遠隔機器制御プロトコルを用いた有線/無線LAN用情報コンセントシステム

西村浩二[†] 秋成秀紀[††]
野村嘉洋[††] 相原玲二[†]

ネットワークの不正利用を防ぎつつ，いつでもどこでも手軽に利用者の携帯する端末をネットワークに接続できる環境を提供するため，利用者認証に基づいたアクセス制御を行う情報コンセントシステムの設置が多くの組織で進められている．その一方で，携帯端末の無線ネットワークによる接続も普及しつつある．今後は有線LANと無線LANが混在するマルチベンダ環境に対応した情報コンセントシステムが必要であり，それらが統一的に制御や管理ができることが重要となる．しかし既存の情報コンセントシステムでは，このような視点での考察が十分に行われていない．本論文では，有線／無線LANの両環境に対応する情報コンセントシステムPortGuardを設計し，実装と評価を行う．筆者らが提案している遠隔機器制御プロトコルRACPを使用することにより，どちらの環境においても同一の制御インタフェースで制御や管理が行えること，アプリケーション指向プロトコルを用いることの有用性を示す．またいくつかの評価実験を通して，PortGuardが実用に耐える性能を有することを示す．

An Information Outlet System for Wired/Wireless LAN Using Remote Appliance Control Protocol

Kouji Nishimura,[†] Hidenori Akinari,[††] Yoshihiro Nomura[††]
and Reiji Aibara[†]

For providing the Internet connectivity at any time and everywhere, several information outlet systems which control the accessibility to the Internet according to the user authentication are proposed and operated. On the other hand, recently, it becomes very popular to connect a mobile terminal to the Internet via wireless LAN. Therefore, it is important that an information outlet system must support the mobile terminals connected via not only wired but also wireless LAN in the multi-vender environment. Furthermore, it should be controled and managed by a standardized protocol. However, there is no system nor discussion from this point of view. In this paper, we design, implement and evaluate an information outlet system, named PortGuard, which supports both wired and wireless LAN. For implementation, we adopt the Remote Appliance Control Protocol (RACP) proposed by us, then we can control both environments with the same interface. Furthermore, we show that PortGuard has enough potential for practical use from the results of our experiments.

1. はじめに

いつでもどこでも，手軽にネットワークに接続してサービスが受けられる環境の整備を望む声は年々高まってきている．ネットワークを高度な教育研究を遂行するための基盤設備と位置付ける大学などでは，図書館や教室など多くの利用者が出入りする場所に情報コンセントを設置し，利用者が携帯する端末（以下，利用者端末と呼ぶ）を接続できる環境の構築が望まれている．

一方，携帯端末のネットワーク接続は次第に無線化の方向に進みつつある．IEEE 802.11bに準拠した無線LANは，設置場所のレイアウトに左右されることなく既存の施設に容易に設置できることから，容易に広い範囲をカバーできる無線LANによる接続は今後の情報コンセントの主流になると考えられる．しかしその一方で，教室などの利用者の密度が高くかつ広帯域を要する場所や，セキュリティに特に注意を要する場所では，引き続き有線LANによる接続が利用されると考えられる．そのため，今後は有線LANと無線

† 広島大学情報メディア教育研究センター
Information Media Center, Hiroshima University
†† 広島大学大学院工学研究科
Graduate School of Engineering, Hiroshima University

LAN が混在する環境で利用できる情報コンセントシステムが必要となる．

利用者認証に基づいたアクセス制御を行う情報コンセントシステムは，すでに研究・開発が行われている[1)~7)]．ところが既存の情報コンセントシステムでは，有線 LAN と無線 LAN が混在することによっていっそう深刻となるマルチベンダ環境への対応の問題や，制御方式が異なるシステムの統一的な制御や管理に関する問題についての議論は十分に行われていない．

そこで本論文では，有線／無線 LAN の両環境に対応する情報コンセントシステム PortGuard を設計し，実装と評価を行う．その際，情報コンセントシステムにおけるアクセス制御機構を抽象化し，その制御インタフェースを共通化するため，筆者らが提案している遠隔機器制御プロトコル RACP（Remote Appliance Control Protocol）[8)] に基づいた設計を行う．そして，RACP を用いることでスイッチングハブ（以下，SW-HUB と呼ぶ）や無線 LAN，ダムハブなどの実現方法の違いによる影響が最小限に抑えられ，PortGuard の実装が容易に行えること，またいずれの環境においても同一の制御インタフェースにより制御や管理が行えることを示す．すなわち，RACP は一種のアプリケーション指向プロトコルであり，これを用いることの有用性を示す．またいくつか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．

以下，2 章では情報コンセントシステムが満たすべき要件について考察し，そのための一般的な実現方法を示す．3 章では遠隔機器制御プロトコル RACP の概要を述べ，情報コンセントシステムに適用するための機能拡張について述べる．4 章では本研究で実装を行った PortGuard の機能および動作の概要について述べる．5 章で実装の概要と評価について述べ，最後に 6 章で本論文のまとめを述べる．

2. 情報コンセントシステム

2.1 システムの実現方法

情報コンセントシステムでは，利用者認証の結果に従って外部ネットワークへの接続性を制御する．既存の情報コンセントシステムでは，次のような方法でシステムを実現している．

(1) 中継ノードでのパケットフィルタリングにより，パケットの到達性を制御する[1)~5)]．

(2) SW-HUB の VLAN（Virtual LAN）機能により，論理的なネットワークの構成を制御する[6),7)]．

（1）では，外部ネットワークへ到達可能な**グローバル LAN** と，到達不能な**ローカル LAN** の境界の中継ノードでパケット通過の可否を制御する．そのためローカル LAN で使用されるネットワーク接続装置に制限がなく，無線 LAN やダムハブを使用する場合はこの方法が用いられる．一方（2）では VLAN 機能を持つ SW-HUB を使用し，利用者端末は最初は利用者認証を行うホストにしか到達できない**ローカル VLAN** に属する．そして利用者認証が完了すると，外部ネットワークへ到達可能な**グローバル VLAN** に切り換えられる．

有線 LAN と無線 LAN が混在する環境で情報コンセントを利用可能とする場合，既存の情報コンセントシステムの組合せでは次のような問題がある．アクセス制御機構の一部であるネットワーク機器の制御方法はメーカや機種に依存するため使用できる機器が限定されるが，有線 LAN と無線 LAN が混在することでいっそう深刻となるマルチベンダ環境への対応が考慮されていない．またそれぞれは独自の手順でシステムを制御しており，利用者端末のアクセス制御という同一の目的であるにもかかわらず制御の手順が統一されていないため，これらを単純に組み合わると運用や管理が複雑になってしまう．しかし，これらを解決するための方策についての議論は十分に行われていないのが現状である．

2.2 セキュリティに関する考察・方針

情報コンセントシステムの目的は，利用資格のない者によるネットワークの不正利用を防ぐことである．そのため，次の機能は必須と考えられる．

(a) 利用者認証機能 利用資格の有無を認証システムによって確認する．

(b) アクセス制御機能 ネットワーク機器を制御して，利用者端末のネットワーク利用を制御する．

(c) アクセス記録機能 いつ・誰が・どこから・どのようにネットワークを利用したか（ネットワーク情報）を記録する．

既存の情報コンセントシステムでは，このほかに次のようなセキュリティ対策も検討されている．

(d) 利用者端末保護（盗聴防止，外部からの攻撃防止等）

(e) MAC（Media Access Control）アドレスおよび IP アドレス偽造防止

しかし本論文では以下の理由から（d),(e）についての深い議論は行わず，情報コンセントシステムの本質的な機能（a）～（c）を満たすために必要な機能に絞って議論を行う．

ローカル VLAN やローカル LAN 内では利用者端末

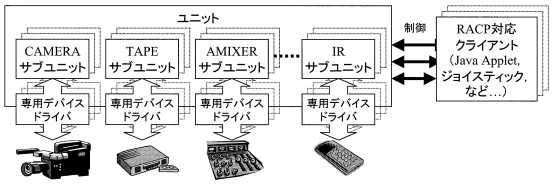

図 1 RACP の概略
Fig. 1 Outline of RACP.

が互いに通信可能であり，盗聴や多量のパケットを流すことによる通信妨害が行われる可能性がある．これらを防ぐには，通信路の暗号化や通信帯域を確保する方法がある．前者については VPN（Virtual Private Network）や SSL（Secure Socket Layer）を用いる方法[9),10)] が提案されている．しかし，通信路が暗号化されるのは利用者端末と中継ノード間のみである．盗聴を防ぐにはエンドツーエンドでの通信路の暗号化が必要であるため，本質的な解決にはなっていない．また後者を実現する具体的な提案はまだない．

一方，MAC アドレスや IP アドレスの偽造防止機能は，すでに認証された利用者へのなりすましを防ぐ機能である．MAC アドレスまたは IP アドレスのいずれか一方のみが偽造された場合は比較的簡単に検出できるが，両方同時に偽造された場合の検出は一般には困難である．VPN や SSL を用いる方法は効果はあるが，サーバの実装方法によっては利用者端末の収容可能数に制約が生じることが分かっている[11)]．

つまり，これらは情報コンセントシステムの機能拡張だけでは本質的に解決しない問題であり，PortGuard の実装にあたっては可能な範囲で対策を行うが，本論文では深く議論しないこととした．

3. 遠隔機器制御プロトコル RACP[8)]

3.1 RACP の特徴

RACP の概略を**図 1** に示す．RACP では制御対象をユニットと呼び，その内部に複数のサブユニットを持つ．実際に制御するデバイス（ビデオカメラなど）の機能によりサブユニットが持つコマンドは異なるが，ここにはデバイスに固有な情報は含まれない．デバイスへの依存部分は，専用デバイスドライバに記述される．このような構造を用いることで，メーカや機種が異なる機器には対応する専用デバイスドライバの追加のみで対応でき，RACP による制御そのものには変更が生じないため，システムの拡張の影響を最小限に抑えることができる．

本研究では，有線／無線 LAN 用情報コンセントシステムにおけるアクセス制御機構の制御インタフェースとして RACP を利用することで，システムの制御手順の統一を図り，容易にマルチベンダ環境に対応可能なシステムを構築する．

3.2 RACP のコマンド

RACP には，ユニットコマンドとサブユニットコマンドの 2 種類のコマンドがあり，コマンドとその応答には ASCII 文字列を使用する．ユニットコマンドはすべてのユニットで必ず実装され，サブユニットコマンドはユニットごとに必要なものを選択して実装する．本論文に関連する RACP コマンドを**表 1** に示す．

TRAP コマンドは RACP において重要なコマンドである．RACP では他の制御プロトコルと同様にユニットに TCP（Transmission Control Protocol）で接続して制御する．ただし RACP は接続時にユニットの状態を変更しているにすぎず，接続を解除した後も制御が継続している場合がある．TRAP コマンドは，ユニットの状態変化を通知する宛先とキーワードを設定する．通知はキーワードとともに UDP（User Datagram Protocol）を用いて送信され，キーワードが一致した場合はその内容に応じた処理を行う．このように，TRAP コマンドは STAT コマンドの補助的な機能として使用し，また受信の確認応答や再送のための機構を持たない．パケットロスなどの影響によって通知が受け取れない場合があるため，より確実な状態把握が必要な場合は接続を維持するか定期的に接続して，STAT コマンドを発行する必要がある．

3.3 VLAN サブユニット

VLAN は，ネットワーク接続装置においてブロードキャストドメインの設定や変更を可能とする機能である．具体的には，ポートあるいは MAC アドレス単位でホストのグループ化を行い，異なる VLAN に属するホストどうしは直接通信をできなくする．

CONFIGURE PORT（PORT） VLAN に属するポートを設定する．ADD，DEL，INI はそれぞれ追加，削除，初期状態である．ポートが使用中（UP）の場合は ADD，DEL による変更が可能であり，未使用時（DOWN）には自動的に初期状態に戻る．

CONFIGURE FILTER（FILT） VLAN にフィルタを設定する．ADD，DEL，INI はそれぞれ追加，削除，初期状態である．IN，OUT でフィルタの方向（それぞれ入力，出力）を指定する．フィルタは（*port*, *mac1*, *mac2*, *ip1*, *ip2*）で表現され，パケット通過の許可を意味する．

SET TRAP（TRAP） TRAP コマンドで指定された宛先に通知するイベントを指定する．NONE,

表 1 RACP のコマンド（抜粋）
Table 1 List of RACP commands (excerpted).

Subunit	Description	Command Syntax
Unit Commands:		
	USER NAME	USER *user-name*
	PASSWORD	PASS *password*
	LOGOUT	QUIT
	SET TRAP	TRAP *keyword* [{*h1,...,h4,p1,p2* | *h1,...,h16,p1,p2* | *host-name port*}]
	SHOW STATUS	STAT [*subunit-name*[*subunit-num*]]
	SHOW HELP	HELP [*subunit-name*[*subunit-num*]]
Subunit Commands:		
VLAN	CONFIGURE PORT	VLAN *n* PORT {ADD | DEL | INI} *port1* [*port2* [...]]
	CONFIGURE FILTER	VLAN *n* FILT {ADD | DEL | INI} {IN | OUT} *port mac1 mac2 ip1 ip2*
	SET TRAP	VLAN *n* TRAP {NONE | ALL | PORT | FILT}
	SHOW VLAN STATUS	VLAN *n* STAT [{PORT [*port*] | FILT [*port mac1 mac2 ip1 ip2*]}]

ALL，PORT，FILT はそれぞれ,「通知しない」,「すべて通知する」,「PORT の変化のみ通知する」,「FILT の変化のみ通知する」を意味する．デフォルトは ALL である．

SHOW STATUS（STAT） 現在の状態を要求する．応答は複数行からなる．1 行目は，OK などの文字列で無視してよい．2 行目以降は，引数の違いにより異なる．

PORT 各行に 1 つずつポート番号，UP または DOWN の状態を表示し，取得できていれば接続されているホストの MAC アドレスが続く．第 2 引数としてポート番号が指定された場合は，そのポートについての状態のみを表示する．

FILT 各行に 1 つずつ IN または OUT の別，フィルタの内容の順で表示する．INI で設定されたフィルタについては，行の最後に INI と表示する．第 2 引数としてフィルタの内容（∗ のみ使用可能）が指定された場合は，そのフィルタにマッチするフィルタを表示する．

引数なし 最初に PORT の内容を表示し，続いて FILT の内容を表示する．

4. 情報コンセントシステム PortGuard

4.1 システム構成

PortGuard のシステム構成を**図 2** に示す．各構成要素の機能概要は以下のとおりである．

SW-HUB コントローラ（有線 LAN 用）

フィルタコントローラ（無線 LAN 用） RACP を解釈し，それぞれのネットワーク機器を制御する．また利用者端末の利用状況を常時監視し，物理的な接続が切れたり，一定時間到達不能になったりした場合には，該当する利用者端末のネットワーク利用を不可にする．

PortGuard サーバ 利用者端末からの認証要求を受け付け，利用者認証を行い，その結果に基づいてコントローラに RACP コマンドを発行して利用者端末のアクセス制御を行う．そのほか，利用者の認証結果や利用者端末の利用状況などの記録を行う．

その他のサポートサーバ ユーザインタフェースや利用者認証などのために使用される．設定以外に PortGuard システム構築のための特別な修正は含まない．

WWW（World Wide Web）サーバ 利用者は WWW ブラウザを用いて利用者認証を行うことができる．認証情報や認証結果は CGI（Common Gateway Interface）プログラムを通じて PortGuard サーバに伝えられる．実装には Apache 1.3.14 を用いた．

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して利用資格の有無を応答する．実装には DTC Radius 2.03p8 を用いた．

DHCP サーバ 情報コンセントに接続した利用者端末に IP アドレスや DNS（Domain Name System）サーバ，デフォルトゲートウェイなどを配布する．実装には ISC DHCP 2.0 を用いた．

DNS サーバ どこでも同一の URL（Uniform Resource Locator）で利用者認証のページにアクセスできるよう WWW サーバの属するドメインのプライマリサーバとして動作する．DHCP（Dynamic Host Configuration Protocol）サーバが配布する DNS サーバに指定されている．実装には ISC BIND 8.2.3

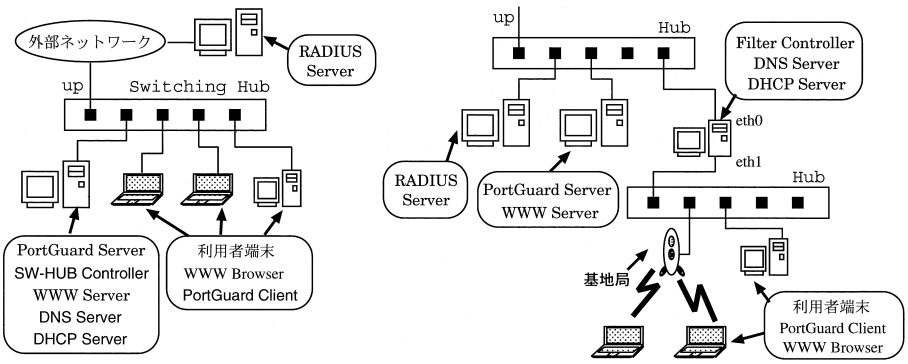

図 2 PortGuard のシステム構成（左：有線 LAN 用，右：無線 LAN 用）
Fig. 2 PortGuard system (left: for wired LAN, right: for wireless LAN).

表 2 サーバ/クライアントホストの仕様
Table 2 Specification of server/client hosts.

	仕様
CPU	Intel Pentium II 300 MHz
メモリ	128 MB
NIC	Intel EtherExpress Pro/100（10 Mbps）
OS	Linux-2.4 + gcc-2.91.66
	Windows98 + Cygnus-20.1

を用いた．

PortGuard クライアント 利用者端末上で実行される専用プログラムである．WWW ブラウザの代わりに使用し，PortGuard サーバに直接アクセスして利用者認証を行う．WWW ブラウザに比べてメモリ占有量が小さく，利用時間の表示や認証に時間制限を設けた場合の自動更新などの付加機能を組み込むことも可能である．

PortGuard は Linux-2.4.0 で動作し，現在は SW-HUB として Cisco 社製 Catalyst 2900/3500 シリーズをサポートしており，IEEE802.1q に対応していれば専用デバイスドライバの追加により他の SW-HUB にも対応可能である．またフィルタコントローラにおけるパケットフィルタリングと NAT（Network Address Translation）の機能は，OS 標準の iptables で実現している．ソフトウェアの開発およびサーバ/クライアントホストには**表 2** に示す仕様の PC を使用した．開発したソフトウェアを**表 3** に示す☆．

4.2 動作の概要

利用者認証の流れを**図 3** に示す．PortGuard の動作は，システムの初期化，利用者端末の接続・利用，利用終了の検出の 3 つのステップからなり，有線 LAN 用，無線 LAN 用ともに RACP のコマンドにより制御される．

表 3 開発したソフトウェア
Table 3 Developed softwares.

ソフトウェア	行数	使用ライブラリ等
(Linux 版)		
PortGuard サーバ	3,500	OpenSSL 0.9.6
SW-HUB コントローラ	2,900	UCD SNMP 4.2
フィルタコントローラ	2,900	
共通ライブラリ	1,600	
CGI プログラム	1,100	OpenSSL 0.9.6
PortGuard クライアント	1,200	OpenSSL 0.9.6
レスポンス計算機	400	OpenSSL 0.9.6
(Windows 版)		
PortGuard クライアント	1,200	SSLeay 0.9.0
レスポンス計算機	400	SSLeay 0.9.0

4.2.1 システムの初期化

PortGuard サーバが起動されると，コントローラの初期化を行う．PortGuard サーバは STAT コマンドを発行し，コントローラが保持する VLAN サブユニットの数を確認する．VLAN サブユニットを複数有する場合は SW-HUB コントローラ，1 つしかない場合はフィルタコントローラと見なして次の処理を行う．

SW-HUB コントローラの場合 VLAN n PORT コマンドにより，利用者端末用ポートとサーバホスト用ポートが属するローカル VLAN を設定する．さらにアップリンク用ポートとサーバホスト用ポートが属するグローバル VLAN を設定する．

フィルタコントローラの場合 VNAN n FILT コマンドにより，グローバル LAN 側に設置した WWW サーバや PortGuard サーバを宛先アドレスとするものを除き，ローカル LAN を始点アドレスとするパケットがグローバル LAN に転送されないように設定する．また 1 対 1 NAT の設

☆ レスポンス計算機は，telnet を用いて利用者認証を行う場合に PortGuard サーバの公開鍵でパスワードの暗号化を行うソフトウェアである．

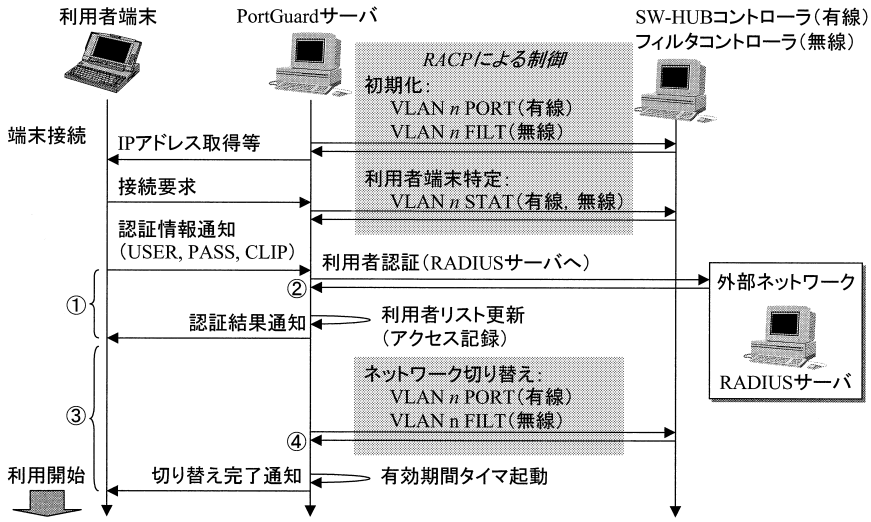

図 3 利用者認証の流れ
Fig. 3 Sequence of user authentication.

定を行う☆.

これらの設定により，初期状態では利用者端末はサーバホスト以外の外部ネットワーク上のホストとは通信できない．そして TRAP コマンドにより，PortGuard サーバを後述するイベントの通知先に指定する．

4.2.2 利用者端末の接続・利用

利用者端末はスイッチングハブあるいは無線 LAN のアクセスポイントに接続し，DHCP サーバから得られる情報を元にネットワークの設定を行う．その後 WWW ブラウザで利用者認証ページを表示し，アカウント名とパスワードを入力する．この時点で，PortGuard サーバは利用者端末の IP アドレス，利用者のアカウント名，スイッチングハブを使用している場合は利用者端末を接続したポートを取得する．認証情報は RADIUS サーバに伝えられ，認証結果が PortGuard サーバに返される．認証に失敗した場合は，その旨を通知して終了する．認証に成功した場合は，次の処理を行って利用者端末のアクセス制限を解除する．

SW-HUB コントローラの場合 VLAN n PORT コマンドにより，利用者端末が接続されているポートをローカル VLAN からグローバル VLAN に切り替える．

フィルタコントローラの場合 VLAN n FILT コマンドにより，利用者端末を始点または宛先とするパケットを，ローカル LAN とグローバル LAN との間で転送するように変更する．

☆ 1 対多 NAT（IP マスカレード）は，利用許可後でも外部ネットワークから利用者端末にアクセスできないなどの制限があるため使用しなかった．

4.2.3 利用終了の検出

コントローラは利用中の利用者端末を常時監視し，次のいずれかに該当するとき，ネットワークの利用を終了したと判断して該当する利用者端末に関する設定を初期状態に戻す．そしてこのイベントを PortGuard サーバに通知する．

- 利用者が利用終了を通知した．
- ポートの状態が DOWN となった．
- 一定時間以上到達不能となった．
- 利用者認証の有効期間が満了した．

SW-HUB コントローラでは，利用者端末をポートから引き抜いたり，利用者端末の電源を切ったりすることによるポートの状態の DOWN を，スイッチングハブの TRAP 機能や定期的な VLAN n STAT コマンドの発行により検出する．またフィルタコントローラでは，利用者端末に対して定期的に ping による到達性の確認を行い，一定回数連続して応答がない場合に利用を終了したと見なす．

PortGuard では定期的な利用者認証を促すため，有効期間が設定できるようになっている．有効期間が定められている場合は認証時に残り時間が通知され，継続して使用するには有効期間内に再度利用者認証を行う．

5. 評　　価

有線/無線 LAN 用 PortGuard を利用している様子を**図 4** に示す．本研究では，有線/無線 LAN 用 PortGuard の実環境における運用を想定した評価実験を行った．

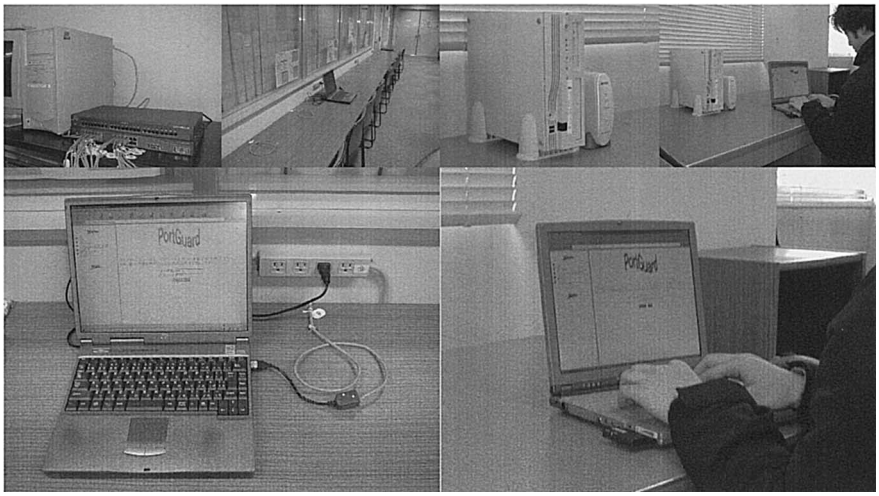

図 4 PortGuard（左：有線 LAN 用，右：無線 LAN 用）
Fig. 4 Snapshot of PortGuard system (left: for wired LAN, right: for wireless LAN).

表 4 評価実験 1 の結果
Table 4 Result of Exp. 1.

区間	処理の概要	時間（秒）
①	認証情報通知〜認証結果通知	0.177
②	利用者認証（対 RADIUS サーバ）	0.147
③	認証結果通知〜設定完了通知	
	有線 LAN 用 PortGuard	0.929
	無線 LAN 用 PortGuard	0.082
④	ネットワークの設定変更	
	SW-HUB コントローラ	0.926
	フィルタコントローラ	0.081

評価実験 1 ネットワーク切替えに要する時間（有線/無線）

評価実験 2 フィルタルール数やその適用順序がパケット転送性能に与える影響（無線）

評価実験 3 利用者認証のいっせい要求に対する耐久性（無線）

以下では，それぞれの評価実験について述べる．

5.1 評価実験 1

利用者が利用手順に従って利用者認証を行った場合の PortGuard の応答時間を，表 2 に示す構成で有線/無線 LAN 用それぞれで調べた．利用者が利用者端末を情報コンセントあるいはアクセスポイントに接続し，WWW ブラウザにより利用者認証の要求を出してから，ネットワークが利用可能となるまでの時間を 4 区間（図 3 中①〜④）で計測した．利用者端末の接続から切断までを 10 回行い，平均した結果を**表 4** に示す．

区間③および④では，SW-HUB コントローラが行う SW-HUB での VLAN 切替え処理に時間を要するため，有線 LAN 用 PortGuard は切替え完了通知に時間を要している．しかし，いずれの場合も利用者が正しく操作を行えば 1 秒程度の待ち時間でネットワークが利用可能な状態となる．

5.2 評価実験 2

無線 LAN 用 PortGuard では，利用者端末が送受信するパケットがすべてコントローラを通過するため，コントローラの処理性能がシステム全体の性能に強く影響する．そこで，表 2 に示す構成で，ある利用者端末が外部ネットワーク上のホストと通信する場合を想定し，コントローラに登録されているフィルタルールの個数と，利用者端末に対応するフィルタルールの登録位置の違いにより，パケット転送性能がどのように変化するかを調べた．フィルタルールの条件は次のとおりである．

（イ） フィルタルール 1 個．
（ロ） フィルタルール 1,000 個．先頭に登録．
（ハ） フィルタルール 1,000 個．末尾に登録．
（ニ） フィルタルール 4,000 個．先頭に登録．
（ホ） フィルタルール 4,000 個．末尾に登録．

結果を**表 5** に示す．ここで，ping は 1000 回の平均応答時間，FTP は 3 MB のファイルを 10 回転送したときの平均転送速度である．フィルタルール 4,000 個で性能の劣化が認められるが，FTP は無線 LAN の転送速度が支配的であり，フィルタルール 1,000 個であれば差は認められない．実際の運用では，利用者端末 1 台あたり 1 個のフィルタルールが追加されることから，実用的な範囲での利用においてはシステムの性能に影響を与えないと考えられる．

表 5 評価実験 2 の結果
Table 5 Result of Exp. 2.

条件	ping [ms]	FTP [KB/s]
(イ)	3.827	462.745
(ロ)	3.864	462.422
(ハ)	4.715	462.164
(ニ)	3.851	461.222
(ホ)	8.199	387.998

5.3 評価実験 3

利用者認証の要求からネットワークの設定の完了までには，要求が逐次的に処理されるボトルネックが 3 つ存在する．

(1) PortGuard サーバの公開鍵による認証情報の暗号化・復号化

(2) RADIUS サーバによる利用者認証

(3) コントローラによるネットワークの設定変更

特に（3）は物理的な制限のない無線 LAN 用 PortGuard でサービス可能な利用者端末数を見積もる際の指標となる．

そこで，無線 LAN 用 PortGuard において，複数の利用者端末からいっせいに利用者認証を要求された場合のシステム各部の処理時間と全体の応答時間について調べた．実験環境では，表 2 のサーバ PC 上で PortGuard サーバとフィルタコントローラを動かした．すべての利用者端末の時計は NTP（Network Time Protocol）サーバに数ミリ秒以内の精度で同期しており，at コマンドによりいっせいに利用者認証が要求される．この環境の下で，利用者端末を 10 台から 60 台まで 5 台間隔で変化させ，利用者認証を要求してネットワークが利用可能になるまでの平均時間，最長時間を 3 回計測した．

結果を**図 5** に示す．利用者端末の台数の増加に従って応答時間が線形に増加していることが分かる．次に RADIUS サーバはそのままで，サーバホストの CPU のみ変更（→Intel PentiumIII 750MHz）し，(1) と (3) の処理を高速化した結果を**図 6** に示す．サーバの高速化により，平均応答時間と最長時間はそれぞれ約 1/3 と約 1/2 に短縮されることが確認された．

以上の結果から，60 台の利用者端末からの利用者認証要求が数ミリ秒以内にいっせいに発生する状況においても，平均数秒の実用的な待ち時間でネットワークが利用可能となることが分かった．このことから，60 台あるいはそれ以上の端末をいっせいに利用する教室などの環境においても，本システムは利用可能であると考えられる．

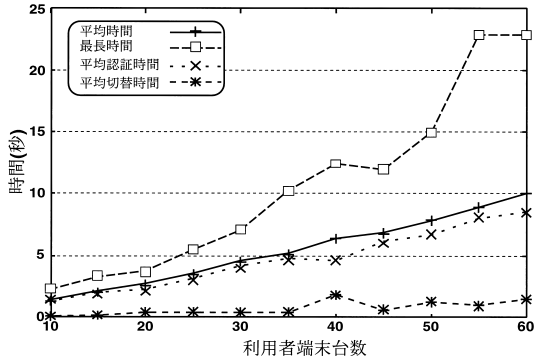

図 5 評価実験 3 の結果
Fig. 5 Result of Exp. 3.

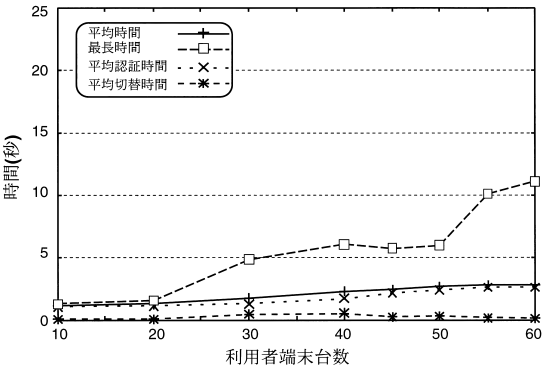

図 6 評価実験 3 の結果（CPU 変更後）
Fig. 6 Result of Exp. 3 (after CPU change).

6. おわりに

本論文では，有線/無線 LAN 用の情報コンセントシステム PortGuard を設計し，実装と評価を行った．ネットワーク機器の制御に遠隔機器制御プロトコル RACP を利用することにより，他のメーカや機種への対応を容易に行うことができる．また有線/無線 LAN の制御方式の違いによらず，利用者から見たユーザインタフェースが同一であるのはもちろんのこと，異なる制御方式が混在する環境において統一的な制御や管理を行うシステムを構築することができた．

本研究で実装した PortGuard は，ホームページ（http://www.portguard.org/）からダウンロードすることができる[12]．また学内ネットワークでは本システムによる実際の運用を行っており，在籍者であれば誰でも利用できる．また学内の宿泊施設では，学外者に対して有効期限付きアカウントを発行するサービスも行っている．

謝辞 日頃から本研究に関して有益なご助言・ご協力をいただく広島市立大学情報処理センター前田香

織助教授，広島大学情報メディア教育研究センター田島浩一助手に感謝します．本研究の一部は，日本学術振興会未来開拓学術研究事業における研究プロジェクト「高度マルチメディア応用システム構築のための先進的ネットワークアーキテクチャの研究」（JSPS–RFTF97R16301）の支援を受けて実施された．ここに記して謝意を表す．

参 考 文 献

1) 東京大学情報基盤センター：ユーザ携帯端末接続環境の試験運用の開始について（1999）．on-line available at http://www.ecc.u-tokyo.ac.jp/announce/1999/07/09_dhcp.html
2) 細川達己：xfw —オープンスペース用 IP 認証システム（1999）．on-line available at http://members.itc.keio.ac.jp/~hosokawa/xfw/
3) 久長 穣，岡田 隆，刈谷丈治：情報コンセントのユーザ認証について，学術情報処理研究誌，No.2, pp.77–81（1998）． on-line available at http://www.cc.yamaguchi-u.ac.jp/jacn/journal/pp077/index.htm
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，情報処理学会研究報告，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，IN99-95, pp.43–48 (2000).
6) 石橋勇人，山井成良，安部広多，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).
7) 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).
8) 西村浩二，前田香織，相原玲二：遠隔機器制御プロトコル RACP のフレームワークとその応用，情報処理学会論文誌，Vol.42, No.12, pp.2869–2877 (2001).
9) 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，2001-DSM-21, pp.7–12 (2001).
10) 石橋勇人，山井成良，森下英夫，森 俊明，安部広多，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，2001-DSM-21, pp.13–18 (2001).
11) 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，2001-DSM-21, pp.19–24 (2001).
12) 広島大学情報メディア教育研究センター（情報通信基盤系）：PortGuard．on-line available at http://www.portguard.org.

(平成 13 年 6 月 13 日受付)
(平成 13 年 12 月 18 日採録)

西村 浩二（正会員）

1990 年広島大学工学部第二類（電気系）卒業．1992 年同大学大学院工学研究科博士課程前期修了．全日空システム企画（株）を経て，現在，広島大学情報メディア教育研究センター助手．マルチメディア機器のリアルタイム遠隔制御，ATM ネットワークの管理に関する研究に従事．電子情報通信学会，Internet Society 各会員．

秋成 秀紀（学生会員）

2000 年広島大学工学部第二類（電気系）卒業．現在，同大学大学院工学研究科博士課程前期在学中．ネットワーク上における機器制御，認証とセキュリティに関する研究に従事．

野村 嘉洋（学生会員）

2001 年広島大学工学部第二類（電気系）卒業．現在，同大学大学院工学研究科博士課程前期在学中．遠隔制御プロトコルを用いたアクセス制御に関する研究に従事．

相原 玲二（正会員）

1981 年広島大学工学部第二類（電気系）卒業．1986 年同大学大学院博士課程修了．同大学同学部助手，同大学集積化システム研究センター助教授を経て，現在，同大学情報メディア教育研究センター教授．工学博士．マルチプロセッサシステムの設計，製作，コンピュータネットワークの研究に従事．電子情報通信学会，IEEE Computer Society，Communications Society 各会員．