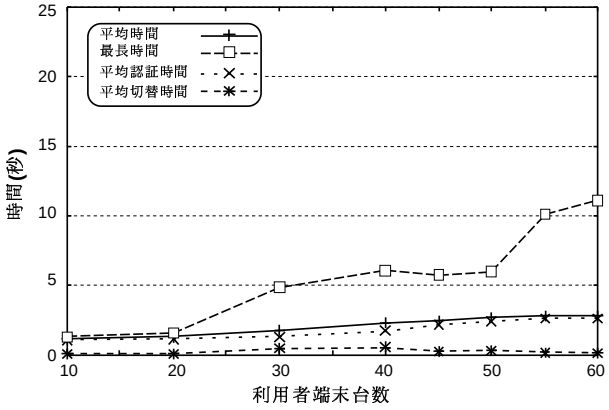

図 8: 一斉認証要求時に要する時間 (Server B 使用)

4 おわりに

本稿では，無線 LAN 環境でも利用可能な情報コンセントシステム PortGuard の実装と評価を行なった．制御インターフェースとして遠隔機器制御プロトコル RACP を用いることにより有線・無線のネットワークが混在する環境においても，制御・管理を統一的に行なうことが可能となった．

現在，PortGuard は学内の図書館など複数箇所で運用を行なっており，在籍者であれば誰でも利用可能である．図 9 に無線 LAN 用 PortGuard を利用している様子を示す．また，PortGuard のホームページ (http://www.portguard.org/)[11] で，GPL に基づいたソースの公開を行なっている．

図 9: 無線 LAN 用 PortGuard の利用

参考文献

[1] 東京大学情報基板センター: ユーザ携帯端末接続環境の試験運用の開始に付いて，http://www.ecc.u-tokyo.ac.jp/announce/1999/07/09_dhcp.html (1999).

[2] 細川 達巳: xfw - オープンスペース用 IP 認証システム -，http://www.itc.keio.ac.jp/~ Ehosokawa/xfw/ (1999).

[3] 久長 穣，岡田 隆，刈谷 丈治: 情報コンセントユーザ認証について，学術情報処理研究誌，No.2，pp.77–81，http://www.cc.yamaguchi-u.ac.jp/jacn/journal/pp077/index.htm (1998).

[4] 丸山 伸，浅野 善男，辻 斉, 藤井 康雄, 中村 順一: 既存の DHCP 端末で利用できる利用者にも管理者にも安全な情報コンセントシステムの構築，情報研報，99-DSM-14，pp.131–136 (1999).

[5] 渡辺 健次，只木 進一，江藤 博文，渡辺 義明: 利用者認証と利用記録機能を実現するゲートウェイシステム Opengate の開発，電子情報通信学会技術研究報告，IN 99-95，pp.43–48 (2000).

[6] 石橋 勇人，阪本 晃，山井 成良，安倍 広多，大西 克実，松浦 敏雄: 情報コンセントにおける認証とアドレス偽造防止を VLAN 機能により実現するシステム LANA2，情報処理学会研究報告，99-DSM-14，pp.137–142 (1999).

[7] 篠宮 俊輔，萩原 洋一: 大学キャンパス無線アクセスシステムの構築，情報処理学会研究報告，DSM-21-2，pp.7–12 (2001).

[8] 石橋 勇人，山井 成良，森下 英夫，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-21-3，pp.13-18 (2001).

[9] 桝田 秀夫，鈴木 未央，中西 通雄: PPPoE を利用した認証付き情報コンセントの実装と評価，情報処理学会研究報告，DSM-21-4，pp19-24 (2001).

[10] 西村 浩二，秋成 秀紀，相原 玲二: 遠隔機器制御プロトコルによる情報コンセントのアクセス制御，マルチメディア，分散，協調とモバイル (DICOMO 2000) シンポジウム論文集，pp.523-528 (2000).

[11] 広島大学情報メディア教育研究センター (情報通信基板系): PortGuard. on-line available at http://www.portguard.org.