高知大学における全学認証 DHCP システムの導入

Introduction of the DHCP System with Authentication at Kochi Univ.

斎藤卓也†，中里一仁‡，石黒克也†，佐々木正人†，
三宮克彦‡，結城朝光‡，豊永昌彦†
Takuya Saito†， Kazuto Nakazato‡， Katsuya Ishiguro†， Masato Sasaki†，
Katsuhiko Sannomiya‡， Tomomitsu Yuki‡， Masahiko Toyonaga†

tsaitou@kochi-u.ac.jp, nakazato@cc.kochi-u.ac.jp, ishiguro@kochi-u.ac.jp, sasaki@kochi-u.ac.jp,
jm-sun@kochi-u.ac.jp, jm-tyuki@kochi-u.ac.jp, toyonaga@is.kochi-u.ac.jp

†高知大学総合情報センター
‡高知大学研究協力部学術情報課

†Integrated Information Center, Kochi Univ.
‡Academic Information Division, Kochi Univ.

概要

高知大学では平成２０年度に全学認証 DHCP システムを構築し，２つのキャンパス（朝倉,物部地区）で利用している．システム構築には４０台におよぶ認証マシンが導入され，その稼働状況は監視サーバにより一括集中的に監視可能となっている．特定多数のユーザが利用できるオープンスペース（教室）における，ネットワークセキュリティーの向上が実現されている．

キーワード

LDAP, 全学認証 DHCP, ネットワークセキュリティー

１　はじめに

インターネットを利用することにより様々な新しいサービスが生み出されている．一方で，インターネットの利用が拡大するにつれ，なりすまし問題等における危険性も指摘され始めている．

大学内部においても，学生の授業成績処理，電子授業や事務の人事給与システムのオンライン化などにより，ユーザ認証に伴うネットワークセキュリティーが重要になる事が増えている．

学内ネットワーク上にあるさまざまなサービスを安全に利用するための一つの方法として，学内構成員であるという本人確認を統一的に行うためのシステム基盤の導入が挙げられる.実際に，高知大学では平成１８年度に LDAP(Lightweight Directory Access Protocol)による全学認証システム導入を行い学内情報の集約によるセキュリティー強化を進めてきた[1-2].

さらに，平成２０年度には，全学認証付きの DHCP (Dynamic Host Configuration Protocol) システムの導入を行った．これは全学認証

LDAP サーバと連携し，全学 ID を保持してあるユーザのみがオープンスペースでのネットワーク接続を可能にしたものである．これまでのオープンスペースでは誰でもネットワークが利用できており，ネットワークセキュリティー面においては不安があった．今回の全学認証 DHCP システムの導入により，ネットワークセキュリティーが向上した．

本論文では，全学認証 DHCP システムの概要とそのねらいおよび導入事例について報告する．

２　全学認証 DHCP システム概要

２．１ 認証のしくみ

システム実装には, FEREC(ネットスプリング社製)を認証ゲートウエイマシンとして用いた．DHCP 認証機能を持つ FEREC は全学認証 LDAP サーバと連携することが可能である．これにより，全学 ID を保持してあるユーザ（全教職員と全学生）のみが，学内ネットワークに接続可能となる．

FEREC はネットワーク LAN 側からのアクセスに対する認証ゲートウエイとしての機能を有している．これにより，全学 ID とパスワードを持った正当なユーザだけにネットワークアクセスが可能になる．これは，FEREC の持つ最も重要な機能の一つであるウエブブラウザ認証機能により実現されている．利用者は，利用端末に特別なソフトウエアをインストールしなくとも，本システムを利用できる．また，ネットワーク接続の環境設定変更等も基本的には必要がない．利用端末 OS の種類によらず，本認証システムの利用が可能となっている．その他の重要な機能として FEREC は１対１の NAT 機能を有する． これを使うことにより, FEREC の LAN 側プライベートアドレスから WAN 側グローバルアドレスへの変換を行っている．（詳細は，文献[3]を参照）

認証の仕組みの概要を図１に示す.実際に，ユーザは認証マシンの LAN 側に接続し，プライベート IP アドレスが DHCP 機能により，それぞれの端末に配布される．次にウエブブラウザを起動することで，ログイン認証画面に強制的に誘導される仕組みとなっている（図２を参照）．初めに，全学 ID とパスワードを入力し，全学認証 LDAP サーバに問い合わせが行われる．次に，本人確認ができたならば，認証マシンの WAN 側から学内ネットワークへの接続が許可される．もし全学 ID を保持していないユーザが認証マシンに接続した場合，プライベートアドレスは配布されるが認証は失敗するため，学内ネットワークへの接続は

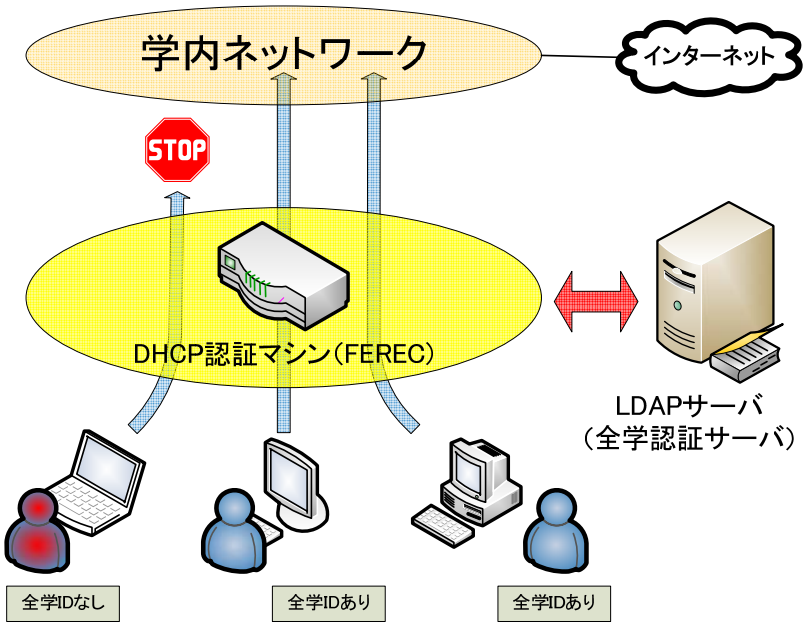

図1：全学認証 DHCP システム概要

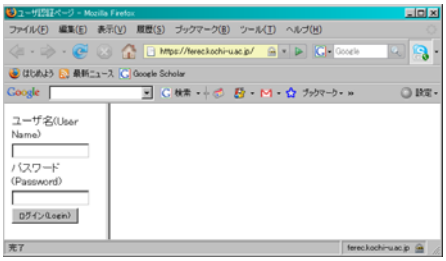

図２：ウエブ上でのユーザ認証画面

禁止される．

２．２ 認証システムの利用場所

本システムは，大学内におけるオープンスペース（教室）において利用されている．ここでは，オープンスペースとは，特定多数のユーザがネットワーク環境を利用できる場所のことを示している．オープンスペースは，総合情報センターの学生利用スペースや，各学部棟の施設に数カ所設置されてある．

２．３ 認証マシンの設置と管理

認証マシン（FEREC）一台で接続できる端末数は２５０までとなっている．高知大学のキャンパスは，大きく分けて朝倉地区，物部地区，岡豊地区と別れて存在する．今回は朝倉地区に３０台，物部地区に１０台が設置された．これは,利用するオープンスペースの数と利用者の数に応じて決めた数である.実際の設置場所は，各地区の情報センターにあるラックに，分散させることなく，集約されてある．朝倉地区のラック搭載状況は図３に示

図３：朝倉地区における認証マシンのラック収納のようす．左写真がラック正面，右写真がラック側面．

されてある．左側は，ラックの正面写真であり，15 台の認証マシンが縦に並べてある．また右側の写真はラックの側面写真である．認証マシンが背面部分を背中合わせにして，前と後ろ（写真では右と左）に合計３０台設置されてある．背中合わせに設置することにより，ラック設置スペースが節約されている．

運用に当たって管理者は，それぞれの認証マシンにログインして設定変更やユーザログ等の確認をすることができる． しかし，認証マシンの台数が増えるにつれて上記管理作業は時間のかかるものとなる．とくに，すべての認証マシンのファームウェアーのアップデートや，ログインしている全体のユーザ数の把握等は面倒な作業となる．

このような作業を効率的に行うために，本システムでは，多数の認証マシンを一括監視・管理することができる監視サーバ(FEREC Center2 ネットスプリング社製)を利用することとした．監視サーバ機能の一つである認証マシンの稼働状況一覧のページを，図４に示してある．ここでは，導入したすべての認証マシンの IP アドレス，利用場所，稼働状況，ログイン人数，ファームウェアーのバージョン等の情報が表示されてある．

また，現在ネットワークを利用しているユーザの ID や MAC アドレス等がリアルタイムで表示される仕組みも実現されている． 図５では，ユーザログイン状況の一覧が表示されてある．ここでは，認証マシンの IP アドレス，ユーザの全学 ID，ユーザが使用している端末に振られた IP アドレスとその MAC アドレス等が表示されてある．

図４：認証マシン監視サーバ．認証マシンの稼働状況リスト

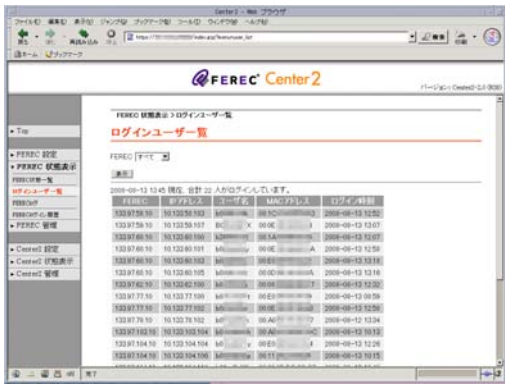

図５：ユーザログイン状況一覧

２．４ 導入に際しての配慮と障害事例

本システムは，主として特定多数の学生や職員が使用するオープンスペースで導入された．そこでは，認証なしの DHCP サービスがこれまで運用されており，認証付き DHCP サービスへの移行については十分な周知が必要であった．そのため，運用開始の数ヶ月前から全学的なアナウンスを，学内グループウエアやメールにより行った．さらに，運用開始直前においては，A３判の簡易手順書を作成した．本導入において，実際にユーザ側で設定を変える箇所は基本的にはないが，ウエブブラウザ認証に変わるということを強調した．手順書を，それぞれのキャンパスの担当者に配布しオープンスペースでの掲示をして頂いた．

導入の一月後，認証マシンの LAN 側に接続された端末からの http ポートへの連続アクセスが行われ，認証マシンがハングアップするという障害が発生した．原因はウイルス等に感染した端末が認証マシンに接続されたためであると推測される．しかし，幸いにもこの障害については、先ごろ公開された認証マシンのファームウェアーのアップデートにより解決されている．

３　まとめと今後

高知大学は，LDAP サーバと連携したセキュアーな全学認証 DHCP システムの導入を行った．

実際の導入に関しては，ネットスプリング社製の FEREC と呼ばれる認証ゲートウエイマシンを採用した．これにより，LDAP サーバとの連携によりユーザ単位でのネットワーク接続認証が可能となった．ユーザ認証はウエブ認証で行われ，利用ユーザは特別必要となるソフトウエアのインストールや設定変更の必要はない．スムーズなシステム導入・移行が可能であった．

本システムは特定多数のユーザが使用するオープン教室等において運用されている．安定的な運用の段階に入りつつあり，より一層の利用を促すべく認証ログイン画面のカスタマイズを予定中である．

導入された認証マシンの台数は４０台におよんだが，分散させることなく，計算機センター内部のラックに集約収納が可能であった．また，すべての認証マシンの稼働状況は，監視サーバにより一括監視が可能となっている．今後，認証マシンの台数が増加したとしても、効果的な管理運用が期待できる．

参考文献

[1]南部匡史，岡本あゆみ，佐々木正人，豊永昌彦，尾崎登喜雄「LDAP を用いた認証/認可基盤に基づく高知大学の総合情報システムの構築」平成 18 年度電気関係学会四国支部連合大会　16-7.

[2]岡本あゆみ，斎藤卓也，佐々木正人，豊永昌彦「高知大学総合情報システムの監視と利用者動向」平成 19 年度電気関係学会四国支部連合大会 16-29.

[3]ネットスプリング社 FEREC に関するウエブページ，http://www.ferec.jp/.