2009-IOT-4 (30)
2009 / 3 / 5

省力化を実現するための忘失パスワード再設定システム

西垣 桂† 齊藤 明紀‡

†鳥取環境大学環境情報学部情報システム学科 〒689-1111 鳥取市若葉台北 1- 1 - 1
E-mail: †{q063021e, saitoh}@kankyo-u.ac.jp

あらまし 大学の情報センターなどでは長期休暇明けなどにパスワードを忘失した利用者が多く発生する．本研究では，パスワード再発行手続を効率化するシステムを提案する．提案システムは，窓口での応対を 1 回だけで済ませるように設計されている．提案システムはパスワード再設定申請を紙ベースではなく専用端末から行なわせることで，多くの申請を効率よく受け付けることができる．また，一旦仮パスワードを設定するのではなく，利用者が希望するパスワードを新パスワードとして受け付けるようになっている．

キーワード パスワード，忘失，再発行，計算機センター，省力化

A system to re-register login password with less human resource

Katsura NISHIGAKI† Akinori SAITOH‡

† Department of Information System, Faculty of Environment and Information,

‡ Tottori University of Environmental Studies 1-1-1 Wakabadai-kita, Tottori-shi, Tottori, 689-1111 Japan
E-mail: †{q063021e, saitoh}@kankyo-u.ac.jp

Abstract In university computer center, especially at the end of long vacation, many users that forgets their password makes center staff busy to handle password re-registration procedure. We propose a system that handles password re-registration procedure with less human resource. In proposed system users need to visit computer center only once through the password re-registration procedure. To achieve efficiency, our system goes without written password re-registration application form, but uses dedicated computer KIOSK terminal that accepts password re-registration request. It does not use random temporary password. User's password will be directly changed to which of user's own choice.

Keyword forget password, resetting password, computer center, work saving

1. まえがき

大学の計算機センターの窓口業務には，パスワードを忘れた学生に対して，パスワードを再発行する業務がある．特に年度初めや長期休暇後にはパスワードを忘れた学生が窓口に集中する.規模の大きい大学だと，休み時間を利用してパスワードの再発行を申請しようとする学生が列をつくることもある．平常時のパスワード忘失頻度は高くないため，ピークにあわせて窓口対応能力を用意することは無駄が大きい．本研究ではパスワード再発行業務での窓口対応の省力化と，学生の利便性の向上を目標とする．

2. 基本的アイディアと考察

現状のパスワード変更手続の問題点を述べ，本研究での提案方式を説明する．

2.1. 現状のパスワード再設定手続

既存のパスワード忘却対応で典型的な方式として，以下の 2 つが挙げられる．

1. 計算機センター側で仮パスワードを発行
2. 学生の希望する文字列を新パスワードに設定

方式 1 は，システムがランダムなパスワードを発行する場合である．学生がパスワード再発行申請書を窓口に提出すると,ランダムなパスワードを設定される．学生は後刻，仮パスワードを印刷した紙を受けとり，そのパスワードで端末にログインして，自分の希望するパスワードに変更する．

方式 2 は，学生が希望するパスワードを新パスワードにする場合である．この場合は，申請書に学生が希望するパスワードを記入して提出する．その後センタースタッフが申請書に書かれたパスワードを新パスワードとして入力する．

しかし，これらの方法にはいくつかの問題点がある．方式 1 は申請書の提出と仮パスワードの受けとりが別であるため，窓口での本人確認を 2 度行わなければならない．また仮パスワードを渡す際に，仮パスワードの紙を大切に取り扱うことと，早急にパスワードを自ら選んだものに変更せよ，など指導伝達が必要なため

に窓口占有時間が長くなる．このように指導しても，それを怠る学生が居るというのも問題点である.また，仮パスワードが窓口の職員の目に触れるということに抵抗を感じる学生もいると思われる．さらに，仮パスワードを印刷した紙を落として，第三者に拾われると大変危険である．仮パスワードを印刷するための紙や封筒を消耗することも資源の無駄である．

方式 2 では，学生が希望するパスワードが，規定されているパスワードの複雑さを満たすかどうか確認が必要である．そのため，職員が確認した結果を学生に伝える必要がある．もし，希望したパスワードが不適切だった場合は，もう一度パスワードを書かなければならない．しかし，それをのぞけば窓口応対は 1 回で済む．また，本人の希望するパスワードを新パスワードとして設定できるので，方式 1 のように学生がパスワードを変更する必要がないというのは利点である．ただし，新パスワードが窓口職員の目に触れてしまうことに抵抗感を抱く学生がいるというのは，1 と同様に問題である．

2.2. 目標

本システムの目標として，まず，パスワード忘失時に，運営側が勝手に仮パスワードを発行するのではなくいきなり当人が希望する新パスワードに変わることが挙げられる．また，窓口での対応が 1 回で済むことも目標とする．さらに，第三者による偽造申請を受けつけないことや，規定されたパスワードの複雑さを満たす申請のみを受けつける仕組みを作る．窓口職員の目にパスワードが触れないというのも重要である．

以降の説明では学生証としているが，教職員のアカウントも同じシステムで取り扱うことが可能である．ただし，以下のような要件を教職員が受け入れる必要がある．

- 学生証同様の顔写真付き教職員証で本人確認を行う
- 教職員の忘失パスワード再発行も，本人が窓口に足を運ぶ

そうでない場合には，教職員の忘失パスワード再発行は提案システムとは別のシステムで行うようなシステム運用とならざるを得ない．

2.3. 基本的アイディア

先に述べた目標を満たすような新システムの基本アイディアを図 1 に示す．

申請端末は，パスワード再設定申請専用の端末である．申請端末を増やせば窓口職員を増やすよりも，低コストで一度に多くのパスワード再設定申請を受け付けることができる．窓口端末は，コンピュータセンターの窓口で係員が操作する端末である．また，本システムのサーバを申請管理サーバとよぶ．対象となる大学の計算機システムの認証サーバを認証サーバと呼ぶ．

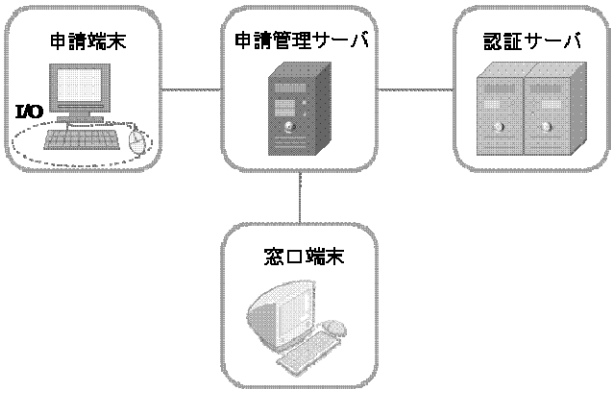

図 1　提案システムの基本アイディア

図 1 では申請情報管理サーバと認証サーバは別の計算機として書いてあるが，同じ計算機上で稼働する別のサーバプログラムという形態も含めて考える．

パスワード変更申請は申請端末から行なう．この端末で申請する場合，申請者は自分のパスワードを忘れているため，パスワードで個人を認証することができない.したがって,申請受付では本人確認は行わない．新パスワードを受付けるがそれを認証サーバには反映させず申請管理サーバに蓄積する．

その後，窓口で本人確認をし，問題がなければ窓口端末から申請受理を指示する．指示を受けた申請管理サーバは新パスワードを認証サーバに送信する．

パスワードを忘れた学生の本人確認は学生証の電磁的記録(磁気カードや IC カード)で行えば足りる，という方針に立つならば，無人の端末での機械的本人確認も可能である．しかし，学生証の貸し借りに抵抗を感じない学生が一定数居ることや財布等の落とし物から他人が学生証を手にする可能性も考え，窓口で職員が当人の顔を見て確認するという方針をとった．

2.4. 基本アイディアに対する考察

基本アイディアの問題点や悪意のある利用者がどのような攻撃をし得るかについて考察する．

まず，サーバや窓口端末のセキュリティを物理的にもネットワーク的にも守るのは当然であるのでこれらへの不正アクセスは除外して他の可能性について考察する．ただし，窓口係員に不正な申告をして誤った操作をさせようと試みる，という可能性は以下で考察する．

悪意のある者の攻撃として，以下の 3 つのパターンが挙げられる．

A. 他人のパスワード変更申請を勝手にする．
B. 他人の新パスワード申請内容を不正に入手する．または改ざんする．

C. 他人が新パスワードを申請するところに介入して，別のパスワードを設定させる．

以上のような問題点を避けるように，設計を行う必要がある．

2.5. パスワード受付方式のセキュリティ設計

上で述べた問題点を避けるために以下のような方式をとる．

窓口では学生証の顔写真で本人確認を行う．これによって攻撃 A は防御できる．

申請端末は，CDROM や USB メモリで持ち込んだ勝手な OS を起動させたり，OS 起動時に割り込みキーを押すなどして介入したり出来ないような防御を行う必要がある．また，通信の傍受や改ざんに備えてサーバとの間は暗号通信を行う．これにより B から防御する．

申請端末は申請を受付けた時には，ユニークな受付番号を表示する．そして学生はその受付番号を窓口で申告するような運営形態とする．また，窓口端末では同一人物のパスワード変更申請が複数存在する場合は，目立つように表示して窓口係員に注意を促す．これによって C は防御できる．

2.6. 方式設計に関するその他の考察

このようなシステムはサーバクライアント方式で，端末のプログラムがサーバにアクセスするような形態をとることが多い．利用者端末や個人所有の持ち込みノート PC などから申請端末を装ったパスワード変更申請を送信するという攻撃を避けるため，申請管理サーバが発呼側となり申請端末を呼び出すような通信形態にする．

パスワードについて，文字数や文字種などの制約を設けている大学は多い．本システムでも，利用者が希望するパスワードが受け付け可能なものかどうかを調べる必要がある．これについては次節で述べる．

3. システムの設計

3.1. システムの機能分割

システムを図 2 に示すように 6 つのサブシステムに分割することにした．

- サブシステム 1: 受付サブシステム
  申請端末上で稼働する申請受付プログラムである．
- サブシステム 2: 申請端末制御システム
  受付サブシステムを起動し，その結果得られた申請データを申請管理サーバで安全に受信する．そして伝えられたパスワード変更申請をデータベースに蓄積する．つぎに，受付番号を受付サブシステム指示して表示させる．
- サブシステム 3： データ管理システム
  申請管理サーバ上で動く申請データ管理システムである．

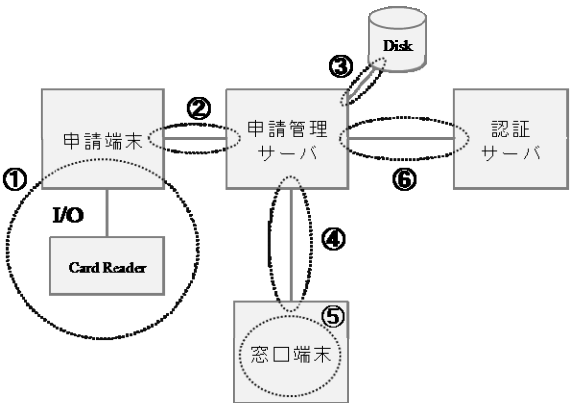

図 2 システムの機能分割

- サブシステム 4: 窓口端末制御システム
  申請管理サーバで稼働するプログラムであり，窓口端末を制御する．
- サブシステム 5 : 窓口端末 GUI システム
  窓口端末で稼働する GUI ソフトウェアであり，窓口係員に情報を提示し，また係員の操作を申請管理サーバに伝える．
- サブシステム 6: 認証サーバ連携システム
  申請管理サーバと認証サーバのインターフェースシステムである．認証サーバに忘失パスワードの再設定を指示する．このサブシステムは認証サーバの方式ごとに開発する必要がある．
- その他，期限切れの申請データのクリーンアップといったデータ保守など，上記のサブシステムに分類されないサポートツールもいくつか開発が必要である．

3.2. システム設計の詳細

システムの使用頻度が低い学生や入学直後の学生はパスワードだけでなくユーザ名も忘れていることがある．そこで，申請はユーザ名ではなく学生番号(教職員番号)で行うことにする．これは学生証に書いてあるため分からなくなることはない．また，窓口での本人確認で学生証が必要であるため，学生証を忘れてきた利用者はそもそも端末を用いた申請ができなくてもさしつかえない．

大学において他人の学生番号を知ることは容易である．本学の学生証は磁気ストライプ[2]付きで学生番号等のデータが記録されている．そこで，他人による申請を少しでも避けるために，磁気カードリーダを取り付け，学生番号はキーボードではなく学生証から読み取ることにする．

パスワードの妥当性チェックは複数のサブシステムで分担して行う必要がある．

字数や文字種の制約は受付サブシステムで確認できる．しかし，現在の設計では学生番号とユーザ名との対応はサーバのみが持っているのであって，サブシ

ステム 1 は持っていない．そのためパスワードがユーザ名と同じ，あるいはユーザ名にちなんだものである場合は受け付けない，という処理は端末では行えず，サブシステム 2 が行う．

「過去に使っていたパスワードは 3 回分は再使用できない」という制約は，認証サーバに「このパスワードはこの学生の新パスワードとして使用可能か？」を問い合わせる機能が提供されていないと実現が難しい．そのため本システムでは，端末での受付時には過去のパスワードの再使用の有無は確認しない．窓口係員がパスワード変更申請の受理を操作した際に，サブシステム 6 がエラーを検知して窓口端末に表示することになる．このため，この場合に限り，利用者は手近な再度申請端末まで移動して再申請が必要となる．

4. 試作システムの実装

前節で述べた設計方針に従って試作システムを実装した．

4.1. システム構成

試作システムの構成を表 1 に示す．認証サーバは申請管理サーバ上で動作する OpenLDAP を用いる．

4.2. 申請端末サブシステム

このサブシステムは，パスワード申請を受け付けるプログラムと，サーバからの応答を表示するプログラムからなる．

申請を受けつけるプログラムを起動すると，まず学生番号の入力をうながす画面を表示する．学生証を磁気カードリーダに通すと，続いてパスワードの入力を行う．

申請受付プログラムは，指定された出力ファイルに学生番号とパスワードをコンマ区切りで書きこむ．パスワードに空白やカンマが含まれている場合に備えて，quoted-printable にエンコードしている．このファイルは一旦**申請端末**に保存するが，サーバに伝達後は消去する．

最後に，サーバから受けとった受付番号を表示して，申請手続は完了する．OK ボタンをクリックするか所定の時間が経過すると，**申請端末**は初期状態に戻って，入力促進画面を表示する．

パスワードに使用可能な文字種やの複雑さの規定は大学によって違う．そこで，いくつかの代表的な制約を組み込み，プログラムの引数で切り替えるようにしている．現状で選択できる制約は以下の 3 種である．

- 制約無し
- 英字と数字が使われていること
- 英大文字，小文字，数字の 3 文字種を含み，6 文字以上 12 文字以下の長さ

本システムを実際に導入する際には，個々のサイトのポリシーにあわせてパスワードの複雑さ制約をチェックするメソッドを書き足す必要がある．

表 1　試作システム

種別	機種	OS
申請端末	自作 PC +USB 磁気カードリーダ	ubuntsu-ja-8
窓口端末	VAIO VGN-S94PS ＋磁気カードリーダ	Windows XP
申請管理サーバ	Sun Java Work-Station W2100z	Solaris 10
認証サーバ (OpenLDAP)	申請管理サーバに同居	

開発言語は java である．まずは CUI ベースのプログラムを実装して磁気カードリーダの扱いなど技術的な確認を行ったあと，GUI ベースのプログラムを実装した．

磁気カードのフォーマットも大学によって違うので，パラメータとして磁気カードデータの何文字目から何文字目までに学生番号が含まれているかを与えるようになっている．クレジットカードやメンバーカードなど学生証ではない磁気カードを読み取った場合にそれを検知して排除するには，個々の大学の学生証の磁気データフォーマットに合わせた改造が必要である．

今回使用した磁気カードリーダが USB キーボードデバイスとして実装されたものであったため，キーボード入力と磁気カードデータの区別がつかない．キーボードから学生証データを入力することも出来てしまわないように，磁気カードデータ 72 文字の入力に 2 秒以上を要した場合は異常と見なすことにした．

4.3. 申請端末制御システム

端末からサーバにアクセスさせるのはセキュリティ的に不安であるので，申請管理サーバが**申請端末**に ssh でアクセスして受付システムを起動するという方式を採った．

申請 1 回について，学生番号と新パスワードを受け取るために 1 回，受付の結果(受付番号またはエラーの)表示のために 1 回，合計 2 回の ssh セッションが張られる．

本システムは受付番号の生成も行う．学生が紙にメモをとらなくても覚えられるように，英字 1 文字と数字 2 文字の受付番号としている．受付番号の桁が短く運用を続けるうちに再利用することになるので，本システムでの申請の識別番号はユーザに提示する受付番号とは別の連番を用いる．

4.4. データ管理システム

試作ではデータ管理システムには MySQL5 を用いた．

データを格納するテーブル(registration)の仕様を表 2 に示す．**申請端末**が受け付けたパスワード再設定申

表 2　申請データ管理テーブル

カラム名	意味
index	自動連番（主キー）
terminalNum	申請端末番号
receiptNum	受付番号
receiptTime	受付日時
studentNum	学生番号
password	パスワード

請のうち未処理のものを蓄えている．

テーブル users は学生番号とユーザ名，氏名，所属との対応表である．システムによってはこのテーブルは認証サーバから得られる場合もあるが，試作システムでは認証サーバとは連動せず申請管理サーバがローカルに持つことにした．

そのほかに，**申請端末**台帳のテーブル terminals などが定義されている．

4.5. 窓口端末制御システム

WEB サーバ Apache と PHP を用いて実装した．窓口端末から学生番号が渡されるとそれに対応する申請一覧を表示する．また，現在の未処理申請一覧を作成するなどの管理機能も持っている．

窓口端末の認証は，PHP のユーザ認証と窓口端末の IP アドレスを組み合わせて行っている．

4.6. 窓口端末システム

窓口係員が学生番号を入力する手間と誤入力の危険性を考えて，窓口端末システムでも申請者の学生番号は磁気カードを用いて入力することにした．

窓口端末制御システムが apache+PHP なので，Windows など適当な OS が稼働するコンピュータで WEB ブラウザが動いていればよい．今回の試作では Windows ノート PC と Firefox を用いた．そこに磁気カードを読み取るプログラム(java で実装)を開発．導入した．

画面構成と遷移を図 4 に示す．

窓口係員は学生から預かった学生証を磁気カードリーダに通す．カードリーダから JAVA プログラムが学生番号を読み取り，WEB ブラウザに指示して対応する URL にアクセスさせる．URL はたとえば以下のような形式である．

http://サーバ名/passwdrereg/rereg.php?idnum=123456

この URL は事前に与えた URL の末尾に読み取った学生番号を付加して生成する．

4.7. 認証サーバ連携システム.

シェルスクリプトと C プログラムで実装した．データベースから取り出したパスワードは quoted-printable でエンコードされているのでこれをデコードし，ldappasswd でパスワードを暗号化した上で，ldapmodify コマンドで LDAP サーバに修正内容を送っている．

図 3　磁気カードリーダ

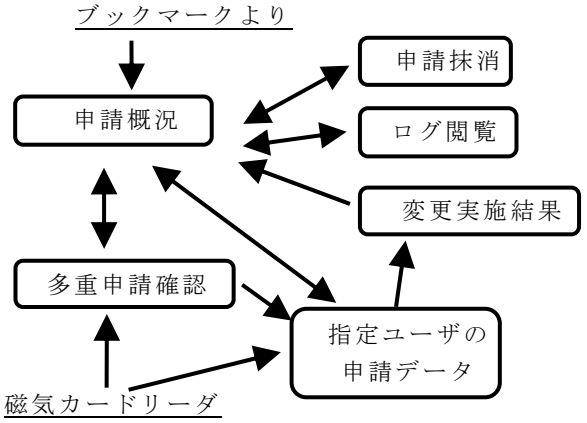

図 4　窓口端末 GUI の画面遷移

試作システムの認証サーバは OpenLDAP に UNIX 認証スキーマを入れただけで特にパスワード制約は実装していない．そのため，実在のユーザである限りパスワード変更は必ず成功する．

5. 動作テストと評価検討

5.1. 試作システムの動作

表 2 の試作システムで動作確認を行い，設計意図通りに，パスワードの受付け，窓口端末でのパスワード変更申請受理指示，といった一連のプロセスが実行できている事を確認した．

図 5~7 は，申請端末の画面である．初期画面は図 5 であり，新パスワードの確認入力が終わった段階が図 6 である．受付が完了すると，受付番号を表示する(図 7)．

図 8～10 は窓口端末の画面である．申請概況画面(図 8)では，未処理の申請が表示される．学生証を磁気カードリーダで読み取ると，指定ユーザの申請データだけ抜き出した画面を表示する．同じ学生が複数の申請をしている場合は，重複申請を警告する画面(図 9)に遷移する．重複していなければ申請を受け入れるか否かの操作画面(図 10)に遷移する．

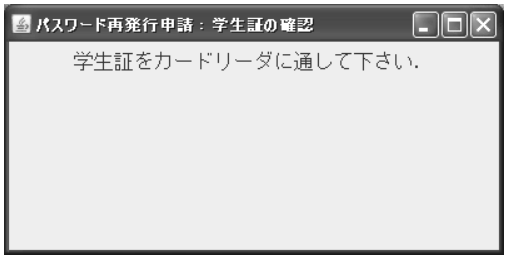

図 5　申請端末初期画面

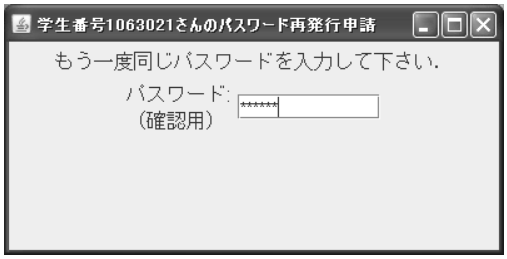

図 6 申請端末　パスワード確認

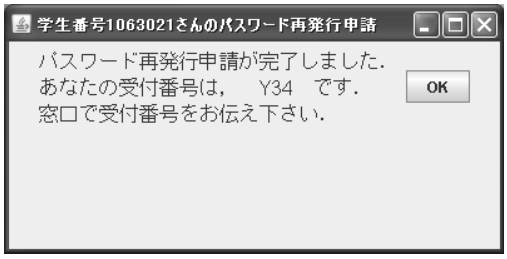

図 7 申請端末　受付完了

図 8 窓口端末―申請概況表示画面

図 9　窓口端末―多重申請者の表示

図 10　窓口端末―申請に重複がない場合

5.2. 検討

キャンパスが複数有るような大規模な大学では，計算機センターもキャンパスごとにあり，パスワード変更受付窓口も複数存在することがある．本システムでは，複数の窓口端末からのパスワード変更受理の際に特に排他制御は行っていない．ただ，同一の学生が異なる窓口に現れることはないので，現状で問題は生じないと考えられる．現状の認証サーバ連携システムは処理性能が低いが，窓口一つあたり　1～2 件/分　程度の仕事しか発生しないので問題はないと考えられる．ただし，本システムに年度初めなどの大量の学生のパスワード新規設定も行う機能を追加しようとするならば，認証サーバ連携システムは高いスループットを持つように再実装する必要がある．

6. まとめ

本研究では，大学の計算機センターなどでの忘失パスワードの再発行作業を省力化するシステムを設計し，試作を行った．このシステムは忘失パスワード変更の申請は専用端末から無認証で行い，後刻窓口で学生証の写真と申請者との照合を行う．そのため再発行の際の窓口応対が 1 回で済む．また，仮パスワードを一旦設定することなく，利用者が望む新パスワードを設定することができる．またその際，新パスワードが窓口係員の目に触れることがないように作られている．

試作した申請端末は PC に受付ソフトウェアを搭載しただけのものなので，物理セキュリティ対策がなされていない．ロビー等への設置を想定した申請端末ハードウェアの製作も今後の課題である．

文　献

[1] 高取　裕，“パスワード忘却時の再発行業務の効率化手法”，鳥取環境大学情報システム学科成果報告書集，Vol. 3，No. 1，March 2006.

[2] "識別カード―記録技術"，JIS X 6302,日本工業規格，2005.