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

Network policy of Oita university medical school, and their implementation

島岡章，板倉紀子
Akira SHIMAOKA, Noriko ITAKURA

shimaoka@oita-u.ac.jp, itakura@oita-u.ac.jp

大分大学学術情報拠点（医学情報センター）

Oita University Medical Information Center

概要

医学部は附属病院を持っており，ユーザのパソコンに患者情報を保有していることが多く，また職員の異動が多いため，より厳格なセキュリティ対策が必要である．ここでは，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，それを制定した背景，それを実現するに至る経緯，技術的に実現することができるようになったシステム構成について検討する．

キーワード

ネットワークポリシー, マルチステップ認証，パソコンのセキュリティ

1. はじめに

かつての大学のネットワークは，インターネットに開かれたネットワークであったが，近年の情報セキュリティや情報漏えい防止の高まりの中で，キャンパスネットワークでも，ファイアウォールを設けてインターネットの脅威から防御し，キャンパス内部でも，Web 認証や MAC アドレス認証などの制限をかけるようになってきている．大分大学医学部（旧大分医科大学）では，以前から厳格なセキュリティポリシーを設けてキャンパスネットワークの保護に努めている．その背景とそれを実現するために行ってきたシステム的な仕組みについてご紹介する．

また，ポリシーを厳格にすれば，必然的に，ユーザにもセンター業務への負担も大きくなる．その負担を軽減するための対応についてもご紹介する．

2. ネットワーク運用ポリシー

(1) ネットワークやシステムを利用するものは申請を出して許可を受けること．

(2) ネットワークに機器を接続する場合は，申請を出して許可を受けること．
(3) ネットワークに接続するパソコンは，セキュリティ対応をすること．
(4) キャンパスネットワークをインターネットの脅威から防御すること．

3. ポリシーの背景

3.1. 医学部の特性

大分大学は，教育福祉学部，経済学部，工学部と本部事務局が位置する旦野原キャンパスと附属小中学校，特殊支援学校が位置する王子キャンパス，病床数 604 床の附属病院を有する医学部の挟間キャンパスからなる，学部学生数が 5,035 人の地方大学である．

医学部は，他学部と比べると，次のような特性がある．

- 学生数に比して職員数が多い（図１）
- 非常勤職員が多い．（図１）
- 職員の異動が多い．（図２）
- 人事異動（退職，採用）があっても，大学とのつながりが継続している人が多い．
- 病院情報システム，医療情報部門が存在している．24 時間オンコールサポートが通例となっている．
- 患者の情報をパソコンに保存しているユーザが多い．
- 情報センターのスタッフが少ない，あるいは医療情報部門が兼任している．
- ウイルス感染事例が多い．

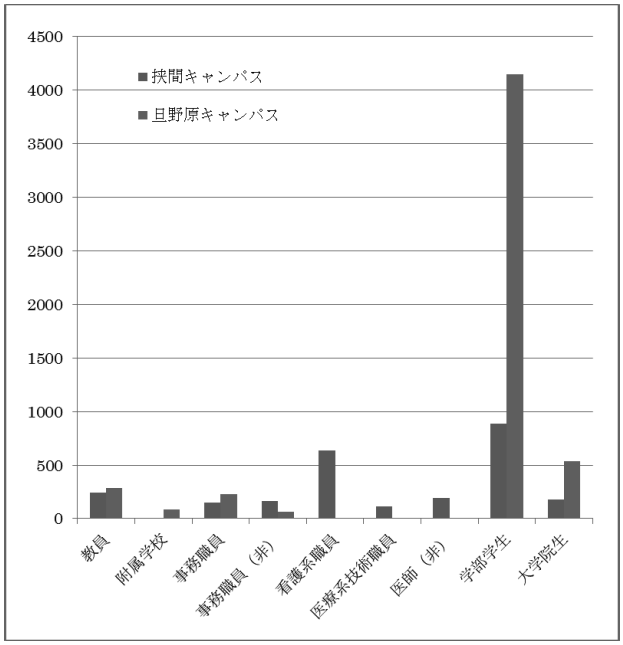

図１．職員数と学生数

3.2. ポリシーの運用の経緯

1995 年の学内 LAN 開設当初から，キャンパス内部はプライベートアドレスを使用している．そのため，インターネットとの間にはファイアウォールを設置して，プロキシサーバを経由してアクセスを確保している．

当初からグループウエアを導入し，ほぼ全職員と全学生にメールアドレスを交付しており，また，組織名や職名アカウントも交付し，古くから，事務連絡はメール（メーリングリスト）で行われている．ユーザアカウントは，このグループウエアにアクセスするためのものであった．

2001 年からユーザ登録申請，端末設置申請をオンライン化し，ユーザに利便性を提供している．申請情報は，センター管理者宛に，サーバに登録するバッチコマンドとともにメールで送信され，管理者の業務軽減，操作ミスの防止につなげていた．

2007 年からは，統合認証システム（コムネット社アカウントマスター） を導入した．アカウントマスターは，ユーザから紙で申請を受けて，管理者が Web 画面に手入力をする仕組みであるため，オンライン申請からメールでバッチ登録用の CSV ファイルを送る方法を取った．

2009 年には，アラクサラスイッチの機能を使って，マルチステップ認証を開始した．この時は，アカウントマスターが MAC アドレスを扱えなかったので，アラクサラに直接 MAC アドレスを登録した．また無線 LAN(Meru)はアラクサラをスルーするため，無線接続する機器の MAC アドレス認証のために，別途 Radius サーバを立てて，この Radius サーバにも MAC アドレスを登録した．登録用のコマンドを，管理者宛の申請メールに記載したので，入力ミスは防げたが，センター業務は著しく増えた．

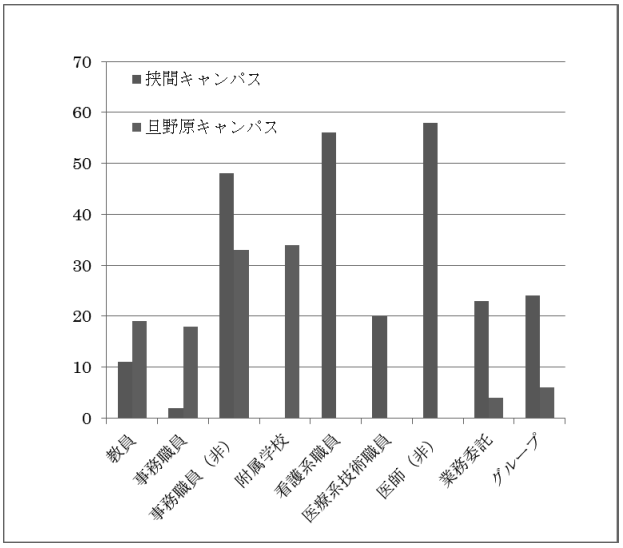

図２．新規ユーザ登録数(2011 年度)

4. セキュリティポリシーの実現に向けて

4.1. ファイアウォール

基本的には, 学内 → 学外は, http, https, ftp のみ通し, 学外 → 学内には, 公開する Web サーバあてにリバースプロキシを経由する http, https のみしか通さない．キャンパス間の業務用通信やサーバ間通信など，必要な場合には，ファイアウォールの穴あけをしている．

4.2. プロキシサーバ

キャンパス内部からは, http, https のみ通すプロキシ(squid)を経由しないと，外部へのアクセスはできない．後に述べるように，ネットワークアクセス時に，Web 認証と MAC アドレス認証を導入したので，学内サーバにアクセスできないゲスト用のプロキシを準備している．

4.3. 統合認証システム

統合認証システムは，新規登録時に，所属に応じて，デフォルトのアクセス権限を設定し，メールサーバ，ファイルサーバ，グループウエア，LDAP サーバへの登録処理が自動的に行われる．AlcNetacademy，WebClass，教務情報システムは，統合認証が行われるが，ユーザ登録は手動で行われている．給与システム，業務可視化システム，物品請求システム，教員業績データ登録システムは，統合認証に参加していない．サーバ，システムのアクセス権限は，変更申請により追加削除する．

職員の新規登録は，本人からのオンライン申請を受けて対応している．これは，人事からの採用情報では，すでに登録済みの人が多数存在するからである．

学生は入学時に全員登録し，オリエンテーションで配布している．学生用パソコンへのログインは，統合認証により行われ，ファイルサーバに保存された個人プロファイルとＺドライブの割り当てが行われる．学生用プリンタの印刷管理，一部の部屋の入退室は，統合認証と連携した Felica カードで認証している．

ユーザ認証を開始したことにより，学外からのお客さんや短期滞在者がネットワーク接続ができなくなったため，ワンディアカウントと短期滞在者用ゲストＩＤの２種類のゲスト用アカウントを準備している．ワンディアカウントは，大学職員が，オンラインで認証後に，リアルタイムに発行を受けることができ，その職員の責任で学外者に利用してもらう仕組みにしている．

4.4. MAC アドレス認証

2012 年 6 月から，MAC アドレス認証方式を変更し，アラクサラから，Radius サーバ経由で，統合認証システムで管理する LDAP サーバに問い合わせを行う方式とした． MAC アドレスの登録は，統合認証システムの新規機能として追加した．

ノートパソコンやスマートフォンのように移動する端末であっても，認証後にユーザごとに設定された VLAN に入り，Meru のシングルチャンネルの仕組みとともに，キャンパス内のどこに移動しても，パソコンの接続性は保持される．

プリンタやＮＡＳなど，ユーザ認証ができない機器には，固定 IP アドレスを付与し，統合認証サーバに認証除外機器として登録している．

学外からのお客さんが持ち込んだパソコンでインターネットにアクセスできるように，学内のサーバやパソコンには接続できない，ゲスト用 VLAN を準備している．また，職員学生が新規にパソコンを購入した際に，MAC アドレスの登録がないためネットワークに接続できず，初期設定やセキュリティ更新ができない状態になるが，その際にも，ゲスト用 VLAN を使うようにしている．毎日認証をするように，MAC 認証の有効時間を 16 時間としている．

4.5. マルチステップ認証

図３に示すように，アラクサラのマルチステップ認証を利用し，Web 認証と MAC アドレス認証の両方を通過したパソコンだけがネットワークに接続できる仕組みとしている．認証情報は，統合認証システムの LDAP サーバに問い合わせするようにしている．

ゲスト用の接続ルートを準備していることは既に述べたとおりである．

4.6. ユーザ登録，MAC アドレス登録の省力化に向けて

統合認証システムとオンライン申請を結合して，センター業務が削減できるようにした．これについては，本研究集会で，板倉が発表する[4].

4.7. ネットワークに接続するパソコンのセキュリティ要件

2011 年 8 月から，セキュリティ対応が行われていないパソコンは，キャンパスネットワークへの接続を許可しないこととしている．

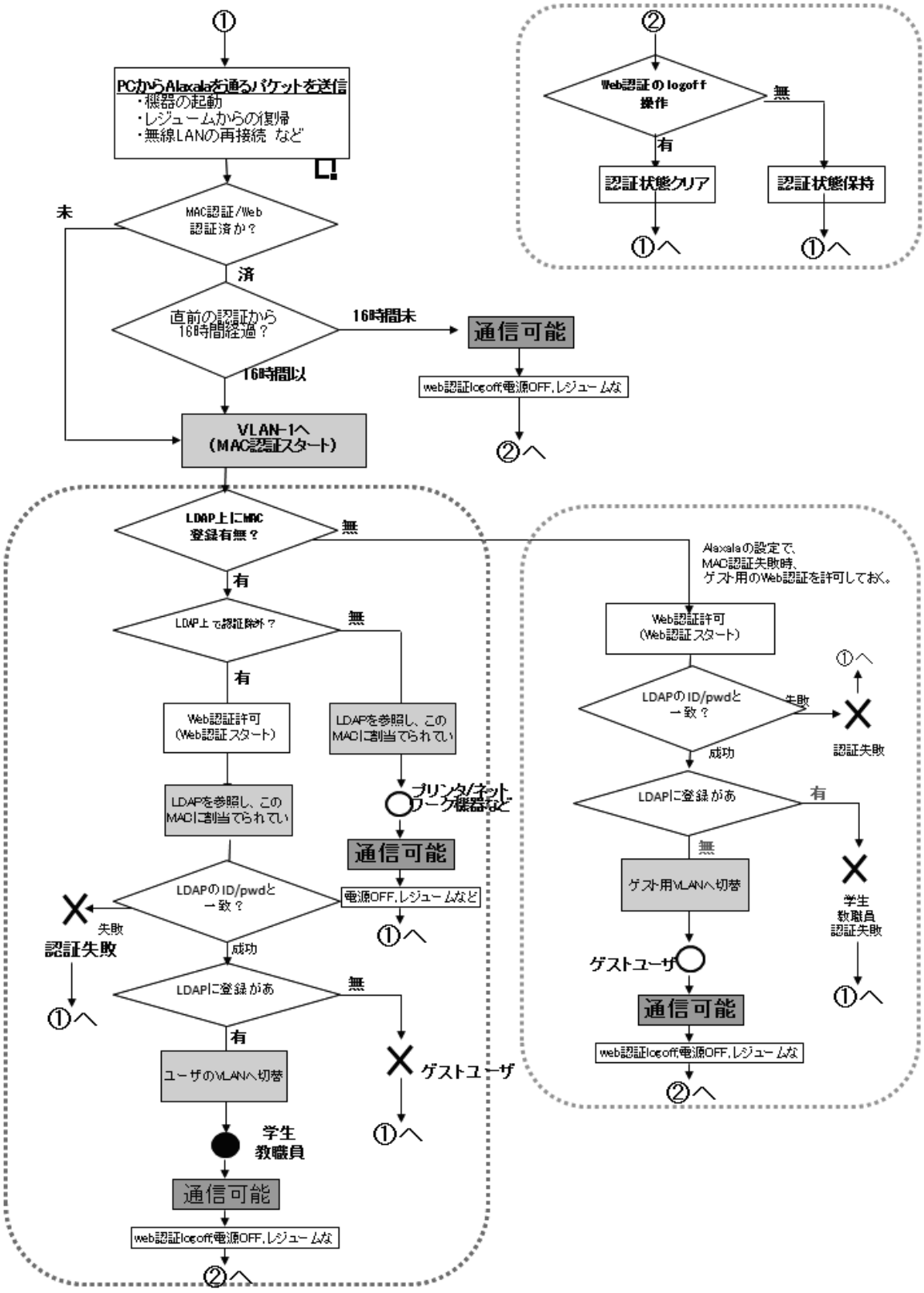

図３．マルチステップ認証の処理フロー

その条件は，ＯＳ，Office, Adobe Reader, Flash Player などのアプリケーションのセキュリティ更新を(自動的に)行うことと，ワクチンソフトのインストールを必須としたことである.

セキュリティ更新のしかたの周知とパソコンのそれらの更新日付の調査を行い，メーカーからセキュリティパッチが提供されなくなった古いＯＳのパソコンは，接続許可を取消した.

ワクチンソフトは，職員学生の私物のパソコンも含め

て無償提供している．登録された MAC アドレスに対して，１回だけダウンロード可能としている．

5. 現在のシステムの問題点と今後の課題

MAC アドレス認証と Web 認証を併用している大学[1][2]や，認証 VLAN を導入している大学[2][3]からの報告があり，これらを参考にしながら，ネットワーク運用ポリシーの実現に努めてきた．

現在利用しているアラクサラのマルチステップ認証は少し無理があるので，次の更新までには，よりスマートな認証方式がとれるように検討したい．

本学では，申請はオンラインで受けているが，他大学では，計算機利用負担金の支払いの名残りがあるせいか，印鑑のついた書類を提出させることが多いようである．本学ではオンライン申請の際に，所属長の承諾を得たかというチェックボックスを設けて，「はい」と答えないと申請を受け付けない仕組みにしている．また許可メールは，所属する講座等にも送付している．情報センターでの事務手続きに，情報システムを使わないのは，どうも理解できないところである．

パソコンのセキュリティ対応状況については，自己申告に頼っているので，今後は，パソコンのＯＳやアプリケーションのバージョンを自動的に収集する仕掛けを導入したいと考えている．

病院情報システムは，ウイルス侵入防止，情報漏えい防止の観点と，電子カルテの普及に伴う病院情報システムの重要性の増大から，インターネットやキャンパスネットワークから切り離される傾向にある．病院情報システムの利用者が要求する，不具合が発生した機器やシステムの短時間での復旧（24 時間 365 日サポート）は，基盤情報システムでも理想的ではあるが，情報センターの少ないスタッフ＋業務委託では現実的に対応できるものではない．

他学部と異なり，医学部ユーザは，医療情報部門のオンコールサービスに慣れているので，対応する情報センターのスタッフには心労をかけている．

ユーザにも使いやすく，センタースタッフの負担も少なく，しかもセキュリティの向上につながる仕組みを検討していきたい．

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] 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 –“，（本年の学術情報処理研究集会にて発表予定）