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 --

Development and operation of consecutive online system, from user/PC application, LDAP registration to user/PC authentication. -- To reduce administrative costs --

板倉紀子*[1]，島岡章*[1]，小谷明義*[2]，吉田和幸*[3]

Noriko Itakura*1, Akira Shimaoka*1, Akiyoshi Kotani*2, Kazuyuki Yoshida*[3]

*[1] 大分大学医学情報センター
*[2] 株式会社コムネット
*[3] 大分大学情報基盤センター

*[1] Oita University Medical Information Center
*[2] Comnet co., LTD.
*[3] Oita University Information Technology Center

概要

大分大学挾間（医学部）キャンパスでは，学内 LAN を利用する際に 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行っている．本稿では，ユーザの利便性を高め，センターの管理業務を軽減するために，ユーザとパソコンの両方の申請について，ユーザはオンラインで申請を行い，メールでセンターに通知され，センターでは，Web 管理者画面で操作すると LDAP サーバや各種サーバに自動的に登録が行われ，申請者あての許可書の印刷や許可メールの発送までの一連の作業を行うことができるシステムを開発したので，その概要と運用経過について報告する．

キーワード

センター運営業務の軽減，オンライン申請，Web 管理画面，Mac アドレス認証, Web 認証

1. はじめに

近年，キャンパスネットワークのセキュリティを高めるために，MAC アドレス認証，Web 認証を合わせたマルチステップ認証を導入している大学があり[1][2]，大分大学挾間（医学部）キャンパスでも，許可されたユーザ・許可された機器のみが学内 LAN を利用することができるというポリシーを実現するために，マルチステップ認証を導入している[3]．それぞれの認証を行うためには，ユーザアカウントと，接続する機器の MAC アドレスに

ついて，ユーザからの申請を受けて，認証サーバに登録する必要がある．従来のセンターの申請処理は，オンラインの申請画面で入力されたデータをセンターがメールで受け取り，それぞれのシステムへの登録処理をバッチ登録で作業をしていた．登録作業を行うにはそれぞれのシステムのサーバや通信機器にログインしコマンドを実行する必要があるため，作業するセンター職員が固定化してしまい，ユーザへ利用許可を発行するまでの時間を要するという課題があった．

ユーザからの申請をオンラインで受けている大学もあるが[4]，センター業務を一元管理するシステムに関する報告は見当たらない．

そこで，このような課題を解消するために，申請から登録までの一連の処理をオンラインシステム化し，Web管理画面から操作できるようにして，センター職員の業務改善を図ることとした．システムを改善するにあたっては，センター職員の誰もがどの処理作業でもできること，作業量が軽減し，尚且つ確実な処理が求められた．

2. システムの概要

2.1. システム構成

本システムで使用しているサーバは，すでに稼動中であるコムネット社のアカウント管理システム（アカウントマスター）の DB サーバ，LDAP サーバと，申請画面を搭載している Web サーバがある．Web サーバには Apache2.2.3 , PHP5.1.6, Mysql5.5.1 がインストールされている．

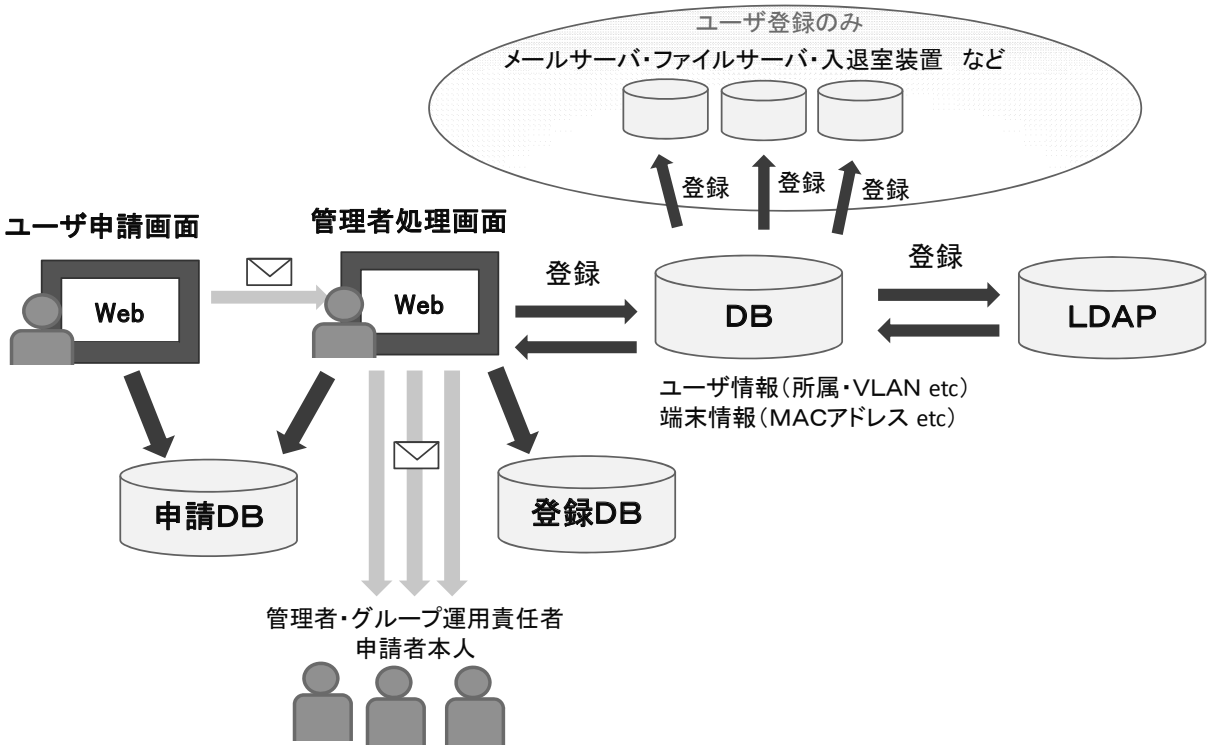

図１．ユーザ・機器登録の流れ

図２．管理者Ｗｅｂ画面

2.2. ユーザアカウント申請処理の構成

ユーザアカウント申請には「新規」「変更」「廃止」の３種類がある．ユーザが申請して処理が完了するまでの流れは共通している（図1）．

ユーザが申請をすると申請 DB に申請内容が保存され，通知メールがセンター管理者に届く．管理者は通知メールにある URL から管理者画面にログインする．管理者画面に表示された申請データを確認し，在籍確認・職員番号入力・重複登録確認を行い，登録ボタンをクリックする．登録ボタンをクリックすると，認証サーバへの DB，LDAP サーバに登録され，各種サーバ・システムへの登録処理を自動的に行い，申請 DB にあるデータは登録済み DB に保存される．登録後に申請者本人・所属グループ･センター管理者に完了通知メールが自動送信される．登録したデータは申請 DB から削除され，登録日時，作業者，コメントの履歴を記録して登録 DB へ移行される．データの動きは管理者画面で確認することができる．

新規登録時には，ユーザアカウントの所属に応じて，VLAN と複数のシステムへのアクセス権限が自動的に与えられる．変更申請時には登録内容の変更と同時にアクセス権限の追加・削除の申請を行うことができる．

2.3. 端末申請処理の構成

端末申請には「パソコン用」「固定機器用」「LAN アダプタ用」，これに共通の「変更」「廃止」の５種類ある．端末申請には大きく分けてパソコン等の認証機器とプリンタ等の認証除外機器があり，それによって入力項目も変わってくるため，申請画面を分けている．申請の流れはユーザアカウント申請とほぼ同じで，申請が届くとセンター職員が管理者画面にログインし，申請内容を確認する．内容に問題なければ登録ボタンをクリックする．同時に DB と LDAP に登録処理が行われ，自動的に申請者・所属グループ・センター管理者に通知メールが自動送信される．

基本的な登録の流れの他に管理者画面にある機能を紹介する．

(1) 申請却下

申請者が誤った申請をした場合や内容に不備がある場合は却下理由を入力し，却下ボタンをクリックすると申請者本人とセンター宛に却下通知が送信され，申請

DB から削除される.

(2) 保留

申請内容を確認するために問い合わせ対応中の申請の場合は誤って他の職員が処理を進めてしまわないように対応中の状況を入力し，保留ボタンをクリックすると，申請未処理一覧に赤く表示される.（図２）

(3) 検索・変更・削除機能

登録中の機器を検索・変更・削除することができる.

(4) 登録中データの抽出

登録 DB にあるデータを CSV で抽出できる.

管理者画面以外にもユーザ向けに，登録内容を確認することができるように，登録内容検索画面が公開されているおり，ユーザアカウント・MAC アドレスから登録中の機器をいつでも確認することができる.

3. 運用状況

3.1. ユーザアカウント申請処理の業務の変化

システム導入前のユーザアカウント登録は，主に以下の作業が発生していた.

(1) メールで申請内容を受け取る
(2) 各種システム用バッチファイル実行用 CSV データ作成
(3) 定期的（10 分間隔）に登録用バッチファイルが実行される
(4) LDAP にユーザ VLAN を設定する
(5) 申請翌日に許可書を印刷

システム導入後は，申請をメールで受け取り，管理者画面にログインして申請内容を確認し，登録ボタンをクリックする．新規登録の場合は登録完了画面に印刷用ファイルが表示され許可書を印刷する．変更・廃止申請の場合は登録ボタンをクリックすると自動的に完了通知メールが送信される.

3.2. 端末申請処理の業務の変化

システム導入前のパソコン等のマルチステップ認証対象機器の登録は，主に以下の作業が発生していた.

(1) １日に一度登録・削除件数をまとめ，登録コマンド用テキストを作成
(2) Alaxala にログインして，登録内容確認
(3) 登録・削除コマンド実行
(4) 登録内容確認
(5) Radius にログインして，登録内容確認
(6) 登録・削除コマンド実行
(7) 登録内容確認
(8) 管理者画面にあるボタンで許可メール送信

認証除外機器の場合も，作業の流れは同じだが固定 IP アドレス・VLAN を設定する作業が発生する．この項目を割り振るには，場所・所属が関係してくるために自動的に連番を与えることができないため，オンラインシステムとは別に IP アドレスのデータを持っている．この点に関してはオンラインシステムで完了していない.

機器申請に関してもシステム導入後には，通知メールを受け取り，管理者画面にログインして申請内容を確認し登録ボタンをクリックするのみになった.

3.3.システム導入後の利点

・登録するシステム別に異なるコマンドを実行する必要がないため，処理ミスがなくなり，主担当者が不在でも処理が行えるようになった.

・管理者画面の未処理一覧で処理されていない申請が確認できるため，処理漏れ（遅れ）が少なくなった.

・以前は，処理ミス防止のため１日分の申請をまとめて処理していたため，処理完了は申請日翌日としていたが，随時処理を行えるようになった.

・機器申請で間違った MAC アドレスを申請してしまった場合に，一度申請をして許可を受けて認証を試すとエラーが出てしまう．そこで初めて申請内容が間違っていたことに気が付くユーザが多く，正しい MAC アドレスを申請するとまた翌日になってしまうこともあった．オンライン後には随時処理を行えるので，ユーザを待たせることが少なくなった.

システム導入前後の申請処理の所要時間を調査したところ，システム更新後の所要時間は，システム更新前に比べるとユーザアカウント申請は 30 分程度、端末申請は 4 分の 1 程度に減少していることがわかる（表１）.

表１．システム導入前後の申請時刻から許可メール発行までの所要時間

	システム更新前	システム更新後
ユーザ申請	10:46:43	10:10:04
端末申請	5:57:23	1:28:27

※のべ勤務時間の中央値（時間：分：秒）
※照会が必要であった事例を除く
※認証機器のみ

ユーザアカウント申請についての所要時間は機器に比べるとそれほど減少していないようにみえるが，これは

登録処理前の人事情報確認作業と登録処理後の動作確認作業に時間がかかる件数がこのシステムを導入した時期（年度末・年度初め）に多かったこと，新しいシステムを導入するにあたって職員番号との連携を取るようにしたことが原因である．

4. 今後の課題

基本的な申請の流れは Web 画面上で完結するようになったが，いくつか改善すべき課題がある．

まずは認証除外機器の登録に必要な固定 IP アドレスの割り振りが自動化されていない．これも自動化できるようにしたい．

もう 1 点は機器申請について，MAC アドレスは各自で調べて入力しているので番号の入力ミスがある．MAC アドレスを自動取得できる仕組みを取り入れ，それと同時にパソコンのセキュリティ情報（OS のバージョン，更新日付，ワクチンソフトの利用状況など）も自己申告して入力しているので確実な情報を得るために自動取得できるような仕組みが必要である．

これらの課題についても引き続き実現できるように検討していきたいと考えている．

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] 久長穣，杉井学，為末隆弘，金山知余，小河原加久治，”山口大学におけるネットワーク運用支援システム”，学術情報処理研究，No.15，pp. 31-39，2011.

[3] 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”，（本年の学術情報処理研究集会にて発表予定）

[4] 岩沢和男，宮原俊行，中川敦，岩田則和，西村浩二，吉冨健一，”センターサービス利用登録システムの再構築”，学術情報処理研究，No.15，pp. 89-97，2011.