Vol.2012-IOT-16 No.25
2012/3/16

Opengateを補完するMACアドレス認証システムOpengateM

渡辺義明[†1] 大谷誠[†2,†3] 江藤博文[†2]
渡辺健次[†1] 只木進一[†2]

タブレット型を始めとする多様な携帯端末の普及により，Web 認証型の利用者用ネットワーク管理は改善を求められている．一方，組織内ネットワークとして適切に利用者認証が必要であることには変わりがない．そのため，従来の Web 型利用者認証を補完する MAC アドレス認証システムを提案する．提案システムは，利用者認証情報と連携した端末情報を管理，更新および記録し，利便性とセキュリティを保持することが可能である．

OpengateM: MAC-address Base Authentication System Complementary To Opengate

Yoshiaki Watanabe,[†1] Makoto Otani,[†2,†3]
Hirofumi Eto,[†2] Kenzi Watanabe[†1]
and Shin-ichi Tadaki [†2]

The Web-based network user authentication should be revised, because of the spread of various mobile terminals, such as tablet type, smart phone and IP phone. But, as ever, the user authentication is neccesary for the network in an organization. We propose a MAC address base authentication system complementary to the conventional Web-based user authentication. The system manages the terminal information matching to the user and records usage log. It can maintain convenience and security.

1. はじめに

大学においては，教育研究を支援するため自由に利用できるネットワーク環境の整備は必要不可欠である．一方，ネットワーク上で頻発するトラブルに備えるには，確実な認証環境を構築する必要がある．

我々は多様な端末に適用可能な 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，2001 年から大学キャンパス全域で運用している．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．この平易なインターフェースのため，学生や教職員，訪問者等の広範囲の利用者が特別な指導なしにトラブルなく利用している．さらに，最近ではシングルサインオンにも対応した[1)]．

しかし最近では，タブレット型端末を始めとする多様な携帯端末のネットワーク利用要求が増加している．これらの端末では，キー入力が不便であることやマルチタスクに対する制限などから Opengate が使いにくくなっている．また IP 電話機やプリンタなどの，Web 機能を持たない端末の利用要求もあるが，Web 機能を前提とした Opengate では使うことができず，個別設定が必要となる．

無線 LAN の認証として 802.1x を始めとする各種の方式も存在するが，これらは端末の互換性や端末設定の煩雑さなど，利用者および管理者にとって使いやすいものとなっていない．

そこで本研究では，これらの端末を包括的に認証でき，Opengate を補完するシステムを提案する．このシステムは，種々雑多な端末に適用可能とするため，端末の持つ固有 MAC アドレスを利用するが，キャンパス規模でも問題なく運用できるようにセキュリティと管理機能を高め，さらに Opengate と同一のゲートウェイ上で併用できるシステムとする．

MAC アドレスをベースとした認証 (以下 MAC 認証）の実現には様々な方法が考えられる．簡単には，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 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

†1 佐賀大学 理工学部
Faculty of Science and Engineering, Saga University
†2 佐賀大学 総合情報基盤センター
Computer and Network Center, Saga University
†3 国立情報学研究所 学術ネットワーク研究開発センター
Research and Development Center for Academic Networks, National Institute of Informatics

る．しかしこれらの方法は，登録する MAC アドレス数が膨大になると機能しない．また DHCP サーバにサービス提供可能な端末の MAC アドレスを登録する方法は，ネットワーク設定を直接入力することで回避できる．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考えられるが[2)–4)]，本研究では，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前提としたシステムを提案する．

2. Opengate の制約

Opengate は，Web 利用開始時に認証ページを強制表示する Captive Portal として動作し，平易に利用できる．また，利用終了の監視を，Ajax スクリプトを使った TCP 接続で実現しているため，監視ソフトウェアのインストールが不要であり，端末の互換性が高い．

しかし上記の方式のため Opengate は Web 機能の存在が前提となる．また終了監視のため，利用中のネットワークサービスと別に，Ajax スクリプトがバックグラウンドで稼働することが必要となる．しかし最近，端末の中に，この前提を満たさないものが増加している．さらに Opengate は，利用開始時にユーザ ID とパスワードのキー入力を要求するが，携帯端末の多くはキーボードを備えていないために入力が面倒である．Ajax スクリプトによる終了監視ができないときは一定時間後に閉鎖する時間監視モードに移行することで対処しているが，Web 機能は必須である．

3. 補完システム OpengateM の提案

提案するシステムは，Opengate においても追求される以下の要求事項を最大限満たし，Opengate を補完するシステムを目指す[5)]．

(1) 利用登録された利用者のみにネットワークの利用を許可し，各利用者の利用記録が取れること．
(2) 利用者にとって平易に利用でき，指導や設定などの教育負担を低減できること．
(3) 汎用のハードウェアとソフトウェアを利用し，システムの導入と運用の負荷が小さいこと．
(4) できるだけ多様な端末に適用可能であること．
(5) キャンパス規模のサービスができること．
(6) 多様なネットワーク環境や利用形態に柔軟に適用できること．
(7) 十分なセキュリティが保てること．

多様な端末に適用させるには，MAC 認証を採用することが妥当である．しかし，ファイアウォールや無線 LAN アクセスポイントに MAC アドレスを登録する方法では，利用者ごとの利用記録の取得や大規模運用に問題がある．

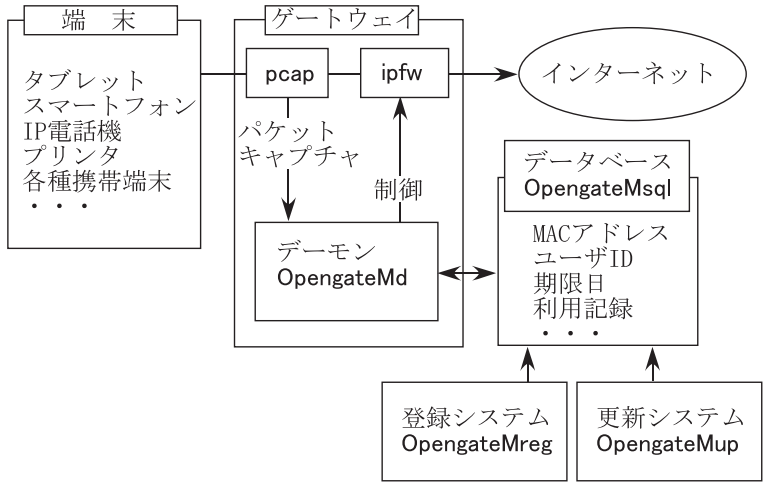


図 1 システムの構成
Fig. 1 Structure of OpengateM

そこで本システムでは，ゲートウェイを通過するパケットのヘッダをキャプチャして MAC アドレスを調べ，許容する端末をファイアウォールに登録し，利用が無くなれば登録を削除する方法を取る．許容する MAC アドレスとその所有者はデータベースで集中管理する．この方法によれば，ファイアウォールのルール数は，登録端末数ではなく，ネットワークを利用中の端末数と同程度であり，現状の Opengate の実績から見て問題ないと考える．またデータベースの情報から，利用者ごとの利用記録を取れる．MAC 認証の難点として MAC アドレスの詐称があるが，この対策として利用許可に期限を設定し，許可期間の延長申請時には利用記録を利用者に提示し確認させる方法を取る．

本システムの中心部分は，ゲートウェイ (OS:FreeBSD) 上でパケットを監視し，ファイアウォールを開閉するデーモンプロセス (OpengateMd) である (図 1)．デーモンはパケットキャプチャAPI(pcap) を使って，ゲートウェイを通過するパケットのヘッダをキャプチャする．ヘッダに含まれる MAC アドレスを管理データベースで調べ，許容するアドレスであれば，ファイアウォール (ipfw) に対して，そのアドレスに対する通過許可ルールを追加す

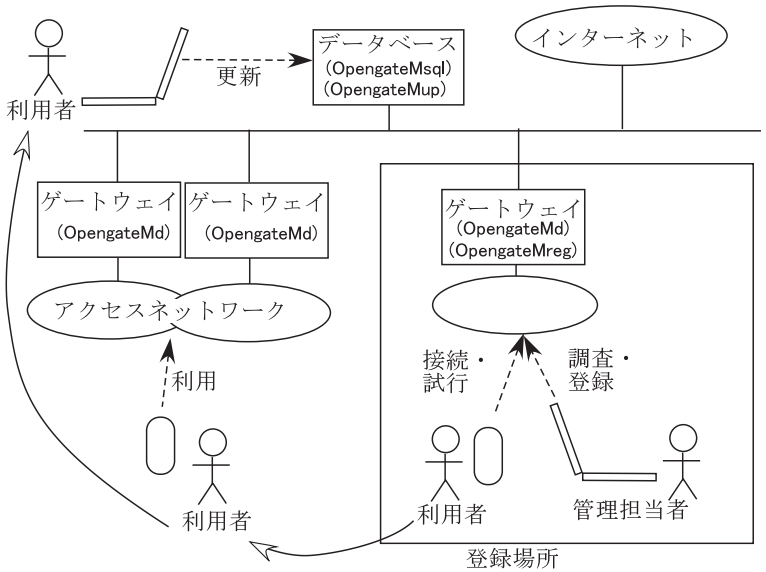


図 2 利用手順
Fig. 2 Usage flow

る．一定時間，検出されない MAC アドレスに対応するルールは削除する．なおルールは，Opengate と共存する必要から IP アドレスベースで設定している．

本システムには，このデーモンプロセスのほかに，データベースへ端末情報を登録し，管理・更新するためのサブシステム群が必要である．この詳細は後述する．

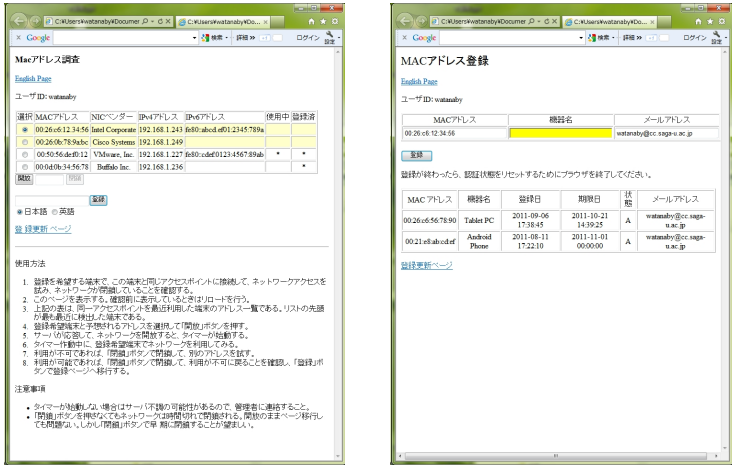
4. OpengateM の利用手順

利用手順を図 2 に示す．端末情報の登録，ネットワークの利用，利用期限の更新の順に実施する．

4.1 端末情報の登録

利用端末の登録は，セキュリティ保持および Web 機能無し端末への適用を考慮して，現状では管理者の介在を必要とする体制を採用している．

利用希望者は，利用を希望する端末を持って，情報センター等に設置された登録場所へ行き，管理担当者に登録を依頼する．管理担当者は以下の手順を実行する．



(a) (b)

図 3 登録時の表示 (a)MAC アドレス調査ページ (b)MAC アドレス登録ページ
Fig. 3 Registration interface (a)Address check page, (b)Registration page

(1) 利用希望者に，登録を希望する端末でネットワークアクセスを行わせ，ネットワークが利用できないことを確認させる．

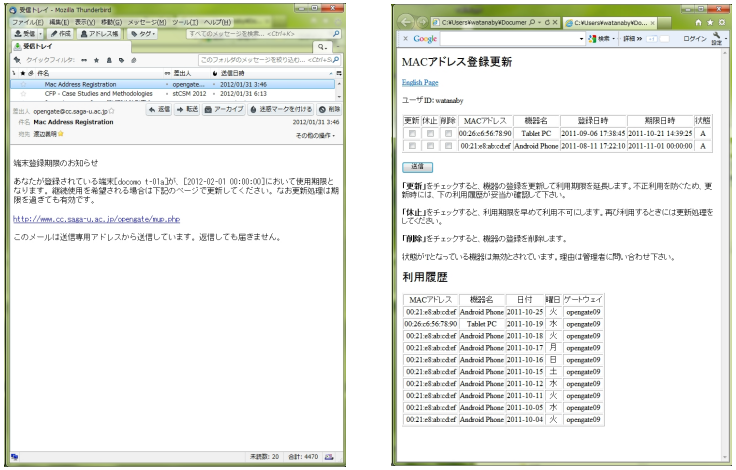
(2) 登録希望端末と同じネットワークに管理用端末で接続して，MAC アドレス調査ページを表示する．ページには同一ネットワークを最近利用した端末のアドレス一覧が表示される (図 3(a))．一覧には MAC アドレスに対するベンダー情報，OpengateM の使用中・登録済みマークを付記し，可能性のある行を色付けして検出時間の新しいものから順に表示する．なお，このページの表示には管理者認証の通過が必要である．

(3) 一覧から登録希望端末であると予想されるアドレスを選択して「開放」ボタンを押す．先頭が最も新しく検出した端末であり可能性が高い．

(4) 「開放」ボタンを押すとネットワークが一定時間（例: 1 分）だけ開放するので，その間に登録希望端末でネットワークを利用させる．

(5) 利用が不可であれば,「閉鎖」ボタンで即時閉鎖して別アドレスの開放を試す．利用が可能であれば,「閉鎖」ボタンで即時閉鎖して利用不可に戻ることを確認し「登録」ボタンを押す．

(6) 利用希望者の認証が要求されるので，利用希望者にキーボードを操作させて，必要事



(a) (b)

図 4 更新時の表示 (a) 期限切れ警告メール (b) 登録更新ページ
Fig. 4 Update interface (a)Warning mail, (b)Update page

項の入力と登録を行わせる (図 3(b)).

4.2 ネットワークの利用

利用者が登録端末を使ってネットワークにアクセスすると，デーモンが MAC アドレスを確認して，ファイアウォールに通過ルールを挿入する．このため最初の通過は若干遅延すると考えられるが，試行する限り問題は起きていない．また多くのシステムは利用者が要求する前にバックグラウンドで通信を始めており，利用者のアクセス時には既に開放されている．

一定時間 (例: 3 時間）連続してネットワーク利用が無いと，デーモンがファイアウォールからルールを削除する．その後に再度ネットワーク利用が起きると改めてルールが追加される．

4.3 利用期限の更新

一定期間 (例: 1ヶ月) が経過すると利用期限が切れる．

期限切れの直前 (例: 1 週間前と 1 日前) には，端末登録時に登録したメールアドレスに期限切れの警告メール (図 4(a)) が届く．利用者は，記載されている URL にアクセスして更新ページ (図 4(b)) を表示し，利用記録を確認して期間延長を行う．更新処理には管理担当者は介在しない．

5. OpengateM の構成

OpengateM は以下に示すシステムから構成される。これ以外に登録更新時に利用者を認証するサーバが必要である。

5.1 監視デーモン OpengateMd

パケットを検知してファイアウォールを開閉するデーモンプログラムである．全てのゲートウェイに導入する．以下の動作により，利用者が任意のプロトコルでネットワークにアクセスするだけで利用可能とするプログラムである．

ゲートウェイを通過するパケットのヘッダをキャプチャし，それに含まれる MAC アドレスを登録データベースで検索する．登録が確認されれば，その端末に対するファイアウォールを開放し，利用ログを記録する．開放した MAC アドレスを含むパケットが一定時間通過しなければ，その端末に対するファイアウォールを閉鎖する．なお，パケットごとにデータベース検索を行うのは負荷が大きいため，デーモン内にキャッシュを設け，一度データベース検索したアドレスはプログラム内にしばらく保持する．

5.2 登録システム OpengateMreg

管理担当者が，利用者の MAC アドレスを調査して登録する Web ベースのシステムである．登録場所をカバーする無線ネットワークのゲートウェイに導入する．

MAC アドレス調査ページでは，ARP，NDP およびデーモンが取得した情報を用いて，検出時間の新しい方から順に並べたアドレス一覧を表示する.「開放」ボタンによる一時開放の要求が来れば，ファイアウォールを開放して一定時間後に閉鎖する.「閉鎖」ボタンによる即時閉鎖の要求が来れば閉鎖する．また「登録」ボタンによる登録要求が来れば，最後に一時開放したアドレスを持って登録ページへ移行する．

MAC アドレス登録ページでは，利用者の認証を通過後，調査ページから渡されたアドレスと認証通過したユーザ情報を対にし，追加入力された端末名等も加えてデータベースに保存する．

5.3 更新システム OpengateMup

利用期限を警告するメール自動発信システムと，それを受けて利用者が登録 MAC アドレスの利用期限を延長する Web ベースシステムとからなる．管理データベースをアクセス可能な場所に導入する．

5.4 管理データベース OpengateMsql

MAC アドレスや利用記録を保持する管理データベースシステム (MySql) である．他の

システムからアクセス可能な場所に導入する．多数のゲートウェイはこのデータを元にして連携動作する．

6. 考　　察

本システムの特徴と工夫点を以下に列挙する．

(1) Opengate と同じゲートウェイ上で併用可能な Opengate 補完システムであり，どちらか一方のシステムで許可されればネットワーク利用ができる．また Web 利用の時は，OpengateM で許可された端末は認証ページ無しでネットワーク利用ができ，許可されない端末では Opengate の認証ページに自動移行する．さらに本システムは，Opengate 無しの使用形態も可能である．

(2) 端末に要求するのはネットワーク接続機能のみである．アクセスポイント機器や端末機器のサポートする認証規格などに依存せず，ほとんど全ての端末機器を包括できる．ただし不特定多数が共用する端末には向かない．

(3) Web 機能を持たない端末に対して MAC アドレスを調査し登録する仕組みを実現した．現状では全ての登録に管理者が介在する方法を取っているが，多数利用者に対応するため，Web 機能を持つ端末については管理者の介在無しで登録する方法も今後検討する．

(4) ネットワークを利用中の端末のみをファイアウォールルールに追加する方式であり，登録利用者が膨大でも適用可能である．ただし同一ネットワークで同時に利用される端末数はゲートウェイやファイアウォールの処理能力に制限されるため，同時利用が多いときは，ゲートウェイ数を増してネットワークを分離する事を考える必要がある．

(5) Opengate との併用のため，ファイアウォールルールは IP アドレスベースとした．ファイアウォールルールを工夫することで，特定のポートやサイトの許可や不許可なども制御も可能である．なお，IPv4 と IPv6 両環境に対応している．

(6) 利用者管理はデータベースに集約されているため容易である．個別のアクセスポイントやファイアウォールなどへのアドレス登録管理作業は不要である．

(7) ゲートウェイからデータベースへのアクセスは負荷が大きいので，一度取得した情報はキャッシュに保持することでパフォーマンスを確保している．データベースが更新された時は，UDP 通信を使って各ゲートウェイへ即座に通知が送られるので，速やかに利用が可能になる．なお，キャッシュは保持時間 (例: 20 分) 後にリフレッシュされる．

(8) 汎用のハードウェアとオープンソースソフトウェアを利用しており，導入と維持コストが少ない．Opengate が稼働しているネットワークであれば，運用を継続したままソフトウェアを付加するだけで済む．

(9) 単純に MAC アドレスをアクセスポイント等に登録する方法と異なり，利用者に対応した利用記録を取れる．

(10) MAC アドレスは詐称の可能性があることを考慮し，利用期限を設定している．期限前には警告メールが届き，利用者自身が利用記録をチェックの上で期間の延長を行う方式としており，不正利用に気付きやすい．更新ページでは，期限延長以外に削除や一時休止が可能である．その URL は警告メールやホームページ等を通じて告知する．

(11) MAC 認証のためルータや NAT を経由して使えない制限がある．そこでパケットキャプチャ時の TTL(Time to Live) 値と標準的システムの初期 TTL 値を比較することで，ルータや NAT を検出する仕組みを導入した．Opengate は，ルータ経由で使用できるが，NAT 経由で一人が認証すると他の利用者も使えるようになる問題がある．上記の検出結果を使うと NAT 経由の利用を発見できる．

(12) Opengate のモジュールを流用しており，データベース登録更新時の利用者認証に多様な方式を使える (POP3，FTP，RADIUS，LDAP，PAM，Shibboleth，Http-Basic)．

7. ま と め

従来の Web 型利用者認証である Opengate を補完してタブレット型を含む多様な携帯端末に適用可能な MAC アドレス認証システムを提案した．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ており，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．

現在，少数台の端末を登録して試行運用を開始している．今後，登録端末の台数を徐々に増加して，問題点を洗い出したい．また Captive Portal 型の登録・更新システムを含めて，大規模運用における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) 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)
3) 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)
4) 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)
5) 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/