VLAN選択機能を持つ情報コンセントシステム

田島 浩一†　西村 浩二†　相原 玲二†
†広島大学 情報メディア教育研究センター

概 要

VLAN 技術により物理的な場所による制限を考慮することのない自由なネットワークが構築可能になった．スイッチング HUB の VLAN 設定機能等を利用した情報コンセントも，いくつか提案されている．筆者らは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，有線および無線 LAN での実装を行なっている．本稿ではこの RACP を用いた VLAN 選択機能を持つ情報コンセントシステムについて紹介し，さらにシステムの評価を通して，同機能が実用に耐える十分な性能を有することを示す．

An Information Outlet System with Selecting VLAN Function

Kouichi Tashima†　Kouji Nishimura†　Reiji Aibara†
† Information Media Center, Hiroshima University

Abstract

VLAN has enabled to construct the free network which does not take into consideration restriction by the physical places. Some information outlet system using the VLAN setting function of Switching HUB are also proposed. Information outlet system based on this framework called PortGuard is proposed and mounting by the wired and wireless LAN is performed. We authors are proposed remote appliance control protocol RACP to model the function of information outlet system and to communalize the control interface over the model. In this paper, we introduces about an information outlet system which has a selecting VLAN function using this RACP, and having sufficient performance to which this function is equal to practical use is further shown through evaluation of a system.

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].

石橋らの開発した情報コンセント（LANA2）[6] では，情報コンセントに利用者端末間のセキュリティを保つ事およびアドレス偽造を防止する機能を VLAN 機能により実現している．認証により VLAN を設定する点で本システムは同様の手法である．

物理的にはなれた研究室などへアクセスする場合には，異なるネットワークからのアクセスになるため，管理ポリシーによりマイクロソフト社の Windows 共有が見えないことや，アドレスによるアクセス制限でアクセスできないことがあり利用環境が制限される．これに対して，久長らの開発した VLAN 選択システム [11] は，利用者に VLAN を選択できる機能を提供し，この要望に答えるものである．本システムではこれと同様の機能を提供するものである．情報コンセントシステムに，この様な機能拡張を行なう場合，これまでのものと同様にそれらの制御を統一して行える（管理できる）ことが重要である．この点については，従来より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 および無線 LAN 用の実装

を行い, 実際に運用を行なっている. 本稿では, このPortGuard システムにたいして行なった VLAN 選択機能の拡張について紹介し, さらにシステムの評価を通して本システムが実用に耐える十分な性能を有することを示す.

2 VLAN 選択機能を持つ情報コンセントシステム

2.1 利用環境

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, 利用者の用意する機器のネットワークカード（有線および無線）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使用する携帯または固定型端末及び無線 LAN カードが利用可能な無線ネットワークへの機能提供を想定している.

また, 接続するネットワーク環境は, 例えば, オープン端末室（端末を利用するユーザ）, 事務室（スタッフ）, 研究室（研究用ネットワーク）, 教官室（自室のプライベートネットワーク）の様に, それぞれ VLAN により異なる LAN に設定されていることを想定している.

本 PortGuard システムでは, 利用者による VLAN の選択を, これまでの PortGuard システム [10][12] や, 他の情報コンセントシステムと同様に, 利用者には, 特別な利用のための形態の必要ない, 利用者の持つ端末に備わっていると推測される機能のみを用いて行う容易な認証を用いる. ここで本 PortGuard システムでは, これまでのユーザに変更を強いないため, 現状の情報コンセントシステムでおこなわれているアカウント名とパスワードによる認証とする. 選択機能を利用するユーザは, ユーザ名の後に, あらかじめ設定された VLAN に対応する識別子を付加し入力し, その VLAN に接続する.

2.2 システム構成

本 PortGuard システムの構成を図 1 に示す. 各構成要素の機能は以下のとおりである.

2.2.1 PortGuard サーバ

利用者端末からの認証要求を受付け, まず, 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.

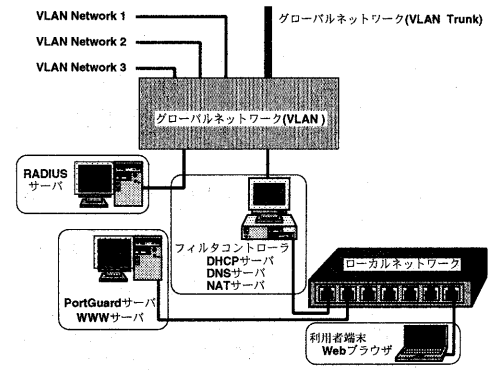

図 1: PortGuard のシステム構成

実際の運用は以下のとおりである.

1. ユーザ名（VLAN 識別子なし）とパスワードによる認証では, 既存の情報コンセントとしてそのネットワークの属する VLAN に接続される.

2. VLAN を選択するユーザは上記の識別子を, アカウントに続けて入力する. たとえば, センター職員の account1 というユーザが, センター職員用 VLAN に接続する場合, account1@center をアカウント名に入力する. この@center が VLAN 識別子となる.

3. 識別子を付加して入力されたアカウント名とパスワードは, その情報コンセントを管理する PortGuard サーバの WEB ページに送信し, デフォルトの RADIUS サーバに RADIUS プロトコルを用いて認証情報に置き換え送信される. ここで, この RAIDUS サーバは, 識別子の有無を確認し, 識別子がない場合はそのサーバ自身で認証し, 識別子がある場合は, 識別子に応じて認証を転送し, その結果を認証結果として送信してきた PortGuard サーバに返送する. この方式は,RADIUS に関する RFC2865 に記述されている機能を利用するものである.

4. 認証の承認が得られれば, このユーザの接続先を識別子の示す VLAN に接続する. この識別子と VLAN の ID および RADIUS サーバ名の対応は, あらかじめ設定されておく必要がある.

これら一連の認証の過程をチャートとして図 4 に示す. ここで, 利用者端末から PortGuard サーバまでの通信は, 従来と同様に, OpenSSL 0.9.6 により暗号/復号化を行っている.

2.2.2 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. 利用者端末の IP アドレスは, 無線 PortGuard システムと同様にここを通過する際に 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. ここで, アドレスが変換されるが, 利用者の選択した VLAN ごとにネットワークが異なるため, グローバルネットワーク側に設定されるアドレスはその選択された VLAN ごとに異なる. 情報コンセントのフィルタコントローラの機能として, 接続を許可されていない端末からのパケットをフィルタリングする機能を持つ. パケットフィルタリング及び NAT には,Linux iptables ver1.2.1a を使用した. また, VLAN セレクターとして接続する VLAN を選択し, グローバル側のスイッチに複数の VLAN パケットを運ぶため IEEE 802.1Q 準拠の VLAN Tagging 方式を用いた. この機能をサポートするためフィルタコントローラ用 PC のカーネルに VLAN のモジュールを組みこみ [14], グローバル側スイッチとして Catalyst 2948 XL-E を用いて検証を行なった.

2.2.3 WWW(World Wide Web) サーバ

利用者は従来の PortGuard システムと同様に,Web ブラウザの備える SSL による暗号化+ CGI を用いて PortGuard サーバに伝えられ, 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. 実装には,Apache 1.3.20 + mod_ssl-2.8.4 を用いた.

2.2.4 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. また, 本システムでは複数台の RADIUS サーバを用いる場合,RADIUS サーバ間の設定も必要とする. これは, 利用者のアカウント情報を必ずしも情報コンセントを管理する PortGuard サーバが保持することを必要としていない. 大学のネットワークの様に管理ポリシーの異なる, 独立したネットワークがあり,VLAN 選択による端末の接続時にもその管理ポリシーに沿うよう, 可能な限り透過的なものとした. このため,RADIUS サーバの設定は, 図 2 に示すように, 他の RAIDUS

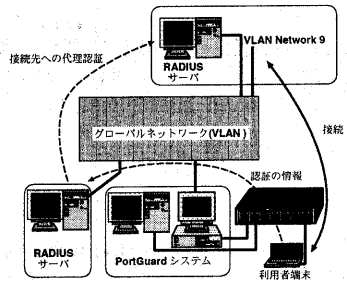

図 2: 管理区分の異なるネットワークでの利用

サーバを参照することを前提としている. 利用者から PortGuard システムへ送信された認証情報は, デフォルトの RADIUS サーバに送られるが, 前述の VLAN 識別子が付化されていた場合は, 他の RADIUS サーバに認証要求の転送 (代理認証) したのち結果を通知する. その結果,PortGuard システムは, 要求のあったクライアントを識別子に対応する VLAN に接続する.

2.2.5 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. 接続した利用者端末と PoutGuard サーバ間は, TCP による通信を用いるため, あらかじめプライベート IP アドレスを割り当てる. 実装には,ISC DHCP 3.0b1pl18 を使用した.

2.2.6 DNS サーバ

利用者からの簡便性を考慮し, 同一の URL 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. IP アドレスによる認証ページ指定では, ブラウザの一般的に持つ URL を記録する機能が利用できない事も, この設定を行なう理由である. 実装には,ISC BIND 8.2.4 を使用した.

2.2.7 ローカルネットワーク構成

端末間のセキュリティを重視しないのであれば, ローカルネットワークは無線 LAN あるいは単なるスイッチング HUB によるネットワークで構成できるが, 端末間での独立性を保つには, スイッチング HUB を用い VLAN 機能を利用して, 端末と PortGuard システムを接続する必要がある. 例えば, 筆者らが提案する有線 LAN 版 PortGuard システムと同様の構成方法で実現可能である.

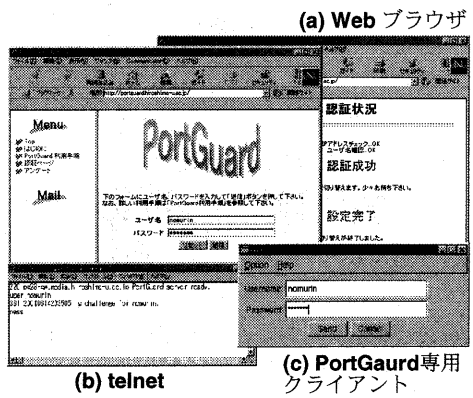

図 3: ユーザインターフェース

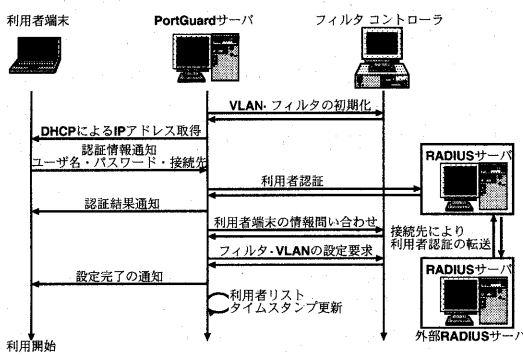

図 4: 利用者認証の流れ

2.3 ユーザインターフェース

ユーザインターフェースに関する箇所および, そこから PortGuard サーバまでの通信は, 従来の PortGuard システムと同じであり, 用意されている利用者認証用インターフェースには, Web,telnet,PortGuard 専用クライアントの 3 つが利用可能である.

各クライアントソフト使用時の認証の様子を図 3 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となることも従来どおりである).

2.4 利用者認証の流れ

PortGuard における利用者認証処理は図 4 の流れで行なわれる. まず, 最初に PortGuard サーバは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.

2.5 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. 最近の OS では ICMP を破棄するものもいつくかみられるため, 実際には,ICMP ECHO_REQUEST 後,ARP テーブルをしらべ MAC アドレスが存在することにより利用中であるかを判断している.

3 PortGuard の評価

3.1 測定環境

本 PortGuard システムのを評価するために, 利用者からみた性能の評価を, 利用フェーズにわけ, 利用開始, 利用中, 利用終了と簡易に分け, このなかで, 利用開始および利用中に関しての評価実験を行なった.

利用開始時に検討すべき項目は, 利用開始のリクエストから実際に利用可能な状態になるまでの時間である. これについては, 3.2.2 の測定にて測定を行なった.

利用中に検討すべき項目は, 多人数で利用する環境など, 利用状況によってどの程度の性能 (スループット) になるかを文献 [12] の実験結果から検討を行なった.

影響 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

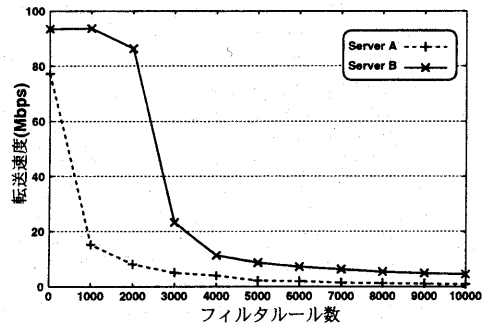

図 5: フィルタルール位置による転送速度への影響

表 1: サーバ/ホスト スペック

	RADIUSサーバ	PortGuard Server
CPU	Ultra SPARC-III 333MHz	Pentium III 750MHz
Memory	128MB	256MB
OS	Sun OS 5.7	Linux 2.4

測定 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

3.2 検証結果

3.2.1 影響

利用者端末が送受信する全パケットは, 本システムのフィルタコントローラを通過する際に IP アドレス・MAC アドレスの組によるルールチェックによりフィルタリングされるため, 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スループット性能となる.

文献 [12] の NAT 数に間する転送速度への影響の測定では, 転送速度は NAT ルールの数や適用順序, には関係が薄く, 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示されている. 本システムは実際に図中のサーバ B 相当のホストを使用している. フィルタのルール数を考慮した場合, 無線 PortGuard システムでは, 1 端末あたり 1 接続相当のルール数で適応であったが, 本システムではその端末 1 台が選択できる VLAN の数に比例してルール数が増加する.

図 5(文献 [12] より引用) に示される, Server B をフィルタコントローラに使用した本システムの場合, フィルタルールによる性能低下の起こるルール数 2000 を下回るつまり想定する（利用者数）×（選択する VLAN 数）をこれ以下とするすることが望ましい.

3.2.2 測定

本システムでは, 接続形態の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, 利用者端末は VLAN 機能の無いスイッチング HUB をで繋がれた端末を使用し, 以下に示す条件の下で行なった.

(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 50 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.

ホストは, 表 1 のスペックのものを使用し, その結果を図 6 に示す. 図 6, 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であり, 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これらの結果から, 本システムでは,100 人程度の利用者端末に対応できる（1 接続あたりの回線の速度は回線容量を共有するが）十分な性能を有しているといえる.

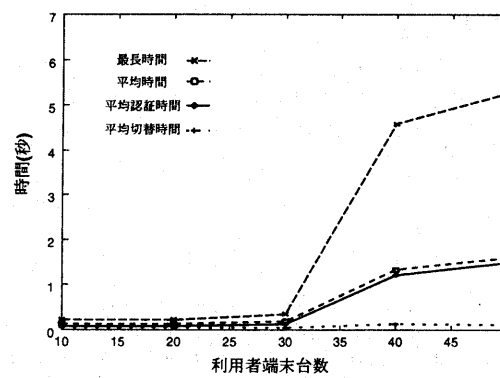

図 6: 一斉要求時数の応答時間

4 まとめ

本稿では, 一般的な情報コンセントを利用する環境と同様の利用形態で利用者の希望するネットワークに接続する, VLAN 選択機能を持つ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 VLAN 機能を持たない機器からの接続に対して本システムを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.

本方式では, 1 対 1 NAT を用いたアドレス変換を行なうため, IP 以外の通信方式に頼るアプリケーションは透過できない. 例えば, Windows のマイクロソフト共有などは, そのままの設定では他の機器が表示されないが, マシン名を直接指定することなどにより対応できるため, 大きな支障はきたさないと考えている.

現在, 本システムは正式な運用前のテスト運用を行なっており, 情報コンセントを利用可能な在籍者でありかつ運用に携わるスタッフは利用可能である. また,PortGuard のホームページ (http://www.portguard.org/) [13] で,GPL に基づいたソースの公開を予定している.

謝 辞

本 VLAN 選択機能を持つ情報コンセントシステムの実装の一部は, 広島大学大学院工学研究科秋成秀紀, 野村嘉洋両氏らによる. ここに記して謝意を表します.

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,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] 久長 穣, 北山 悟史, 渡邊 孝博, 棚田 嘉博, 井上 裕二: 複数 VLAN の動的切り替えネットワークの構築について, 情報処理学会研究報告,DSM-22-7,p.39-44 (2001).

[12] 野村 嘉洋, 秋成 秀紀, 田島 浩一, 西村 浩二, 相原 玲二: 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, 情報処理学会研究報告,DSM-22-8,p.45-50 (2001).

[13] 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.

[14] 802.1Q VLAN implementation for linux http://scry.wanfear.com/ greear/vlan.html