MAC アドレス認証システム OpengateM の紹介

総合情報基盤センター
大谷　誠

1. はじめに

大学において、教育や研究を支援するために PC を自由に利用できるネットワーク環境は、今や必要不可欠となっています。しかし、PC を自由に接続できるネットワークは、セキュリティなどに関するトラブルが発生する可能性があります。よって、誰がいつネットワークを利用したか等を把握するための認証環境が必要となります。

総合情報基盤センターでは、Web ブラウザを利用して認証するネットワーク利用者認証システム Opengate を開発し、2001 年頃よりキャンパス全域で利用できるようにしてきました。この Opengate は、認証していない PC が Web を利用しようとする場合に強制的に認証を行うページに誘導します。そして認証に成功した場合はネットワークを利用できるようになります。また、認証を行った Web ブラウザを閉じることでネットワークの利用終了(ネットワークの利用が不可)となります。

このように Opengate は佐賀大学の学生や教職員が簡単に利用できるシステムとなっています。来訪者の方や、佐賀大学で開催される研究会に参加される方などにも申請を行うことによって、利用してもらうことが可能です。また学認[1]に参加している組織の方は、申請なしに利用すること可能で、様々な利用者に対応しています。

しかし近年になって、この Opengate に PC 以外の様々な機器が接続されるようになってきました。たとえば、スマートフォンや、タブレット端末、IP 電話機といったような機器です。このような機器は画面サイズが小さかったり、タッチパネルが搭載されていたりと、PC に比べ認証情報を入力することが難しい面があります。また、マルチタスクに対する Web ブラウザの制限や、バッテリー消費節減のために通信を停止させるような機能を持つ機器には、Opengate によって満足なネットワーク環境を提供できません。IP 電話機やプリンタなど Web 機能を持たない機器では、Opengate で認証を行うことができずに個別の対応が必要となります。その他に、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やソフトウェアも増えており、これらの問題に対応する必要が出てきました。

そこで、Opengate と併用が可能で、多様な機器を扱うことのできる OpengateM を新たに開発しました。この OpengateM は、各機器に割り当てられている MAC アドレスを認証に用います。利用する機器の MAC アドレスをあらかじめシステムに登録しておくことで、Opengate

[1] 学術認証フェデレーション, http://www.gakunin.jp

による認証を行う必要がなくなるというシステムです。本稿では、この OpengateM について簡単に紹介します。

2. OpengateM の概要

OpengateM では使用する機器の MAC アドレスを登録し、その登録された MAC アドレスを持つ機器の通信を自動的に許可します。具体的には、OpengateM がネットワークを流れる通信(パケット)を常に監視(キャプチャ)しておき、登録された MAC アドレスの端末の通信を確認したら、ファイアウォール(ipfw)で許可するという流れになります(**図 1**)。逆に通信が一定時間確認できなくなったらファイアウォールを閉鎖します。また、利用記録などを管理データベースに保存し、利用者が確認できるような仕組みも入っています。

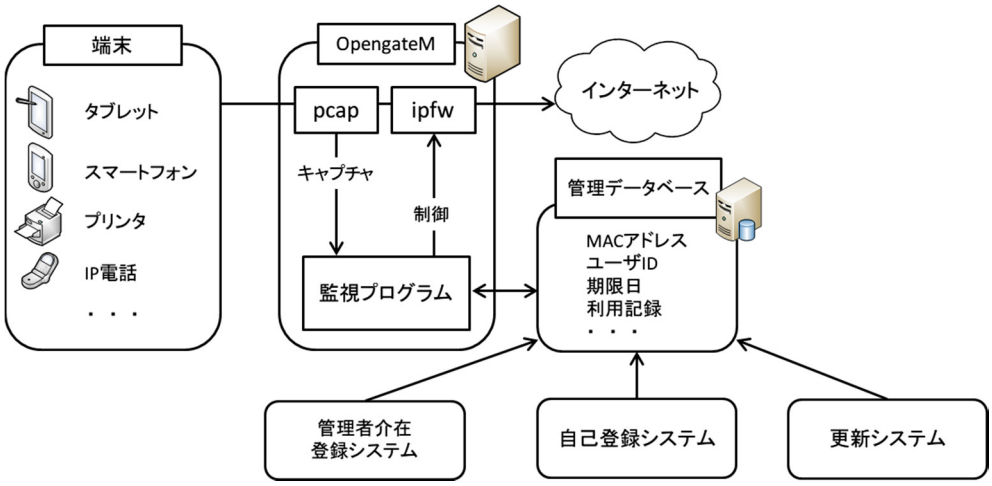

図 1 システムの構成図

利用する機器の登録方法には主に 2 種類あります。利用者が直接登録する方法(自己登録システム)と、管理者に登録を依頼する方法(管理者介在登録システム)です。

2.1. 自己登録システム

利用者が直接登録する自己登録システムでは、機器を登録する際にまず Opengate で今まで通り認証します。Opengate では認証に成功した際に認証許可ページと呼ばれるページが表示されます。このページを表示している間はネットワークの利用が可能です。このページを閉じることでネットワークの利用を終了したと判断します。OpengateM では、この認証許可ページに登録用のリンク(**図 2**)を設置します。機器を登録したい場合は、そのリンクをクリックすることで機器の登録が可能となります。

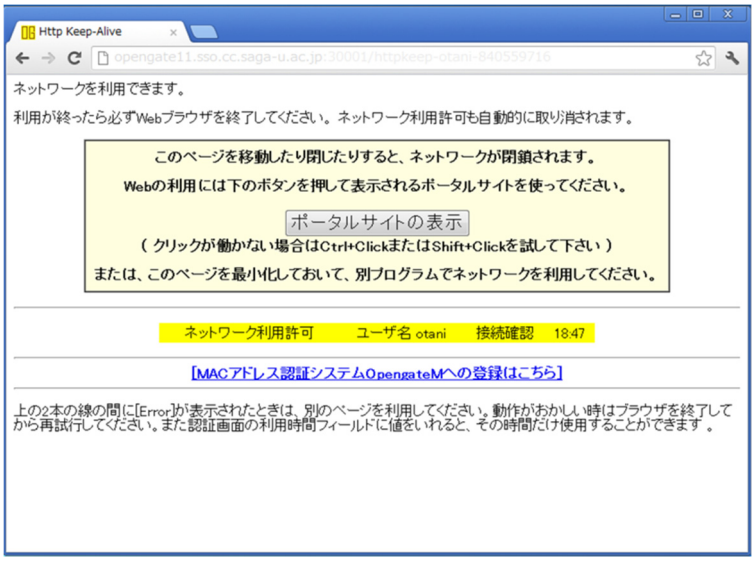

図 2 認証許可ページと OpengateM 登録用リンクの例

登録リンクをクリックすると、登録画面(図 3)が表示され、後は登録する端末を識別するための名前(機器名)を付けて「登録」ボタンを押すと登録完了です。利用者は、わざわざ登録したい機器の MAC アドレスを調べる必要はありません。登録が完了すると、次回からは Opengate の Web による認証が不要になります。

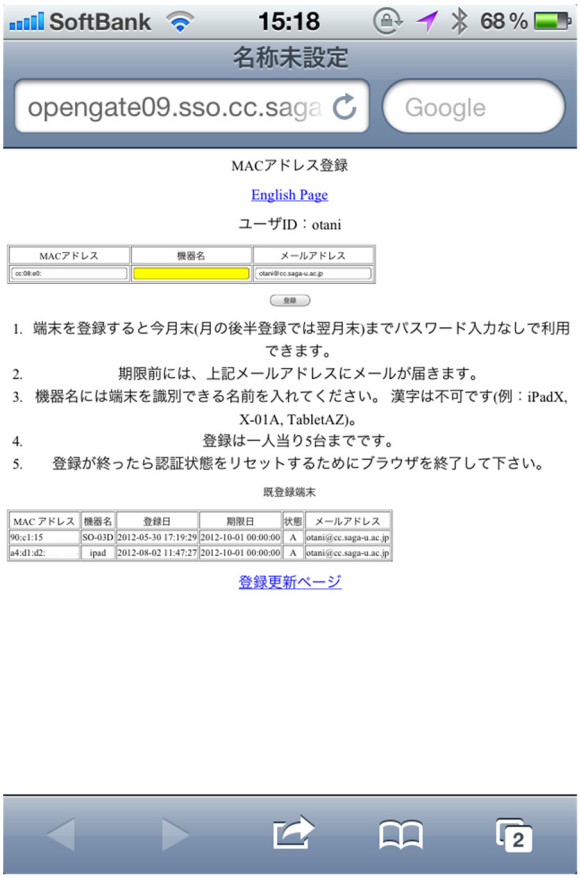

図 3 登録画面(iPhone における登録画面)

2.2. 管理者介在登録システム

自分で自ら機器の登録を行う自己登録システムでは、従来通りにまずは Opengate で認証し、次に認証許可ページにある登録用のリンクを経由して端末を登録する方法となっています。しかしながら、はじめに述べたように Web ブラウザの機能を持たないような IP 電話機やプリンタといった機器は、この方法では登録できません。そこで、別途利用者が介在して機器を登録するためにシステムも導入しています。管理者が登録を行う場所に実際に機器を持ってきてもらいそこでネットワークに繋ぐと、その機器の MAC アドレスが自動的に調査され、その MAC アドレスを管理者が登録する仕組みとなっています。

2.3. 更新システム

機器が一度登録されると、Web ブラウザの認証なしにネットワークが利用できるため、登録した端末を利用しなくなった場合を定期的に登録から消す仕組みも実現しています。それが更新システムとなります。登録の際に利用期限が設定されており、利用期限が近くなると、利用期間を延長するかを確認するメール(図 **4**)が利用者に届きます。

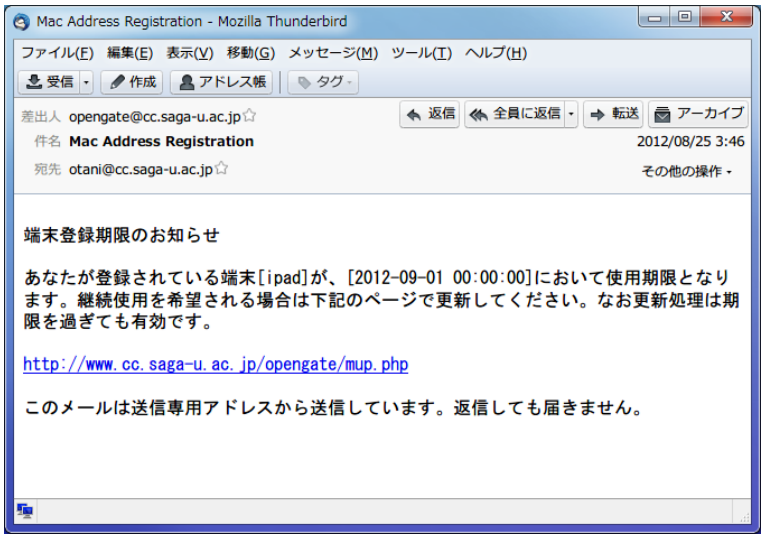

図 4 期限切れ警告メール

このメールに書かれているリンクにアクセスすると、利用の延長や一時的な停止などの申請(図 **5**)を行うことができます。この更新申請は、特に登録を行った機器で行う必要はありません。登録している機器が複数ある場合には同時に更新することが可能です。

図 5 MAC アドレス登録更新画面

登録画面には、これまで登録した機器の利用履歴が表示されます。不正な利用を防ぐため、更新時に利用履歴が妥当なものであるかを確認してもらうようになっています。以下が OpengateM の全体的な利用のイメージとなります。

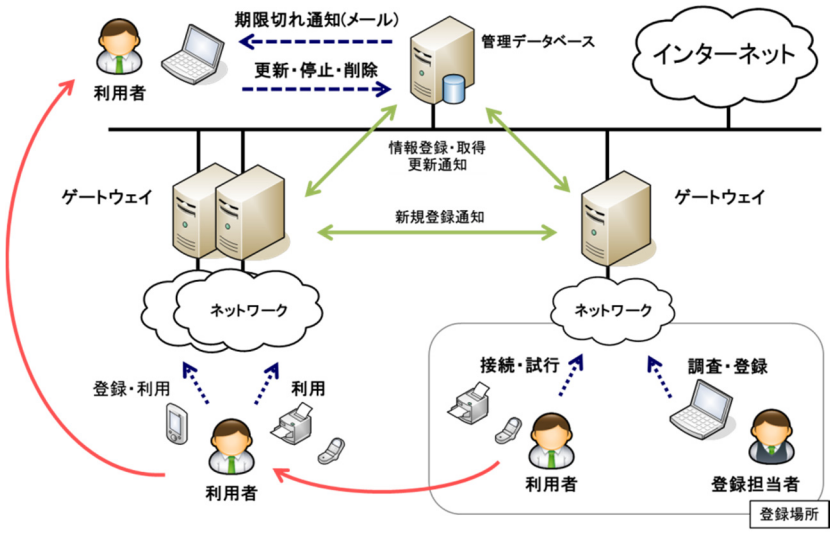

図 6 OpengateM の利用イメージ

3. おわりに

Opengate によるネットワークの利用に不向きなスマートフォンや、タブレット端末、IP 電話機等に対応するため、機器の MAC アドレスをベースに認証を行う認証システムである OpengateM を開発しました。この OpengateM は、現在(2012 年末)全学において利用できるようになっていませんが、近々、学内でだれもが利用できるような状態で公開する予定です。その際は是非ご利用いただければと思います。