

GUI によるユーザ管理システムと活用システム —マイページ提示システムと組織内連絡システム—

河田 進* 鱈目 正志* 真鍋 伸也**

User Management System by GUI and The Systems using This - My-Page Presentation System and Connection System in an organization -

Susumu KAWATA*, Masashi SAWARAME* and Shinya MANABE**

Abstract

GUI による操作可能なユーザ管理システムを開発した。ユーザは階層構造化されたグループに所属するが、グループの作成や削除、登録ユーザの変更はシステムの管理者が行うのではなく、グループ毎に設定された管理者が個々に許された範囲で行う分散型管理体制を実現した。また、グループ化されたユーザ情報をWebアプリケーションが有効利用できるための方法と、ユーザ管理システムの利用例として「マイページ提示システム」と「組織内連絡システム」を紹介する。

Keywords : GUI, ユーザ管理, Webアプリケーション, 単一ログイン, マイページ

1. 緒言

多くの高専において高専機構認証サーバ（以下認証サーバと略す）を利用しており、計算機センタの演習室で利用できるシステムへのログインなどに使われている。香川高専詫間キャンパスにおいては全教職員と全学生を登録している。

また、キャンパス内には教職員や学生を対象としたWebアプリケーション（以下アプリと略す）やホームページ（以下HPと略す）が多々存在している。特にアプリにおいてはユーザを特定して利用させる必要があるものもある。その様なアプリにおいてはユーザ管理が必要であるが、認証サーバの情報を利用していない場合が多い。理由としては認証サーバ内においてユーザがグループ分けされていないためや、アプリ開発者が簡単な操作で認証サーバのグループ管理をすることが困難なためである。

香川高専詫間キャンパスの認証サーバの年度更新処理やユーザの一括登録などはサーバ管理者（教員）

が行っている。サーバ管理者以外の者がユーザ管理を行いたい場合、サーバ管理者に登録や権限の設定を依頼する必要がある。そのため、時期によっては認証サーバに対する作業に多くの時間が割かれ、負担となっていることが予想できる。

そこで、グループの作成や削除、ユーザ登録などを特定のシステム管理者が行うのではなく、グループを階層的に構成でき、さらにグループそれぞれにグループ管理者（例えば、教員用学科は学科長、学生は教務主事、学生会は学生主事など）を置き、下層のグループ管理はそのグループ管理者が行う分散型ユーザ管理システムを提案する。さらに操作性を良くするためGUIによる操作を可能とする他、グループ構造の可視化を行う。

ここではシステム構成やアプリにおいてシステムを利用する方法を示す他、活用例として「マイページ提示システム」と「組織内連絡システム」を紹介する。

2. ユーザ管理システムのシステム構成

2.1 ユーザ管理機能

* 香川高等専門学校情報工学科

** 九州工業大学情報工学部

ユーザは図1に示すような木構造をしたグループの階層構造の中で管理をする。親ノードがルートである1つの部分木の中で特定の個人は1つのグループにのみ所属させる。例えばAさんを5ITに所属させた場合、5ITからたどれる親グループ(5年、学生、全体)に所属していることになる。5ITの中に新しくグループを作ってAさんがそのグループに所属する場合は、5ITから新しいグループに移動させる。

しかし、クラブのように個人が複数のクラブに所属することが可能である場合を考慮し、部分木に同一人物のユーザコードを複数登録することも可能とする。

このような管理をすることの利点は以下の通りである。

- (1) 登録する個人コードの総量を少なくできる。
- (2) 年度更新のための処理が簡単である。
- (3) 個人の削除や所属変更の必要が生じても、ルートを親ノードとする1つの部分木の中で処理する個人コードは僅かである。

表1にユーザ管理機能の一覧を示す。

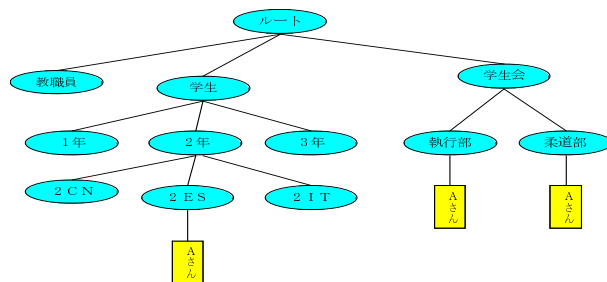


図1 グループの階層構造図

表1 ユーザ管理機能一覧

機能名	処理内容
ユーザ登録	個人のユーザコードを木構造の指定位置に登録する
ユーザ削除	指定した木構造からユーザを削除する
ユーザ移動	指定した木構造内のユーザ(個人または集団)の所属グループを変更する
グループ追加	現在の木構造の任意のグループに子グループとして新しいノードを追加する
グループ削除	指定したグループを削除する(所属しているユーザは親グループに移動)
グループ情報変更	グループ名などの情報を変更する
木構造表示	指定したグループ以下の部分木の構成を表示する
グループ管理者権限設定	グループを管理できるユーザの登録や変更を行う

2.2 グループ管理機能

木構造をしたグループに対する権限の種類を表2のように定める。あるグループにサブグループ作成権限を与えられたユーザには、自由なグループ管理を実現できるよう作成したサブグループ以下の部分木に対しては管理者権限を与える。

表2 グループ管理機能の権限一覧

権限名	内容
管理者権限	指定されたグループをトップノードとする部分木の完全なアクセス権を持つ
ユーザ管理権限	指定されたグループをトップノードとする部分木のノードにユーザを登録したり移動、削除などを行える
サブグループ作成権限	指定されたグループのノードに子ノードを作成・削除できる
権限設定権限	指定されたグループをトップノードとする部分木を管理する権限を与えたり削除したりできる

2.3 データベース

ユーザ管理システムのデータベースは表3のようなテーブルで構成している。グループの木構造はあるグループが親となるグループに所属する形を採っている。また、ユーザ氏名テーブルに存在しないユーザIDを所属テーブルや権限テーブルに登録することはできない。

表3 データベースのテーブル一覧

テーブル名	フィールド			
ユーザ氏名	ユーザID	漢字氏名	仮名氏名	
グループ	グループID	親グループID	マルチ許可SW	
グループ名	グループID	グループ名		
所属グループ	ユーザID	グループID		
権限	ユーザID	グループID	権限	

2.4 実装

図2はグループ構造を可視化したものであり、図3はグループ管理ページである。

Firefox

和英辞書... | goo | http://dhtml | マイページ | グループ構... | +

sk-lab.dikawa-nct.ac.jp/mypage/tree_vjs | Google | 最新ニュース | my | FortiGateウォーティゲート...

香川高専統合ユーザ管理システム

グループ構造(括弧内の数字がグループID)

```

root(1)
  ---教職員(2)
    ---通信ネットワーク工学科(6)
    ---電子システム工学科(7)
    ---情報工学科(8)
    ---一般教育科(22)
    ---学生課(23)
  ---学生(3)
    ---1年(9)
      ---5組(16)
      ---6組(17)
      ---7組(18)
    ---2年(10)
      ---通信(19)
      ---電子(20)
      ---情報(21)
    ---3年(11)
    ---4年(12)
    ---5年(13)
      ---情報(24)
      ---就職(27)
      ---進学(28)
    ---電子(25)
    ---通信(26)
    ---専攻科1年(14)
    ---専攻科2年(15)
  ---学生会(4)
    ---住居形態(5)
    ---寮(29)
    ---自宅(30)
    ---下宿(31)
  
```

ログアウト

図2 可視化されたグループ構造図

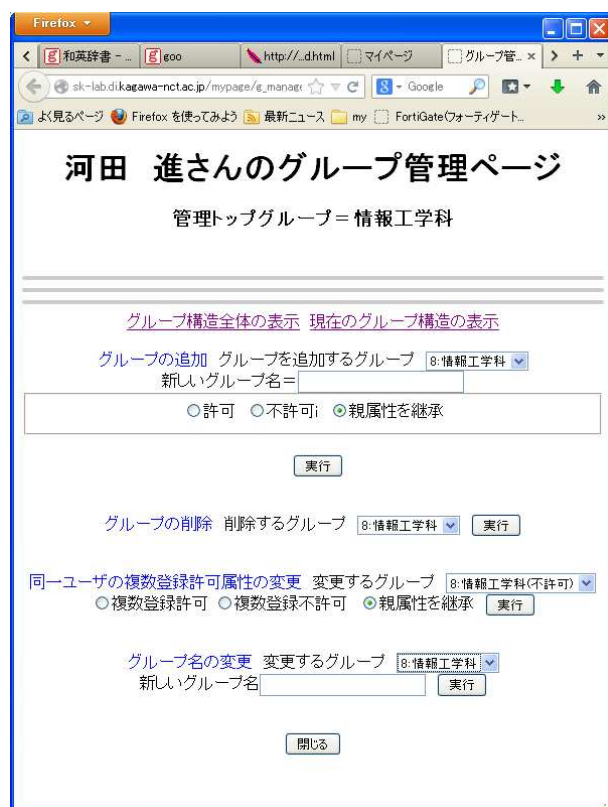


図3 グループ管理ページ

3. マイページ提示システム

3.1 概要

香川高専（詫間キャンパス）で教職員や学生に利用されているアプリやHPを表4に示す。HPは主に情報公開用なのでログインを必要としないが、アプリはログインを必要とするものが多い。

しかし、これらのアプリやHPも存在を知らなければサービスを受けることが困難である。また、アプリの幾つかは利用ログなどの蓄積のためにユーザの特

定が必要で、認証手続きを行う必要がある。そのためアプリ開発者はユーザの認証のためのユーザ登録／更新作業や認証プログラムの用意が必要で開発者の負担になっている。さらに、アプリ毎にログイン作業が必要でユーザの負担になる。

そこで、ユーザ管理システムのユーザ情報を利用することで開発者側のユーザ管理／認証作業を不要とする他、利用可能なアプリやHPを容易に認識できるマイページ提示システムを提案する。尚、マイページへログインすれば、そこで提示されているアプリへのログインを不要とする単一ログインのための仕組みもここで示す。

3.2 マイページ提示システムのシステム構成

ユーザが利用できるアプリやHPの情報を図4のように2.1で示した木構造のグループと関連づけて記憶する。例えば2年生の微積1に関連するアプリやHPは2年生全員が受講するので「2年」というグループに関連させるが、2年情報工学科のデジタル回路1に関連するアプリやHPは「2IT」というグループに関連づける。これにより重複した登録をせずに済む。

Aさんのマイページは、所属するグループ（「2IT」と「柔道部」、「執行部」）それぞれから親ノードを辿って関連づけられたアプリやHPを集め表示する。

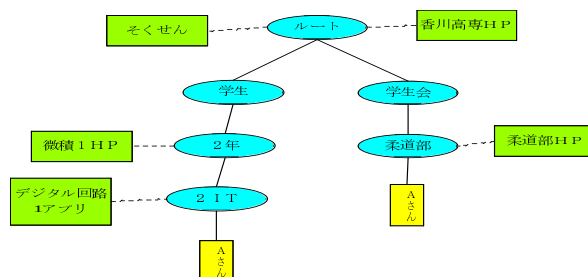


図4 グループとアプリ・HPとの関連図

表4 Webアプリケーションおよびホームページ一覧（2013. 5 調査）

タイトル	目的	対象者	種別	ログイン	記録	開発者
法定外控除提示システム	法定外控除費の通知	教職員	アプリ	必要	無し	教員
寮通知システム	郵便物情報などの通知	寮生	アプリ	必要	有り	学生
小テスト管理システム	小テストの実施と管理	情報3年	アプリ	必要	有り	教員、学生
プログラミング状況認識支援システム	C言語プログラミング支援	2年	アプリ	必要	有り	教員
専攻科・大学試験問題データベース	専攻科・大学入試の過去問	学生	アプリ	不要	無し	学生
教務Webシステム	成績管理	教職員・学生	アプリ	必要	有り	業者
Webclass	自習学習や小テスト、アンケート	教職員・学生	アプリ	必要	有り	業者
寮生外泊・欠食システム	寮生の外泊・欠食届けの提出	教職員・学生	アプリ	必要	有り	業者
そくせん	教職員・学生へのメール送信	教職員・学生	アプリ	必要	有り	業者
クラブホームページ	クラブ紹介	誰でも	HP	不要	無し	教職員・学生
科目ホームページ	科目の紹介や自主学習用	学生	HP	不要	無し	教員
その他ホームページ	女子キャリア支援など	誰でも	HP	不要	無し	教職員・学生

3.3 アプリやHPの登録

ユーザ管理システムが管理しているデータベースの権限テーブル以外のテーブルへの読み取り権限を設定し利用するが、グループにリンクさせるアプリやHPの情報はマイページ提示システムのデータベースに記憶する。誰にアプリやHP情報を登録させるかという登録権限もデータベースに記憶するが、それを行える者はユーザ管理システムで登録されているグループ管理者である。

例えばIT2年の科目担当者が学生に参照させたいHPをグループIT2年にリンクさせただけで、IT2年のクラス担任やさらに上位の2年団長、さらに上位の教務主事に権限設定を依頼することになる。

3.4 データベース

マイページ提示システムのデータベースは表5のように2つのテーブルから構成される。

表5 データベースのテーブル一覧

テーブル名	フィールド	
URL	グループID	URL
権限	ユーザID	グループID

3.5 実装

利用者は図5のように利用可能なアプリやHPを参照できる。また、アプリやHPの登録権限を有する者は図6に示すページを利用できる。尚、ユーザ管理システムの管理権限を有する者も図5のページから操作を開始できる。

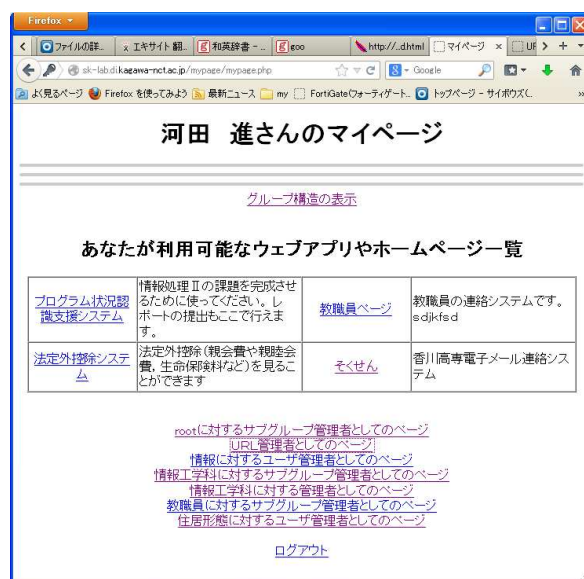


図5 マイページ画面

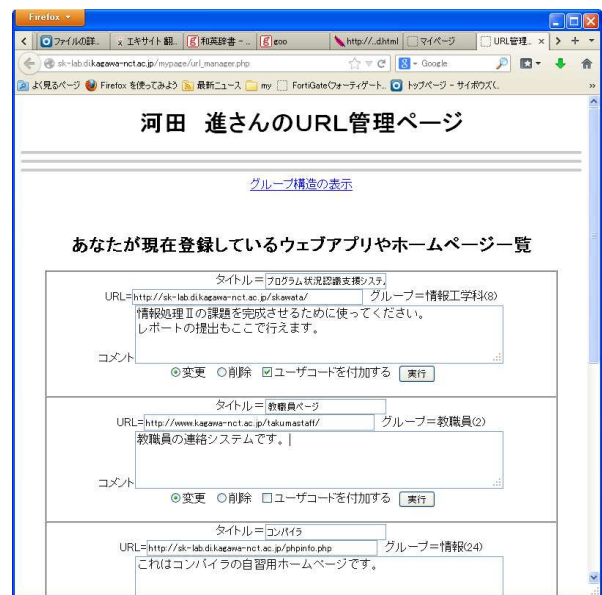


図6 アプリやHPの登録管理ページ

3.6 単一ログインの仕組み

図7はユーザ管理システムやマイページ提示システムとアプリとの関係図であるが、マイページを経由せずに不正にアクセスすることができないようにするための仕組みを示す。

3.6.1 アプリとの連携処理

(1)マイページへログインしたとき、システムはアプリ単位にランダムなアクセスキーを割り振り、以下のようなリンクをマイページ内に生成する。その際システムは、ユーザコードとアクセスキーのペアをデータベースに記録する。

http://***** (URL) ?ucode=ユーザコード
&KEY=A87BE109CF72E83E

(2)ユーザがアプリへアクセスした際2つのデータはアプリへ送信されるが、アプリはこれをセッション変数などに記憶し、他ページへジャンプした際、アクセスキー管理ツールに対してユーザコードとアクセスキーのペアが有効であるかどうか確認し、有効でなければマイページへのログイン画面へジャンプさせる。

3.6.2 アクセスキー管理ツール

アクセスキー管理ツールはLinuxのデーモンとして動作しているが、アプリからの確認要求に応えると共に、データベースに記憶しているユーザコードとアクセスキーの最終確認要求時間から一定時間が経過したとき、アクセスキーの有効期間が過ぎたものと見なし破棄することで、アプリへの不正なアクセス

を防ぐ。尚、アプリとアクセスキー管理ツールとの通信はソケットを利用する。

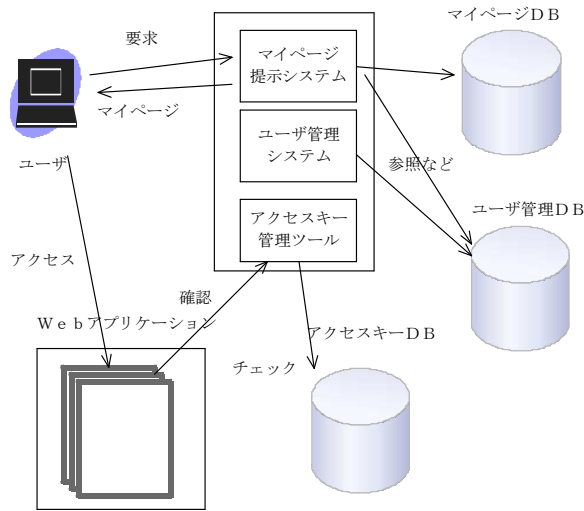


図7 単一ログインのためのシステム関連図

4. 組織内連絡システム

4.1 概要

現在 GUI を使ったメールグループを管理できるメールシステムが開発されている。本校にもメール通知システムとして「そくせん」があるが、以下のような問題点がある。

①学生はメール受信しかできない

「そくせん」では、学生はメールを受信することしかできず、送信機能を利用することができない。また、グループ管理機能も利用できないので、クラス内や、部活動内で連絡を取る手段として利用できない。

②送信者が不明

「そくせん」のメールの差出人は、常に「システム管理者」になっているので、本文に名前がないと誰が送信者かわからない。つまり、なりすましの危険性がある。また、返信してもシステム管理者にしか届かないので、返信が必要な場合は本文に返信先を記述する必要がある。

③ メール送信の成功/失敗が不明

エラーメールは「そくせん」のシステム管理者に送られて送信者には届かないので、送信が成功したかどうか不明である。

そこで、メール機能とユーザ管理システムを利用した組織内連絡システムを構築する。

4.2 組織内連絡システムのシステム構成

図8は組織内連絡システムとユーザ管理システム

との関連図であるが、以下にメール送信の流れを示す。

- ①ユーザ管理システムからグループ構造の取得
- ②ユーザ管理システムへ送信先ユーザグループIDの送信
- ③ ユーザ管理システムからユーザ情報の取得
- ④ ユーザー一覧の表示
- ⑤ 送信先ユーザの指定
- ⑥ 返信先 (Reply :) の指定
- ⑦ メール作成
- ⑧添付ファイルの指定
- ⑨ 署名の自動挿入と送信
- ⑩ エラーメール処理

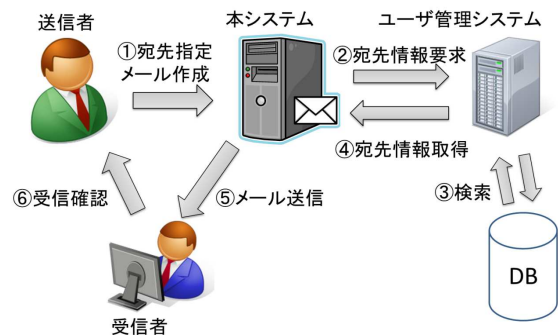


図8 組織内連絡システムとユーザ管理システムとの関連図

メール作成権限には制約を持たせず、登録ユーザであれば誰でもメール作成を行える。学生がクラス内に実験の班グループを作って連絡を取りたい場合、クラスのグループ管理者であるクラス担任に新しいグループの作成を依頼し、管理権限を設定してもらうことで、組織内連絡システムを班内の意識疎通のツールとして利用できる。

また、システムは送信者の所属と氏名を自動挿入することでなりすましや迷惑メール作成を防ぐ。

エラーメールが発生した場合は、Reply で指定されたアドレスにエラーメールを転送することでメール送信失敗を知らせる。

4.3 データベース

データベースにはユーザのメールアドレステーブルと送信ログテーブルがある。

4.4 実装

図9はメール作成画面であるが、個人情報保護のために以下のような改良を今後行う。

- ① 送信先を選ぶときメールアドレスは表示されない。
- ② To:ではなくBcc:に送信先を記述することで、複数

人に同一メールを送っても受信者以外のメールアドレスを知られないようにする。

新規メール作成

図9 メール作成画面

③ 卒業生に対する処理方針の決定

また、単一ログインを実現するためには以下の問題点を解消する必要がある。

- ① 提案した方法で不正アクセスが本当に防げるか実証する必要がある。特に組織内連絡システムが悪用されれば、学生に被害が及ぶ可能性がある。
- ② マイページシステムやユーザ管理システム、アクセス管理ツールがダウンすると全てのアプリが利用できなくなるので、システムのデュアル化が必要である。

5. アプリによるユーザ管理システムの活用

現在、ユーザ管理システムが利用しているデータベースは、権限テーブル以外は誰でも参照できるように権限を設定しているので、アプリ開発者は必要なSQL文を作成することで情報を利用できる。そこで、利用者を限定する必要があるアプリは以下のような手順でユーザを限定できる。

- ① 認証サーバによりログイン認証を行う。
- ② アプリにアクセスできるグループにユーザIDが含まれているかどうか確認する。
- ③ アプリがユーザ毎のログなどを記録する必要がある場合は、データベースなどにユーザIDをキーとして情報を蓄積する。この場合、予めグループに登録されているユーザIDを全て抽出登録してから蓄積を行うのではなく、新規ログインの判断により新しいレコードの生成と蓄積を開始する方が効率的である。

6. 終わりに

ユーザ管理システムに登録されているユーザは認証サーバに登録されているユーザと同一であるので、本来は認証サーバの登録情報を直接使うことが望ましいが、まだ実現できていない。また、実用化するためには以下の方針決定や機能の実現が残っている。

- ① 年度更新処理
- ② 留年、退学、転科などの処理確認（処理そのものはユーザの削除や移動などで行える）