マルチステップ認証導入に伴うゲスト利用について

板倉 紀子、島岡 章

大分大学 学術情報拠点（医学情報センター）

itakura@oita-u.ac.jp

概要：大分大学挾間（医学部）キャンパスでは、Web 認証と MAC アドレス認証を併用したマルチステップ認証を導入し、あわせてセキュリティ対応が行われていないパソコンは接続を許可しないこととしている。大学では，来客者の持ち込みパソコンなど、未登録のユーザや機器をネットワークに接続したいことがある。本報では、マルチステップ認証を補完するための対策として、ゲスト用ＩＤとゲスト用 VLAN、ゲスト用プロキシサーバからなるゲスト利用システムを構築し、運用を開始したので報告する。

1　はじめに

ここ数年、情報セキュリティの確保のために、マルチステップ認証を導入する大学が増えてきている[1][2][3][4][5]。大分大学挾間（医学部）キャンパスでも、2011 年に、MAC アドレス認証と Web 認証とを併用したマルチステップ認証を導入し、あわせて、セキュリティ対応が行われていないパソコンは接続を許可しないこととしている[6]。この導入に伴う不都合な点を補完するための対応策として、ゲスト用ＩＤとゲスト用 VLAN、ゲスト用プロキシサーバからなるゲスト利用システムを開発した。

2　マルチステップ認証の導入とその問題点

2.1 マルチステップ認証

図１に、導入当初のマルチステップ認証の流れを示す。MAC アドレスが未登録である場合、ユーザＩＤとパスワードの組み合わせが登録されていない場合は、いずれも、ネットワーク接続が拒否される。 ネットワークを利用する個人の責任を明確にするするために、グループＩＤでの認証は許可していない。

2.2 接続するパソコンのセキュリティ要件

挾間キャンパスでは、ネットワークセキュリティを確保するために、キャンパスネットワークに接続するパソコンは、OS や Adobe Reader 等のアプリケーションソフトの脆弱性に対してセキュリティ更新を行い、さらにワクチンソフトを最新の状態で機能させることを要求している[6][7] [8]。

2.3 問題点

マルチステップ認証を導入すると、その目的そのものではあるが、未登録の人は利用できない、未登録のパソコンは接続できない状態となる。

来客がキャンパスネットワークを利用したい場合や機器納品業者の設定作業などの場合に、未登録の人に代わって、登録済みの職員がＩＤパスワードを入力して、その機器を利用させる、という好ましくない状況が起きていた。また、職員が新規に購入したパソコンは、ＯＳの最新のセキュリティ更新が行われておらず、ワクチンソフトがインストールされていなかったり、定義ファイルが古い状態である。これを最新の状態にしないと接続許可を出さないことにしているので、キャンパスネットワークに接続できないという矛盾が生じていた。

3 ゲスト利用システムの構築

3.1 ゲスト利用システム

図２に、従来のマルチステップ認証にゲスト用 ID、ゲスト用 VLAN、ゲスト用プロキシサーバで構成されるゲスト利用システムを組み込んだシステムの概要を示す。

MAC アドレスが未登録のパソコンをキャンパスネットワークに接続すると、未登録であるという情報とともに中間 VLAN に入る。Web 認証で、ゲストＩＤとパスワードでログインすると、ゲスト用 VLAN に入る。

MAC アドレスが登録済みのパソコンでは、ゲ

スト ID を使っても、ゲスト VLAN には入れず、エラーとなる。ユーザ登録されているＩＤでは、ユーザごとに登録された VLAN に入るため、ゲスト用 VLAN には入れない。

3.2 ゲスト用ＩＤ

ゲスト用ＩＤとして２種類のＩＤを用意している。いずれも職員が申請し、職員に交付される。持ち込みパソコンのセキュリティ対応状況は、ゲストＩＤを申請した職員の責任においてチェックすることになっている。

(1)　ワンデイアカウント

職員がオンラインで申請をすると、即時にメールで申請者宛に、ＩＤパスワードと利用方法が書かれた添付ファイルが送信される。これを申請者のパスワードで開封する。発行の翌朝８時まで有効である。

来客、研究会などの一時利用、搬入機器の動作確認（業者）用などの利用を想定している。

学生の場合は、医学情報センターで発行する。

(2)　短期滞在者用ゲストＩＤ

職員がメールで申請し、センターからメールの返信で交付する。有効期間は１か月である。

短期留学生、短期研究員の利用を想定している。

3.3 ゲスト用ＶＬＡＮ

ゲスト用 VLAN は、学外のサイトには接続できるが、キャンパス内のセキュリティを確保するために、学内のサーバや学内ユーザの VLAN には接続できないように、幹線通信機器のアラクサラで制御している。

3.4 ゲスト用プロキシサーバ

ゲスト用 VLAN は、ゲスト用プロキシサーバ以外の学内のサーバには接続できない。ゲスト用プロキシからは学外のサイトに接続できるだけで、学内のサーバには接続できないように設定している。

4 利用状況

2012 年 1 月のサービス開始以降、10 か月の ID 発行数を表１に示す

表１．ゲスト用ＩＤの発行数と利用目的

ワンデイアカウント	101
PC のセキュリティ更新	66
医学図書館での学外者利用	22
機器のデモ、説明会	3
その他	10
短期滞在者用ゲストＩＤ	14
研修医	6
留学生	4
共同研究	3
アルバイト	1

ワンデイアカウントの利用目的は、当初想定していなかった、購入直後のパソコンのセットアップ、セキュリティ更新、ワクチンソフトの最新化のためのネット接続のために、利用される事例が最も多かった。次いで、図書館での患者や学外利用者のパソコン利用のためのもの、その他は、機器の点検修理、留学生、アルバイト、会議資料閲覧などで、当初想定した来客の持ち込みパソコンを接続するための申請は１例もなかった。また、学内で開催されている研究会での利用事例もなかった。

短期滞在者用ゲストＩＤの利用目的は、学外の医療機関に所属する研修医が、大学で研修（１か月）する際に持ち込みＰＣを利用するためのものが多く、次いで、留学生、共同研究で来学した者、短期アルバイトとなっている。

5 成果と課題

マルチステップ認証を導入すると、未登録の人は利用できない。未登録のパソコンは接続できない状態となる。大学では、職員学生以外の者が立ち寄り、ネットワークを利用することがあり、また一時的に未登録のパソコン等を接続したいことがある。今回報告したゲスト利用システムの導入により、こういったマルチステップ認証の不都合な点が解消できたものと思われる。

マルチステップ認証を行うには、ユーザ登録、MAC アドレス登録を行う必要があり、センター業務が増加し、また、ユーザにも負担がかかる。い

ずれも情報セキュリティを高めるためにやむを得ない負担増である。

我々は、先に、オンライン申請からオンライン登録処理、LDAP 登録が可能となる一連のシステムを構築し[8]、センター業務の省力化、ユーザの負担軽減を実現することができた。

ゲスト利用システムは、想定した機能を果たすことができたと考えているが、学内で開催されている研究会などでの利用が進んでいない。こういった非日常的なネットワーク利用が、マルチステップ認証の制約によって制限を受けることがないように、また、職員が接続して他の人に使わせるといった不正行為を行うことがないように、周知を広げていきたいと考えている[9]。

参考文献

[1] 谷内田昌寿、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。

[2] 岡山聖彦、山井成良、大隅淑弘、河野圭太、藤原崇起、稗田隆、”岡山大学における認証・ロケーションフリーネットワークの構築”、学術情報処理研究、No.15、pp.161-165、2011。

[3] 内田奈津子、因幡哲男、”フェリス女学院大学におけるネットワーク認証システムの構築”、View Point、No.10、pp.86-90、2010。

[4] 打矢隆弘、松井俊浩、齋藤彰一、山本大介、内匠逸、松尾 啓志、"名工大における大規模ダイナミック VLAN ネットワークの管理・運用"、大学 ICT 推進協議会 2011 年度年次大会論文集、pp198-202、2011。

[5] 森河良太、松崎日出海、宮川毅、小杉義幸、関口薫、加藤 哲太、"東京薬科大学における無線 LAN システムの導入と LISM との連携"、大学 ICT 推進協議会 2011 年度年次大会 論文集、pp187-190、2011。

[6] 島岡章、板倉紀子、” 大分大学医学部キャンパスのネットワーク運用ポリシーとシステム構成について”、学術情報処理研究、No.16、pp.178-182、2012。

[7] 挟間キャンパスの情報ネットワークに接続する機器の満たすべき技術的基準 http://www.med.oita-u.ac.jp/mic/lan01/kijun.html

[8] 板倉紀子、島岡章、小谷明義、吉田和幸、”ユーザと機器のオンライン申請、登録、認証システムの開発とその運用について -- センター管理業務の削減の観点から –“、学術情報処理研究、No.16、pp.183-187、2012。

[9] ゲストＩＤ申請・取り扱い（大分大学医学情報センター） http://www.med.oita-u.ac.jp/mic/lan01/guestid.html

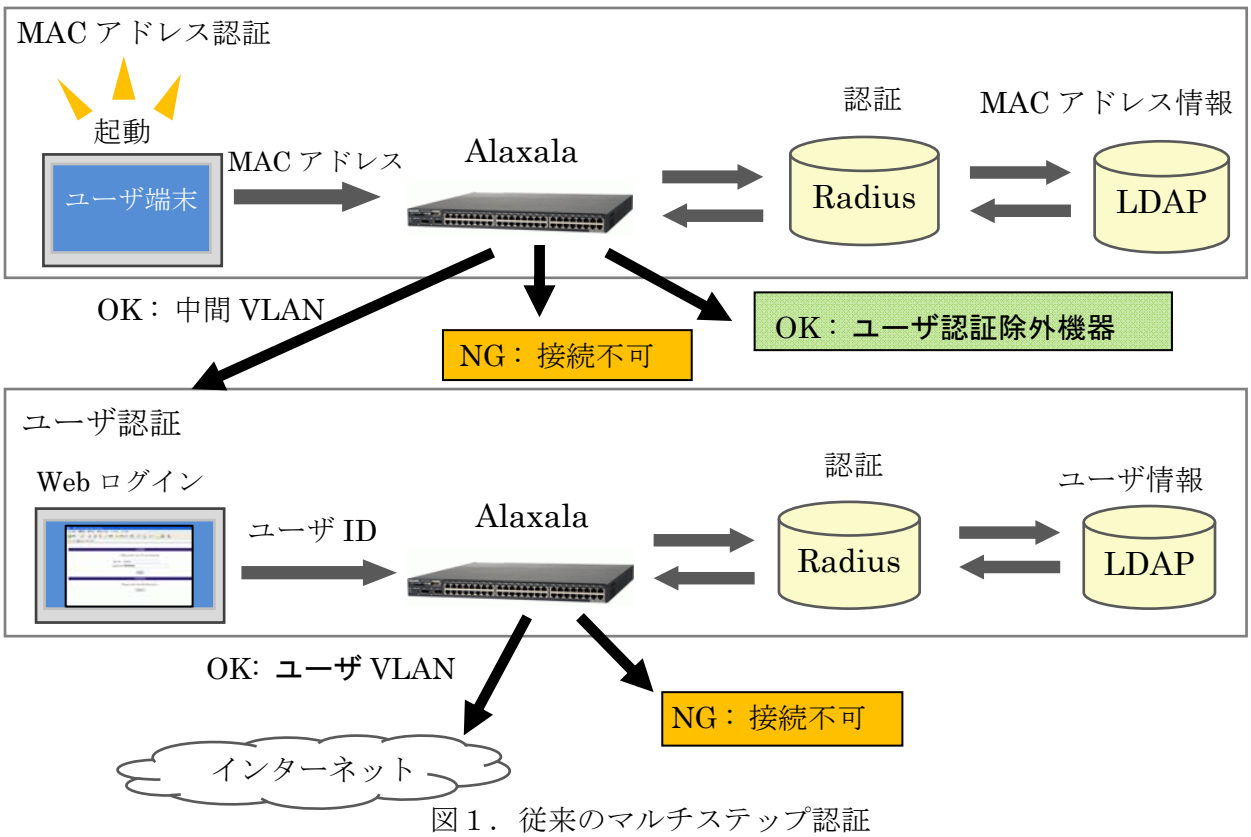

図１．従来のマルチステップ認証

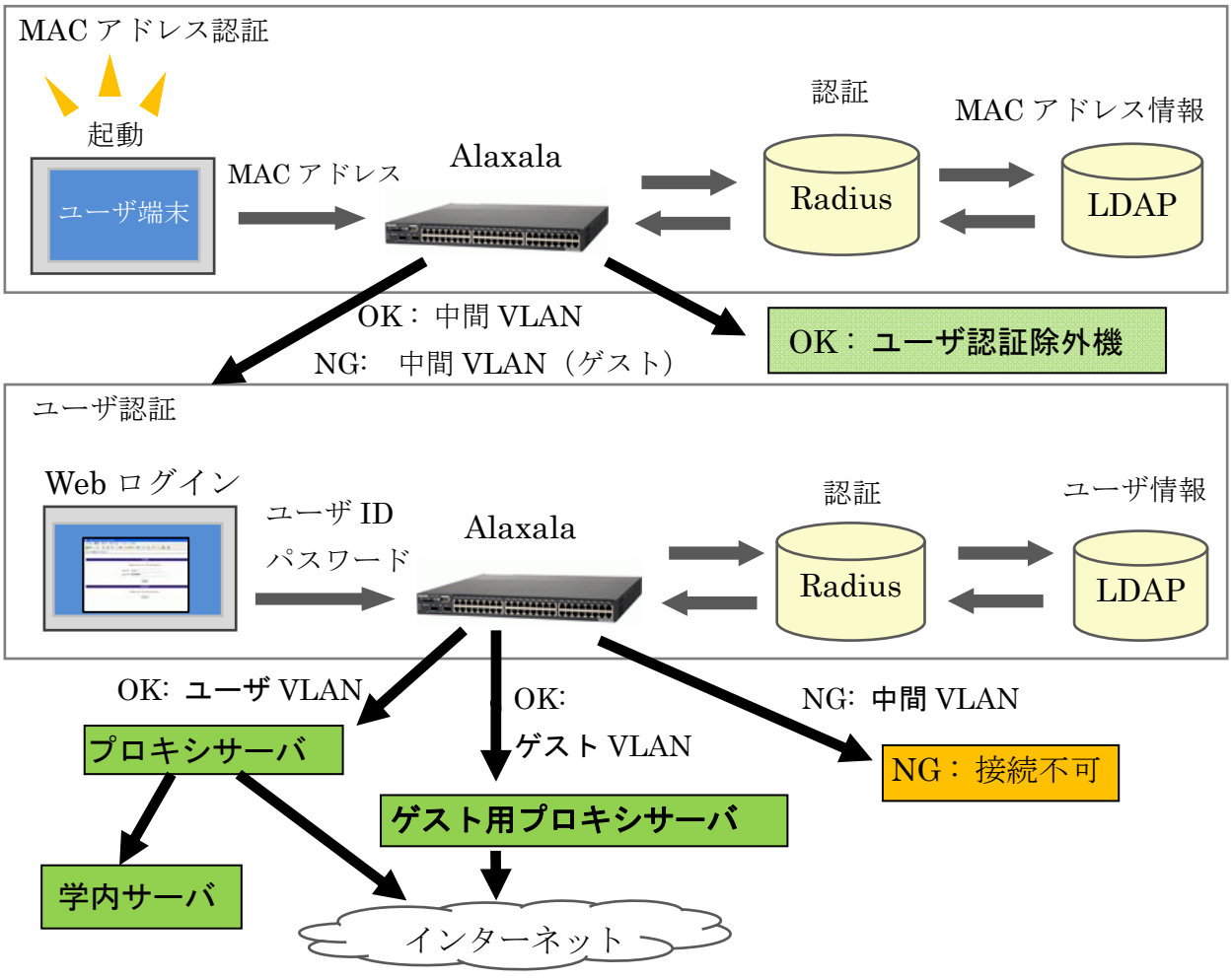

図２．マルチステップ認証の中にゲスト利用を組み込む