Vol.2012-EVA-39 No.12
Vol.2012-IOT-19 No.12
2012/9/28

キャンパス規模で運用可能なMACアドレス認証システムOpengateM

大谷 誠[1]　江藤 博文[1]　渡辺 健次[2]　只木 進一[1]　渡辺 義明[2]

概要：タブレットやスマートフォンなどキャンパスネットワークへの接続端末が急速に多様化している．我々はこれらに対応できキャンパス規模で運用可能な認証システム OpengateM を提案した．このシステムはゲートウェイを通過するパケットの送信元 MAC アドレスを検査してパケットの通過を制御し，利用者のログを取る．多数端末に対して MAC アドレスと所有者の情報を円滑に登録管理するために，今回，管理者が介在する登録システムに加えて，Captive Portal 型の登録システムを提案する．また負荷調査とキャンパスネットワーク環境への試験的導入についても報告する．

MAC-address Base Authentication System OpengateM Applicable to Campus Network

Makoto Otani[1]　Hirofumi Eto[1]　Kenzi Watanabe[2]　Shin-ichi Tadaki[1]　Yoshiaki Watanabe[2]

Abstract: In recent years, various mobile terminals, such as tablet type and smart phone are connected to campus networks. We propose the authentication system OpengateM which supports such various mobile terminals. This system controls Internet communication by checking the source MAC address of packets which passes the gateway, and saves users log. In order to carry out registration management of the information (MAC address and user information) on many terminals smoothly, we propose the Captive Portal type registration system, in addition to the registration system requiring administrator's intervention. This paper also describes the load of the system and the test operation in a campus network.

1. はじめに

大学において，教育研究を支援するために自由に利用できるネットワーク環境の整備は，今や必要不可欠となっている．しかしながら，自由に利用できるネットワークはトラブルが発生しやすいため，それに備えるための認証環境の整備が必要となってくる．

そこで我々は，Web ベースのネットワーク利用者認証システム Opengate を開発し，大学キャンパス全域で運用してきた．このシステムでは，Web 利用の開始時点で強制的に認証ページへ誘導して認証を行い，ネットワークを開放する．また Web ブラウザを閉じれば，即時にネットワークを閉鎖する．利用が簡単であるため，学生や教職員，訪問者等の利用者がトラブルなく利用している [1].

しかし近年では，タブレットや，スマートフォン，IP 電話など多種多様な端末が登場し，これらがキャンパスネットワークで利用されることが非常に多くなってきた．これらの端末では，画面サイズやタッチパネルの影響で，認証のためのキー入力が不便な場合がある．また，端末がマルチタスクに対する制限や，バッテリー消費節減のために無線を停止させるような機能を持つ場合には，Opengate によって満足なネットワーク環境を提供できない．また，IP 電話機やプリンタなど Web 機能を持たない端末では，Web 機能を前提とした Opengate で認証を行うことができず，個別設定が必要となる．さらに起動時からネットワークに接続されていることを前提としたシステムが増えており，

[1] 佐賀大学 総合情報基盤センター
Computer and Network Center, Saga University
[2] 佐賀大学 大学院 工学系研究科
Graduate School of Science and Engineering,Saga University

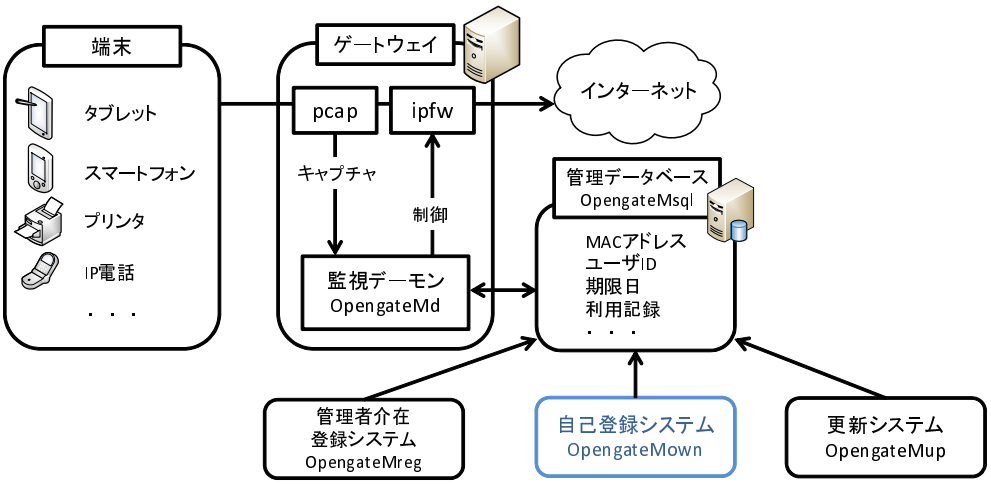

図 1 システム構成
Fig. 1 Structure of OpengateM

対応が必要となっている．

そこで，我々は，キャンパス規模で Opengate と併用可能で，多様な端末を扱えるシステム “OpengateM” を実現した [2], [3]．本システムは，特定端末のみが許可された高度なセキュリティが必要なネットワークに適用するものではなく，多様な端末が多数のユーザにより利用されるキャンパスネットワークにおいて，利用者の制限と利用記録を行うことを主眼とおり，MAC アドレス認証をベースに構築した．MAC アドレスに基づくシステムは端末互換性が高い．しかし，MAC アドレスを登録する際の手間や，MAC アドレス偽装への対応の難しさなどの弱点もある．我々はこの弱点を緩和して，キャンパスネットワークで運用可能とした．

本稿では，管理者が介在して端末を登録システムに加えて，Captive Portal 型の登録システムを提案する．また負荷調査とキャンパスネットワーク環境への試験的導入についても報告する．

2. OpengateM の概要

本システムはゲートウェイ上でパケットをキャプチャし，送信元 MAC アドレスに基づいて通過を制御するデーモンと，端末の MAC アドレスや所有者の情報を登録管理するいくつかのシステムからなる．これらについての詳細は次節で解説する．また，システム構成を**図 1** に示す．

- 監視デーモン opengateMd
- 管理者介在登録システム opengateMreg
- 自己登録システム opengateMown
- 更新システム opengateMup
- 管理データベース opengateMsql

利用者がネットワークをアクセスすると，ゲートウェイ上で動く監視デーモン (opengateMd) がそのパケットをキャプチャする．データベース (opengateMsql) に送信元 MAC アドレスが登録済みであれば，ファイアウォールを開放し，ログに利用開始を記録する．一定時間パケットが検出されなければ，ファイアウォールを閉鎖してログに利用終了を記録する．

送信元 MAC アドレスの登録が無い場合は，ファイアウォールルールに従ってパケットが処理される．例えば，Web パケットであれば，MAC アドレス登録ページへフォワードし，その他のパケットは拒否することが考えられる．本学では Web パケットを Opengate 認証ページへフォワードする設定を行い Opengate と併用する．

端末の MAC アドレスと所有者の情報は，2 つの登録システムのいずれかを使って登録する．Web 機能を持つ場合は，所有者自らが管理者の介在無しで登録できる (OpengateMown)．上記のフォワード設定があれば，未登録時には登録ページが自動表示される．それ以外の端末は，申し出により管理者が直近のアクセス履歴を確認して端末を特定し登録する (OpengateMreg)．

端末登録には期限が設定されており，期限前に更新ページの URL を示した警告メールを送付する．利用者は利用履歴を確認の上，各自で登録を更新する (opengateMup)．

なお，登録・更新ページは全て認証を行い，誰が登録・更新しているかを特定可能としている．

3. OpengateM の構成要素

3.1 監視デーモン opengateMd

opengateMd は，ゲートウェイ上で動くデーモンプロセスであり，以下の処理を繰り返すことで，パケット監視とファイアウォール制御を行う．

(1) pcap を使ってゲートウェイを通過するパケットヘッダをキャプチャし，送信元 MAC アドレスと IP アドレスを取得する．
(2) そのアドレスペアがキャッシュにあれば最近チェックしたものなので，(3)〜(6) の処理を行わず次のパケット処理へ進む．
(3) アドレスペアが開放中であるか調べる．また，MAC アドレスが管理データベースにあるか調べる．
(4) 許容される MAC アドレスであり，開放中でなければ MAC アドレスに対応する IP アドレスの通信を開放する．
(5) 許容されない MAC アドレスであり，開放中であれば MAC アドレスに対応する IP アドレスの通信を閉鎖する．
(6) 許容される MAC アドレスであり，開放中であればパケット検出時間を更新する．
(7) 定期的に，パケット検出時間を調べ，古いままの開放中 IP アドレスの通信を閉鎖する．

高速化のため，最近チェックしたアドレスペアは (3)〜(6) の処理を行わないようにしている．よって MAC アドレスの登録状態が更新されたとしても，(3)〜(6) の処理が行われない限りデーモンに状態が反映されない．そこで UDP によってアドレス登録状態の変更通知をするようにした．変更通知が届くと該当アドレスをキャッシュから消す．なお，通信が失敗した場合はキャッシュの更新後に遅延して反映される．

3.2 管理者介在登録システム opengateMreg

opengateMreg は，利用者端末の MAC アドレスを，管理者が介在して調査し登録するシステムである．利用者は，持参した端末でネットワークにアクセスする．管理者は，直近のアクセス一覧を Web ブラウザに表示し，候補アドレスを順番に短時間開放することで特定する．詳細説明は以前の [3] に記述している．

3.3 自己登録システム opengateMown

上記の管理者介在登録システムは，Web 機能を持たない，IP 電話のような端末でも対応できるが，管理者の手を煩わせることになる．大学の全構成員を対象とする場合，この運用上の手間が問題となる可能性がある．そこで Web 機能があれば所有者自ら，管理者を必要とせずに端末を登録できるシステム (opengateMown) を作成した．

このシステムは Web ベースであり，認証を経由してアクセスする．アクセスした端末の MAC アドレスを取得し，認証した利用者 ID で MAC アドレス登録を行うページを

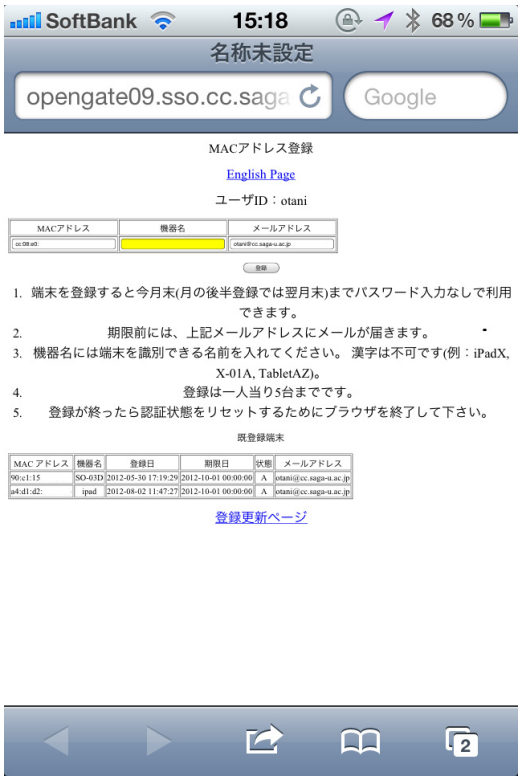

図 2 登録画面
Fig. 2 Registration page

表示する．利用者は端末名などを入力して登録する．登録ページの表示は管理者介在の登録ページとほぼ同等であるが，管理者介在ページの場合には，管理者認証下で選択した MAC アドレスが登録できるのに対して，自己登録のページでは今アクセスした端末の MAC アドレスのみが登録できる (**図 2**)．また，その端末が登録済みのときは，更新ページを表示する．なお，NAT やルータを経由したアクセスは拒否される．

本学では，通常の PC 機器では従来の Opengate を使い，当面はパスワード入力が煩雑な端末や，Opengate の利用が難しい端末のみを MAC アドレス認証に移行することを考えている．管理者介在の登録では，機器の種別判断は管理者の目視で可能である．自己登録システムにおいても機器の種別判断ができるようにするため，HTTP の User Agent 文字列を取得して，設定ファイル内の正規表現指定した許容パターンと比較している．これにより MAC アドレス認証システムを特定の端末群 (User Agent で判断できる範囲) に限定してサービスすることができる．

3.4 更新システム opengateMup

MAC アドレス登録には期限が設定してある．期限前には，更新ページの URL が記述されたメールが届く (**図 3**)．その URL にアクセスし，認証を受けて更新ページを表示すると，本人が登録している MAC アドレス一覧と，利用

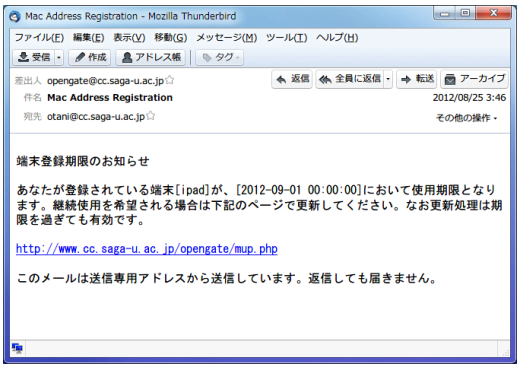

図 3 期限切れ警告メール
Fig. 3 Warning mail

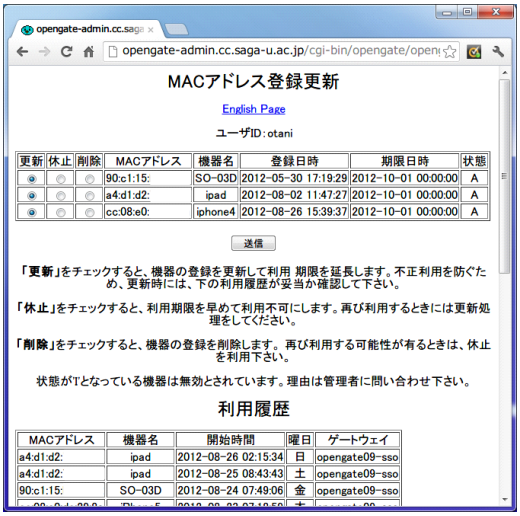

図 4 更新画面
Fig. 4 update page

履歴が表示されるので，アドレスの更新・休止・削除を指示する (**図 4**).

以上の管理者介在登録システムと自己登録システムおよび更新システムの，利用者からの利用手順を**図 5** に示す.

3.5 管理データベース opengateMsql

MAC アドレス登録テーブル，利用履歴テーブル，更新履歴テーブルなどを保持し，ゲートウェイや管理システムからアクセスする．MAC アドレス登録テーブルには，MAC アドレス・デバイス名・状態フラグ・利用者 ID・利用者メールアドレス・登録日時・更新日時・期限日時が記録されている．状態フラグは，A(Active)，I(InActive)，D(Deleted) を持つ．I は，管理者の都合により無効にされた状態であり，利用者はそれを変更できないとした．利用者自らが休止を選択すると，フラグは A のまま期限日時を早める．端末削除が指示されたらフラグを D にして保持する．これは利用履歴表示に使うためである．MAC アドレス登録テーブルは MAC アドレスをメインキーとしている．再登録を考慮して，フラグが D の場合には，メインキーに重複を許している.

4. 負荷テスト

本システムは，全パケットを検査する方式のため，ゲートウェイにおける負荷の見積もりが必要である．そこで通常の PC でクライアントマシン (CPU:3.40GHz, Memory:2GB)，ゲートウェイ (CPU:3.00GHz Core 2 Duo, Memory:4GB)，サーバマシン (CPU:3.40GHz, Memory:1GB) を構成し，1Gbps ネットワークを使って相互に接続した実験環境を作って調べた.

ゲートウェイ上のデーモンプロセスにおける各種処理時間を計測したところ，キャッシュチェックに約 1μ 秒，データベースアクセスおよびその他雑多な処理に約 10m 秒という結果であった．今回，キャッシュの保持時間を 30 分と設定しており，ほとんどのパケットは μ 秒オーダで処理されると考えられる.

また，サーバからクライアントへファイルダウンロードを行ったところ，500Mbps 程度の速度を維持できた．この際，ゲートウェイマシンの CPU 負荷は最大で 60%程度であった．さらにディスクアクセスは，転送バイト数:0.02MB/s であり busy 状態になることはなかった．また，実運用環境において iperf 等によりスループットの計測を行ったが，同等の通信性能が計測できた．以上から，最大流量においてハードウェア負荷に問題はないと考える.

次に，送信元 MAC アドレスをランダムに変化させながらパケットを送り付けるプログラムを作成して，多数端末の同時アクセスの模擬試験を行った．約 19,000 パケット/秒の送信を行ったところ，プログラム開始時に新規アドレス確認のデータベースアクセスが集中して，パケットのキャプチャ漏れが発生した.

30 分間のキャプチャ漏れ発生率は，1000 台では 1%未満であるが，1 万台では 10%，10 万台では 73%程度であった．CPU 負荷の変化から 1000 台程度であれば，すぐに処理し終えていることが確認できる．また，10 万台の同時アクセスであってもキャッシュ保持時間以内にはほぼ処理できていることから，新規アドレスでのアクセスが分散して発生する状況なら，この規模でも対応できる．ただし一時点に許可できる台数はファイアウォールが許容するルール数の上限に縛られる.

さらに，極端に端末数を増やした状態で十数時間連続アクセスしても，マシンやデーモンプロセスが停止することはなかった．アクセスが集中している際，別端末からのアクセスが通りにくい場合があるが，繰り返しアクセスすればいずれ処理されることが確認できている.

なお，処理時間を短縮するには，ローカルメモリ上に全

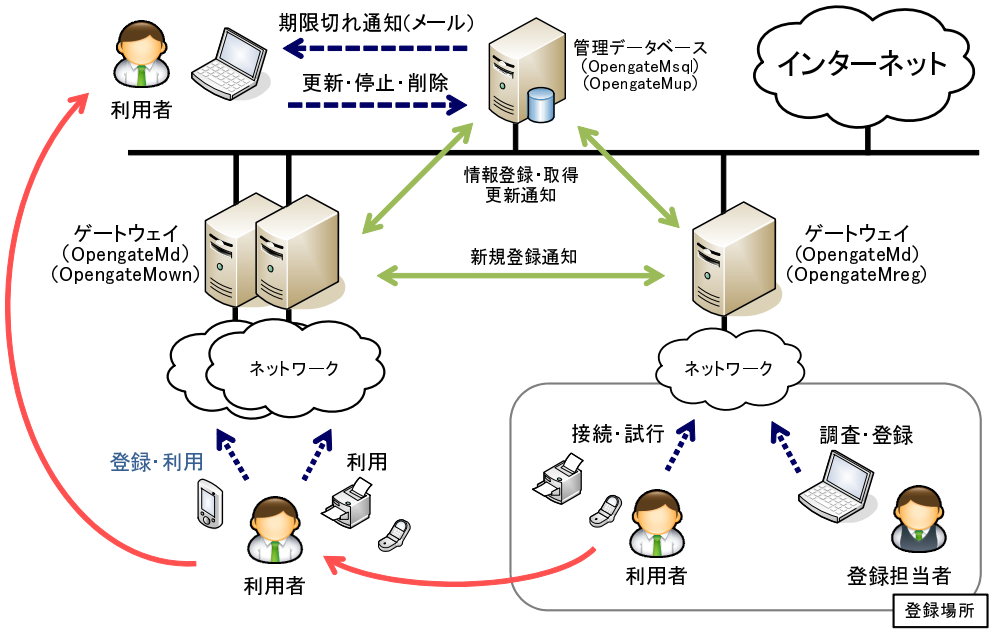

図 5 利用手順
Fig. 5 Usage flow

端末の情報を保持すれば良いと考える．しかし，以下の理由から，当面はこの方法を取らないこととした．まず，高速化するとアドレス総当たり攻撃によって，許容するアドレスを見つけ出すことが，短時間で実行できるようになる．また，情報更新時のサービス連携が複雑になる．なお本認証システムは，不正アクセスを防止するためには小さいサブネットに分割して運用する方が望ましく，一つのゲートウェイに膨大な端末数を想定しなくて良い．

5. 試験運用

本システムでは，Web 機能を持つ端末は所有者が登録ページへアクセスすれば，アクセス端末の MAC アドレスを自動取得して端末を登録することができる．Opengate 等の Captive Portal が稼働している場合は，登録ページへ誘導するリンクが可能である．本学においては，Opengate をすでに運用中である．そこで，管理者介在型の登録システムとともに，運用中の Opengate と連携し登録ページへ誘導する形での自己登録が可能とする OpengateM の試験運用を開始した．

先に述べたが，本学では通常の PC 機器では従来の Opengate を使い，当面はパスワード入力が煩雑な端末などのみを MAC アドレス認証に移行することを考えている．そこで試験運用においても HTTP の User Agent 文字列から，スマートフォンやタブレット端末と思われる端末のみ登録ページへのアクセスを可能とし，それ以外の端末を拒否する設定で運用している．管理者介在の登録では，機器の種別判断は管理者の目視によって判断する．

現在は，試験運用ということで 10 数名程度と主に関係者のみの利用であるが，iPad などのタブレット端末や，iPhone,Android などのスマートフォン端末など様々な端末が登録されており，これら登録端末が MAC アドレス認証 (延べ 238 回:2012 年 7 月の 1 ヶ月間) によって，全学で問題なく利用できている．

6. 考察

本システムの稼働には，デーモンプロセスの高速かつ安定な稼働が重要である．実際の通信制御は FreeBSD 標準であるファイアウォール ipfw に依存している．デーモンはファイアウォールに対して通過ルールの追加削除を行うのみであり，これは従来の Opengate の動作と同様で複雑ではない．

パケットはキャプチャ用の標準的ライブラリ libpcap を使用している．トラフィックが多くデーモンの処理が間に合わないとキャプチャ漏れが起こるが，繰り返しアクセスすればいずれキャプチャされるので遅延のみの問題となる．さらにデータベースの検索負荷を減らすため，一度チェックしたアドレスはキャッシュに置き一定時間無視するようにする．

キャンパスネットワークにおいては，教職員，学生，訪問者等の多様で膨大な利用者が存在する．本システムの運用には，MAC アドレスとその端末の所有者の情報を適切に収集管理できることが重要である．

まず，MAC アドレスをそのままアクセスポイント等の中継機器に設定することは，中継機器の性能や登録の手間

などに問題が出る．そこで MAC アドレスと利用者の情報をデータベースに登録しておき，利用時に必要分のみを中継システムに設定する方法とした．この方法により開始時に利用者の記録が取れるようになり，中継システムが許容する登録数とできる．本システムでは，中継システムとして Opengate と同様に FreeBSD 構成のゲートウェイを用いた．

次に MAC アドレス登録の手間削減が重要である．そこでアドレス登録においては，管理者介在の登録，所有者自らの登録を用意した．まず，Web 機能を持たない端末は，管理者が介在して登録する方法を取るが，MAC アドレスはマニュアル設定ではなく調査ページを用いて容易に決定できるようにした．さらに Web 機能を持つ端末では，所有者が登録ページへアクセスすれば，アクセス端末の MAC アドレスを取得して登録できるようにした．さらに，この登録ページを Captive Portal ページとして設定できるようにした．利用者は，端末を使って Web アクセスすると，MAC アドレスが登録されていればそのまま利用でき，未登録の場合は登録ページが表示される．既に Opengate 等の Captive Portal が稼働している場合は，そのページから登録ページへ誘導するリンクも可能である．他に，MAC アドレスと利用者 ID の一覧表を組織的に作成できるなら，SQL スクリプトを使ってデータベースに登録する方法も可能である．

さらに登録状態を適切な状態に維持することも必要である．そこで，登録には期限を設けて，定期的に更新しなければ使えなくなるようにした．期限前には，更新ページの URL を付加した警告メールを送り更新を促すとともに，更新ページをホームページ等にリンクして，期限切れ後も更新可能とした．また期限切れした端末で Web アクセスすると，登録ページの代わりに更新ページが表示されるようになる．なお更新時は，過去の利用履歴を提示し，不正な利用がされていないか確認させる．

他人への端末譲渡の際には，更新ページにおいて登録を削除すると新たな利用者の端末として登録できる．元の利用者が削除しないまま放置した端末は，期限切れ休止状態にあり新たに登録できない．元の利用者に削除してもらうか，管理者権限の操作を依頼する必要がある．卒業時期には多数の期限切れ休止端末が発生すると考えられる．大学の認証サーバに登録がない利用者 ID の端末を定期的に削除する処理も入れた方が良いと考える．

MAC アドレスをベースとした認証の実現には様々な方法が考えられる．ファイアウォールに MAC アドレスベースの許可ルールを登録する方法や，無線端末の場合は無線 LAN のアクセスポイントに接続を許容する MAC アドレスを登録する方法が考えられる．これらの方法は，登録する MAC アドレス数が膨大になると機能しない．MAC アドレスによる振り分けをサポートした認証スイッチを用いる方法も実際に用いられている [4], [5], [6]．本システムでは，特別な機器を採用せず，一般的なハードウェアおよびオープンソースソフトウェアを用いたシステムとして構築した．

7. まとめ

キャンパス規模で Opengate と併用可能で，タブレット型を含む多様な携帯端末に適用可能な認証システムを，MAC アドレス認証をベースに実現した ．本システムは，管理データベースに所有者情報を含む端末情報を一元化し，キャンパス規模でも利便性とセキュリティを保持することが可能である．管理者が介在して端末を登録するシステムに加えて，今回は Captive Portal 型の登録システムを提案するとともに本学において試験導入した．

本システムは，全パケットを検査し認証を行うシステムであり，ゲートウェイにおける負荷を考慮する必要があると考え，負荷テストをあわせて行った．1Gbps のネットワークにおいて，十分な帯域を確保できるとともに，CPU 等の負荷においても実運用上問題のない計測結果を得ることができた．今後は，利用者数を大学の全構成員にまで拡大するとともに，大規模運用における，より一層の利便性の向上と，管理者の負担減を検討したい．

参考文献

[1] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明, “ シングルサインオンに対応したネットワーク利用者認証システムの開発”, 情報処理学会論文誌, Vol.51, No.3, pp.1031-1039 (2010)
[2] 渡辺義明 他, “OpengateM － MAC アドレスに基づくネットワーク利用者認証システム”, http://www.cc.saga-u.ac.jp/opengate/opengatem/
[3] Opengate を補完する MAC アドレス認証システム OpengateM, 渡辺義明, 大谷誠, 江藤博文, 只木進一, 渡辺健次, 情報処理学会研究報告, 2011-IOT-16, pp.1-6, 北海道大学 (2012.03.16).
[4] 田島浩一, 近堂徹, 岸場清悟, 大東俊博, 岩田則和, 西村浩二, 相原玲二, “大規模キャンパスネットワークにおける MAC アドレス認証の管理手法”, 情報処理学会研究報告, 2009-IOT-4, pp.265-270 (2009)
[5] 谷内田正寿, 白清学, “MAC アドレス認証と Web 認証併用キャンパスネットワークの導入”, 学術情報処理研究, No.14, pp.140-143 (2010)
[6] 浜元信州, 五十嵐瑛介, 青山茂義, 三河賢治, “ホスト登録システムを利用したネットワークアクセス認証システムの運用”, 情報処理学会研究報告, Vol.2010-IOT-9,No.4, pp.1-6 (2010)