◇◇◇◇◇◇
特　集
◇◇◇◇◇◇

情報科学センターシステムのアカウント管理・登録方法について

冨重　秀樹 [1]
中島　孔志 [2]
甲斐　郷子 [3]

1　はじめに

本センターの計算機システムは，大きく分類して，主に学部の情報基礎教育等に用いられる教育用システム，研究目的で用いられ利用度合に応じて課金される研究用システム，情報技術セミナーに利用される社会人教育用システム，学生自習用 Windows パソコンなどがあり，その他サービスとして電子メールサービスやダイアルアップ接続サービスなどがあります．基本的に本学に属するすべての職員・学生には，本センターの計算機システムを利用する権利がありますが，これらのシステム・サービスの利用を希望する場合，システム毎に利用者自身のアカウントを登録する必要があります．利用者アカウントはシステムの利用権を示しており，アカウント登録を申請して利用権を認められた者には利用者毎に異なる ID とパスワードが配布され，システムが利用できるようになります．

現在，本センターでは，このアカウント登録申請が Web ベースで行なえるようになっています．本稿では，アカウント管理に関する考え方について述べた後，教育用システムを例にとってアカウント登録申請手順について説明します．

2　利用者による ID とパスワードの管理

2.1　利用者 ID とパスワード

通常，アカウント登録申請を受けたシステム管理者は，その申請者をシステム利用者として認めるかどうかを審査し，個々の利用者を識別するための利用者 ID とパスワードの作成・登録，利用者が使える計算機資源の割り当て，利用者環境の基本的整備といった作業を行なった上で，申請者に利用者 ID とパスワードを配布します．

利用者 ID とパスワードは，銀行のキャッシュカード (キャッシュカード番号) と暗証番号と同様の働きを持ちます．利用者 ID は，個々の利用者に対する計算機資源の割り当てや個人認証に用いられる基

[1]情報科学センター，tomisige@isc.kyutech.ac.jp
[2]情報科学センター，naka@isc.kyutech.ac.jp
[3]情報科学センター，kay@isc.kyutech.ac.jp

本的な利用者識別符号で，そのシステム上で異なる利用者の ID は必ず異なるように割り当てられます．パスワードは，利用者 ID と対で個人認証に用いられるものであり，利用者 ID は一般に隠されていませんが，パスワードは当該の利用者以外には明らかにされません．

利用者 ID とパスワードによる個人認証では，利用開始時に利用者 ID とパスワードをシステムに入力し，その対がシステムに登録されている文字列と一致したら正当な利用者だと判断し，利用を許可するという方法です．利用開始時のこの作業のことをログインと呼ぶので，利用者 ID のことをログイン ID と呼んだりもします．

この方法だと，システム側も何がしかのパスワード情報を保持しなければなりません．しかし，本センターで用いられている UNIX 系のシステムでは，パスワードの文字列をそのまま保持しているわけではなく，一方向性ハッシュ関数を用いて別の文字列に変換 (暗号化) して保存しています．従って，システム管理者といえど，自分以外の利用者のパスワード文字列はわからないのが普通です．パスワードの認証を行なう際は毎回システム側で一方向性ハッシュ関数を用いて処理を行ない，その値をシステムに保管してある予め処理された文字列と比較して判断します．

2.2 情報科学センターの利用規定と利用心得

アカウント申請時にはシステム管理者による利用者審査があると前節で述べましたが，それはいったいどのようなものなのでしょうか．

一般にシステム管理者は，計算機システムの利用資格，利用目的，利用形態などをあらかじめ決めた上でシステムを運用しています．本センターのシステムについても，九州工業大学情報科学センター利用規定[4]において，第 2 条には「センターの利用は，教育，研究，教育研究支援，その他本学の運営上必要と認められるものに限るものとする」と利用目的が，第 3 条にはシステムの利用資格が「1. 本学に所属する職員及び学生」「2. 情報科学センター長が特に許可した者」と定められています．

つまり，システム管理者による利用者審査とは，アカウントの申請内容が利用規定に定められた条項に合致するか否かを調べることなのです．

また，本センターではこの利用規定以外に，ネットワーク利用が増加している最近の利用形態を鑑み，図 1 に示す情報科学センター利用心得を策定しています．これは，計算機システムが学内ネットワークだけでなくインターネットとつながることにより，システムの目的外利用や不正利用の悪影響が従来考えられていたものと比べ広範囲にわたる可能性が高くなっているため，策定されたものです．つまり，本センター計算機システムの利用者がネットワークを介して他システムの正常な運用を阻害したり他人の権利やプライバシーを侵害したりしないよう，逆に，ネットワークを介して他システムの利用者が本センターシステムの正常な運用を阻害しないよう，それらの不都合な状態をなるべく防ぐための利用形態の制約が図 1 に示す利用心得なのです．

すべての利用者は，アカウント申請にあたり，情報科学センター利用規定と利用心得を遵守することを誓約しなければなりません．また，利用に際し利用規定と利用心得を破った場合には，利用の承認を

[4]情報科学センター利用規定は以下の URL で全文が公開されていますので，ぜひご一読ください．

`http://www.isc.kyutech.ac.jp/rule/kitei.html`

上記以外にも，目的外利用の禁止，利用状況の届出，損害賠償，利用の取消，経費の負担などについて規定されています．

1. 公序良俗に反する利用
2. 著作権，特許権など，知的所有権を侵害する利用
3. 営利，宗教，政治など，本センターで認めた目的以外の利用
4. 利用者 ID およびパスワードの第 3 者への開示，貸与，あるいは譲渡
5. 他者の利用者 ID あるいはパスワードの不正な入手
6. 他者のプログラムやデータのファイル類への不正アクセスあるいはそれらの改ざん
7. 「連鎖」メールや「迷惑」メールなど，好ましくないメールの発信
8. 本センターおよび他組織の計算機およびネットワークシステムの正常運営に支障を来す利用
9. 上記の他，法令や社会倫理に反する，あるいは他者の正常利用に支障を来す利用

万一これらに違反した場合は，本センター利用規定第 8 条により利用の承認を取り消されたり，さらには関連法令によって処罰されることがあります．

図 1: 情報科学センター利用心得

取り消されたり，内容によっては学内規則や法令[5] によって処罰される可能性もあります．

2.3 悪いパスワードとよいパスワード

図 1 の利用心得における 4 番目と 5 番目は，利用者 ID とパスワードの管理に関する項目です．項目 4 は利用者のみが知っているはずのパスワードを利用者自身が第三者にもらさないこと，項目 5 は第三者が利用者のみが知っているはずのパスワードを不正に入手しないことが，定められています．つまり，パスワードは利用者のみが知っている状態を保つよう，システム管理者が利用者に求めているのです．

パスワードが第三者にもれた場合，どのようなことがおこるのでしょうか?

パスワードは利用者 ID と対でシステムの個人認証に用いられるものですから，パスワードがもれた場合，第三者が正当な利用者になりすますことができます．正当な利用者になりすました第三者は，利用者のデータを閲覧，改ざんしたり，正当な利用者にのみ利用を許可されているプログラムを使ったり，ネットワークを介して悪事を働いたりするかもしれません．その結果，正当な利用者は，自分のプライバシーがもれたり，せっかく作成したデータを失ったりするだけでなく，名誉や信用が損なわれたり，金銭的な負担が課せられたり，法的な措置が取られたりする可能性があります．何がしかの事件が起きれば，システム管理者や大学側も何らかのペナルティを負うかもしれません．

利用者による ID とパスワードの適正な管理は，その利用者およびその利用可能な計算機資源を守るだけでなく，計算機システム全体，ひいてはネットワークにつながった計算機システムを正常に運営するための基本です．そのため，パスワードを他人にもらさないことは，あたりまえに行なわなければならない事柄です．さらに第三者によるパスワードの不正入手を容易にしないよう，他人が簡単に推測できる脆弱なパスワードをつけないようにすることにも留意しなければなりません．

他人が簡単に推測できる脆弱なパスワードとはどのようなものでしょうか?

入力できるパスワードの長さはシステムにより異なりますが，本センターで提供しているシステムで

[5]現在法令化が進みつつある分野であるため法令自体を列挙することは避けますが，政府や公的団体の Web サイト (例えば内閣官房情報セキュリティ対策推進室 http://www.bits.go.jp/) において，参照時点での関連法令の全文が公開されているはずです．

は 8 文字です．パスワードとして利用できる文字は，アルファベット (大文字と小文字で 52 種) と数字 (10 種)，24 種類の記号[6]の計 86 種類です．すなわち 86 の 8 乗種類のパスワードが考えられますが，この 86 の 8 乗という数字は天文学的であり，いくら高速化した現在のコンピュータでもパスワード解読にかなりの時間が必要となります．

しかし，利用者は自分のパスワードを覚えていないといけないので，何らかのルールに則った文字列や文字数の少ないものを選びたい気持ちになりがちです．そのため，たとえば ID から連想可能な文字列あるいは自分の名前や誕生日などをつける人がいますが，そうすると利用者以外の他人にとってもパスワードの推測が容易になってしまいます．辞書に載っている単語の文字列を選んだとしても，辞書に載っている単語は多くても 100 万語程度であるので，そのような中からパスワードを推測するのは，プログラムを使えばかなり容易となります．また，文字数や字種の少ないパスワードも，探索対象となるパスワードの種類を減らすことになり，同様のことが言えます．したがってこのようなパスワードは脆弱なパスワードと言えるでしょう．

脆弱なパスワードは，利用者の計算機資源そのものや信用を危うくするだけでなく，ネットワークで学内外につながっている計算機システムのセキュリティホールとなりかねません．管理者にとって利用者の脆弱なパスワードは，本当に「悪い」パスワードなのです．

ちなみに，本センターで管理用ツールを使って学生のパスワードの脆弱性を調べたところ，実に 300 人近くの学生のパスワードが脆弱であることが判明しました．さらに，パスワードの脆弱性が判明した学生に対して変更を依頼したのですが，度重なる要請に対しても変更を行わなかった人がいました．このことは，情報処理教育を行っている本学のような工学系大学の学生であっても，ID とパスワード管理に対する危機意識が低いことを示していると言えます．

それではどのようなパスワードをつければよいのでしょうか? 絶対的によいパスワードなどというものはないので，よいパスワードは悪いパスワードでないものと言えます．以下によいパスワードの特徴を列挙します．

- パスワード全体の文字列の長さは，8 文字までが許されるシステムの場合は 8 文字のものを，それ以上が許されるシステムの場合はそれ以上がよい．
- たとえば数字のみというように同じ字種のみから選ばず，英字でも大文字と小文字を取り混ぜたり，数字や記号を含む文字列を選ぶ．
- 氏名や生年月日，学生番号，電話番号という比較的入手・推測しやすい個人情報や，地名や趣味に通じる名 (商品名や作品タイトル名等) といった安易に推測できる文字列は使わない．
- 辞書に記載されている単語をそのまま使わない．

また，パスワード管理については以下の事柄に留意してください．

- 1 つのアカウント (ID，パスワード) の使いまわしをしてはいけません．自分のパスワードを他人に教えるなどして自分のアカウントを他人に使わせないでください．

[6]具体的な記号については情報科学センター編「ISC ローカルガイド」を参照してください．

- 利用開始時に配布された初期パスワードはできるだけ早く変更してください．また，パスワードは定期的に変更すると安全性が高まります．
- 利用者 ID とパスワードを書いた紙を人目につく場所においたりしてはいけません．計算機内部に格納するのは論外です．複数の人間が使用するパソコンなどから利用する場合，ログイン画面やサービスのパスワード入力画面上にパスワードが残るような設定にしないでください．
- 周囲の人が見ていたとしても分からない速度でパスワード入力できるようにしてください．自信がない場合には，周囲に人がいないことを確認してパスワードを入力してください．
- 複数のシステムを利用している場合には，1 つのパスワードがもれた場合でも他に影響しないよう，それぞれ異なるパスワードにしてください．
- パスワードがわからなくなった場合には，即座にシステム管理者へ申し出てください．
- ログインできなくなったり，ファイルの増減や改ざんがあったり，アクセス履歴に覚えがないなど，何か変だと思われる事柄があったら即座にシステム管理者へ通報してください．

3 管理者による利用者 ID とパスワードの管理

システム管理者は，利用者のアカウント管理として，利用者 ID とパスワードの発行・廃止，個人認証機能の実現・設定，各種ログの管理などを行ないます．

3.1 利用者 ID とパスワードの発行・廃止

表 1 に，本センター計算機システムにおける主なアカウント種別と，種別毎の利用者 ID とパスワードの発行・廃止時，ID が選択可かどうかについて示します．このうち，すべてのアカウントの基本となっているのが (1) 教育用システムの (1a) 学生用および (1b) 職員用です．(1a)(1b) 以外のアカウント申請には (1a)(1b) の利用者 ID とパスワードが必要となるからです．

表 1: 情報科学センター計算機システムのアカウント種別

アカウント種別		利用開始	利用終了	ID の選択	備考
(1) 教育用システム	(1a) 学生用	入学時	卒業時	不可	—
	(1b) 職員用	申請時	退職時	可	—
	(1c) 講義用 (教官・技官)	申請時	申請年度の末日	可	継続利用可
	(1d) TA 用 (学生)	申請時	申請年度の末日	可	—
(2) Windows PC		申請時	卒業又は退職時	(1a)(1b) と同じ	—
(3) 研究用システム		申請時	申請年度の末日	(1a)(1b) と同じ	継続利用可
(4) ダイアルアップ接続		申請時	卒業又は退職時	不可	—

表 1 を見てわかるように，本センターの計算機システムを利用するためには基本的にアカウント申請が必要です．ですが，教育用システムの学生用アカウント (表 1 の (1a)) に関しては，入学してきた学生全員のアカウントを自動的に作成するようにしています．これは，本学のすべての学生が情報処理教育を受けることとなっており，毎年 4 月初めの数日間で約 2000 人もの新入生 (編入生，大学院生，聴講生含む) に対し，入学直後の授業開始時までにアカウント発行を間にあわせなければならないこと，毎年大量に入れ替わる学生の ID を学生の自由につけると管理上不都合が多いことなどを考慮した結果です．教育用システムの学生用 ID は，学生番号，氏名等の情報から，パスワードは 2.3 節で述べたよいパスワードの条件を満すよう作られています．

これらの利用者 ID とパスワードは，学部 1 年生と 3 年次編入生については，入学直後の本センターを利用する授業において講義担当者から配布されます．利用規定と利用心得については講義担当者から教わることを前提としているからです．大学院生と聴講生については，本センターに学生証を持参した学生に対して，その場で利用規定と利用心得を読んでもらい，遵守することを誓約してもらった上で，本センター職員が配付しています．

(1a) 以外については，オンライン上から利用者自身で登録申請ができるようになっています．登録申請の方法については 4 節で説明します．

3.2 個人認証機能の実現・設定

本センター教育用システムとして講義室に数百台の Linux 端末を設置していますが，これらの Linux 端末はどこからログインしても利用者 ID とパスワードは有効です．これは，ネットワーク上の複数の計算機において利用者 ID やパスワード等を共有する機能を利用しているからです．

この機能の実現については，NIS(Network Information Service) や NIS の機能向上版である NIS+ と呼ばれるソフトウェアを利用するのが普通ですが，現システムの運用開始時にはこれらを使わないと決定しました．NIS については，それ自身セキュリティ的に脆弱であり，また近年のシャドウパスワード[7]やロングパスワード[8]などの新しいパスワード形式にも対応していないという欠点を持っていたからです．これらの点を改良した NIS+では，実際の大規模システムでの利用例がほとんど見当たらず，多数の利用者が一斉に利用する場合の応答性などの情報が得られなかったという事情がありました．

そこで現システムでは，共有システムファイル領域に含まれる Linux 標準のパスワードファイル (シャドウパスワード) をそのまま共有する方法をとりました．この方法では，login 操作などに際して参照するだけなら，特別なことをしなくても全端末でパスワード情報を共有することができます．

ただし，この方法では，既存のパスワード変更方法 (passwd，yppasswd) は使えなくなるため，オンラインでパスワード変更が行えるよう Web ページを作りました．以下の URL で示されるオンライン登録ページから「パスワード変更」の項を選択し，ID，パスワード，新しいパスワードなどの必要事項を記入した上でパスワード変更ボタンをクリックすれば，30 分ほどでパスワードが変更されます．

戸畑キャンパス `http://edu.tobata.isc.kyutech.ac.jp/touroku/`

飯塚キャンパス `http://edu.iizuka.isc.kyutech.ac.jp/touroku/`

[7]暗号化したパスワードを一般ユーザが参照できない場所に置く方法

[8]8 文字以上使えるパスワード

これらのページは教育用システムのみに対応しており，また学外からのアクセスを制限しています.

3.3 各種ログの管理

ネットワークや計算機に障害がおきた場合，管理者は早急に通常状態へ復旧させるよう努力するだけでなく，障害の原因を解析して同様の障害が再発しないようにも心がけなければなりません．また，利用状況に関する統計情報を収集し，特定の計算機資源に対する利用状況の変化などに追随できるようにすることも重要です．そのため，管理者はネットワークや計算機システムを監視しており，重要な管理用データについてはそのログを一定期間保存します．例えば，利用者が計算機を使うとき，まずログインし，その後は例えば電子メールを使ったり Web ナビゲーションしたりするわけですが，このような計算機利用に関する情報もログとして記録されています.

管理者は自システムに対する不正アクセスだけでなく，他の管理者が管理するシステムに対する不正アクセスに対しても，ログを使って不正アクセスの原因を特定したり，不正アクセスから計算機資源を守るようシステムの設定変更をおこなったりします．しかし，利用者が多数でシステム構成が複雑な場合，管理者は小規模な不正アクセスが発見できない場合もあります．利用者によるこまめなチェックが大切です.

4 教育用システムの職員用アカウントの登録手順

教育用システムのアカウントは本センターの基本的なアカウントですので，教職員[9]が本センターの何がしかのシステムまたはサービスを利用希望する場合，希望者自身でまず教育用システムの教職員用アカウント登録申請する必要があります．ここでは教職員がオンライン上から登録申請する方法について説明します.

1. 以下に示すオンライン登録ページから「各種 ID 登録」の項を選択します.

   戸畑キャンパス `http://edu.tobata.isc.kyutech.ac.jp/touroku/`
   飯塚キャンパス `http://edu.iizuka.isc.kyutech.ac.jp/touroku/`

   オンライン登録ページは SSL(Secure Sockets Layer) に対応しているため，初めて登録ページを利用する場合サイト証明書ウィンドウが表示されます．SSL はデータ通信路上に流れるデータを暗号化する機能であり，第三者が通信路を盗聴したとしてもプライバシーに関わる情報を知られることが防止できます．つまり，SSL を用いることで，利用者が入力した利用者 ID とパスワードは守られるのです．ここでは，サイト証明書を受け付ける手続きを行わないと，SSL 機能が有効にならないことに加え，登録ページを開くことができないので注意が必要です.

   サイト証明書を受け付ける手続きでは，表示される情報が正しい場合に「続ける」または「次へ」ボタンをクリックし，手続き終了時には「完了」をクリックします．証明書を受け付けるかどうか尋ねるパネルでは「証明書を受け付ける (有効期限まで)」を選択します.

[9] 学生については 3.1 節で述べた通り，授業での配布か本センター窓口での配布になります.

2. サイト証明書の手続きが終了後,「情報科学センター利用心得、承諾確認パネル」が表示されるため，**情報科学センター利用心得**を一読後,「遵守する」をクリックします.

3. 図 2 に示す各種 ID 登録パネルが表示されるので必要事項を記入します．登録項目のプルダウンメニューでは「職員用」に変更します．記入終了後誤りがなければ「次へ」をクリックします.

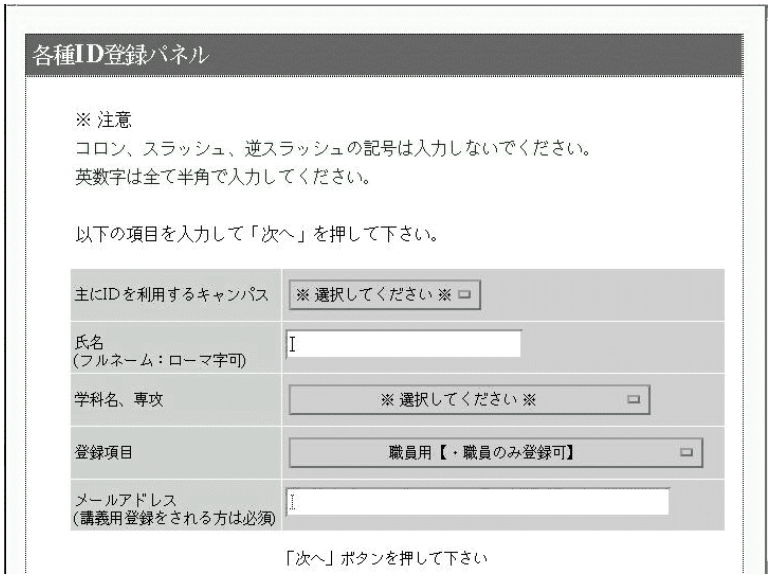

図 2: 各種 ID 登録パネル (1)

4. 図 3 に示すパネルが表示されるので必要事項を記入します．ログイン ID(利用者 ID) はユニーク (自由) な名前を指定することができますが，大文字は指定できないので注意が必要です.

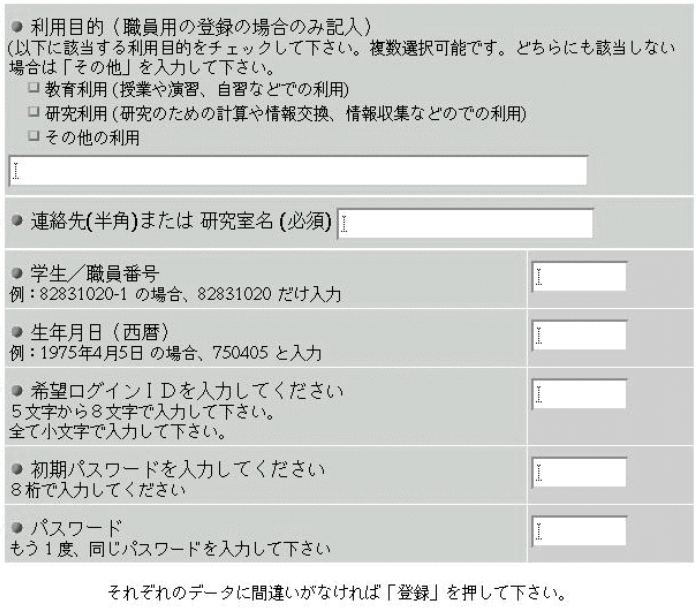

図 3: 各種 ID 登録パネル (2)

5. 記入終了後誤りがなければ「確認」をクリックします．およそ 30 分ほどで登録が完了し，ログイン ID(利用者 ID) は利用可能になります．

この後，教育用システムの講義用アカウント登録[10]をしたい方や，Windows PC，研究用システム，ダイアルアップ接続などを利用したい方は，教育用システムの職員用アカウントが登録されたことをログインしてみるなどして確認した後，今回のアカウント登録と同様に各システムのアカウント登録を行なってください．

5 おわりに

本稿では，一般的な利用者のアカウント管理に関する考え方について述べた後，本センターの利用者アカウントの管理と登録申請方法について説明しました．アカウントの管理は計算機利用の基本ですが，ついつい基本なだけに，長く利用していると簡単に使いたい気持ちが強くなってしまい，安易な方向に流れてしまうこともあるかと思います．しかし，新聞や TV，インターネット上でも，情報セキュリティに関する事件が毎日のように報告されていることからわかるように，ほんのちょっとしたことと思っていることが，大きな事件を引きおこすことにもなりかねません．ネットワーク時代において安全なコンピュータライフをおくるために，安全な利用者アカウント管理を心がけてください．

[10] 講義用と TA 用のアカウント登録は，事前に申請書の提出が必要です．