

休眠アカウント調査のためのWebを利用した情報サービス利用者確認システムの構築と運用

櫻田 武嗣[†], 石橋 みゆき[†], 萩原 洋一[†]

[†] 東京農工大学 総合情報メディアセンター

情報サービス利用アカウント、特に学会等のイベント開催用に取得されたアカウント等が利用・管理されなくなると不正利用される危険性がある。このため定期的に利用者確認調査を行い、アカウントの廃止処理を行う必要がある。本稿では情報センター系施設において提供するサービスを一元管理するためのシステムとこれを利用したWebによる情報サービス利用者確認システムの構築と運用結果について述べる。Webによる情報サービス利用者確認では紙で行うよりも回収率は上昇した。これによりWebを使うことによる回答回収に影響が無い、むしろ回収率が向上することが確認できた。また利用者の回答日は電子メール送付日または翌日に集中しており、電子メールを読んですぐに回答の行動に移っていることが分かった。未回答者へ回答を促す電子メールの再送信を早めに行うことにより、回答回収率は向上した。しかしながら、毎年ほぼ一定数が回答を行っていないことが判明し、その未回答者の半数は紙でもWebでも全く回答をしないことが分かった。今後さらに未回答者の特徴を分類して行く予定である。

Construction of an investigation system of user account with Web interface.

Takeshi SAKURADA[†] Miyuki ISHIBASHI[†] Yoichi HAGIWARA[†]

[†] Information Media Center, Tokyo University of Agriculture and Technology

This paper describes a database system for information service management and an investigation system of user account with Web interface. Since there are some risks that user accounts of information service is used illegally if once they are not used or administrated, periodical investigation of usage and invalid process of unused accounts are required. Thus, we constructed a database system and an investigation system of user account with Web interface. Regarding information service user confirmation, collection rate was more increased with web than with paper. Besides, it has been clarified date of user response is concentrated on the day email with questionnaire has been sent or the next day, and respondents decide to answer soon after reading email. With this result, we could raise the collection rate of response by sending unanswered respondents the email to press them to answer. We are going to classify the characteristics of non-respondent in future.

1 はじめに

近年情報化が進み多くの情報サービスが利用されている。大学も例外ではなく、大学の情報センター系施設の多くは日々多くの情報サービスの提供を行っている。昨今は産学官連携の流れもあり、情報サービスは教職員、学生だけでなく企業や他の研究機関から受け入れる共同研究者等に対しても提供することが多くなっている。年々扱う情報サービスの種類、利用者数共に増加しているにも関わらず、情報センター側の人員強化などを見込むことは難しく、少ない人員で対応しなくてはならない現状がある。

情報サービスの管理では、利用者情報の管理が欠かせない。大学では教職員、学生以外にも企業や他の研究機関からの共同研究者の受け入れ、短期留学生や単位互換学生、聴講生など様々な身分の方が大学の施設を利用しており、利用期間も長期、短期と様々である点に特徴があり、受け入れ窓口も様々で一般企業のように利用者情報の一元管理を行うことは現実的に難しかった。

東京農工大学（以下本学と記す）は約7000人の構成員（学部生約4200人、大学院生約2000人、教職員その他約800人程度）を抱える組織である。その他に産官学連携などによる研究員受け入れ等が

あり、全学共同利用施設である総合情報メディアセンター（以下、本メディアセンターと記す）では構成員の人数7000人を大幅に超える利用者に対してサービスを提供している。現在提供している主要なサービスは、メールアドレスの発行、端末演習室・無線LAN・リモートアクセスの利用、学内ネットワーク接続、Webサーバの利用、固定IPアドレスの発行である。

本メディアセンターでは2005年度からデータベースの再構築を行うと共に、Webによるアカウント等の新規・廃止申請を含めた自動化システムを構築し、日々改良を行っている。本学においても構成員データが完全には一元管理できていないため構成員の移動情報の漏れが生じる恐れがある。また学会等イベントを開催後に利用されなくなったアカウント等の廃止申請が出されず、管理されずに放置されるケースが目立っていた。これらはソフトウェアのライセンス資源やIPアドレス資源等に無駄を生じさせるばかりでなく、使われていないアカウントが不正利用されてしまう危険性もあり問題である。そのため、本メディアセンターでは使われていないアカウントを洗い出すため、年1回利用者に対して利用者確認調査を行っている。調査結果を基に、アカウントの廃止処理を行い、放置されたアカウントが不正利用される危険性を減らしている。

本稿では、情報センター系施設において提供するサービスを一元管理するために構築・運用しているシステムについて述べる。またこのシステムを利用したWebによる情報サービス利用者確認システムの構築と3年間運用した結果について述べる。

2 提供サービスを一元管理するシステムの構築と運用

Webによる情報サービス利用者確認システムの構築と運用について述べる前に、提供サービスを一元管理するために構築・運用しているシステムについて述べる。

2.1 大学における情報系センターでの管理問題

大学の情報系センターでは、各種情報システムとネットワークを主に管理しており、管理しているデータは大きく情報システム利用のためのアカウント情報、ネットワーク接続のためのIPアドレスに関する情報^{1) 2)}の2種類に分類される。

アカウント情報は統一認証に含まれるシステムであれば基本的に1人1アカウント分を管理すれば良いが、そうではないもの、例えば統一認証に含まれない古いシステムや利用形態が1人1アカウントではない（1アカウントを複数人で共用したり、1人で授業用、個人用などと複数アカウント使用したりする旧来の）システムには対応できないため、統一認証システムを導入してもこれらは別途管理する必要がある。統一認証の導入だけでは管理コストの削減が難しい状況^{3) 4) 5) 6) 7)}があった。

また大学特有の状況として、正規教職員、学生以外にも研究員やアルバイト、単位互換聴講生、公開講座などでの地域住民の利用などがあり、利用する可能性のある人物を全て把握することが難しい点や人の出入りが多い点がある。以前に申請されたアカウントやネットワークが現時点でも使用されているかを知るためには定期的に何らかの方法で確認をとる必要がある。実際に、利用者自身は在学、在職だが、使われていないアカウントが放置されることがあり、これら不要な休眠状態のアカウントが放置された場合、それを足がかりに不正使用される危険性がある。全ての大学で何らかの調査を行い休眠アカウントを拾い出す処理をしているわけではないが、本学の場合は毎年1回、利用者に向けて書面を送り、実際にアカウントや固定IPアドレスを利用しているかを確認する「利用者確認調査」を行っていた。この作業も利用者の所属の確認、書面の作成、発送、回収、集計といった手間がかかってしまう。しかしながら、実際の利用者の入れ替わりを確実に把握するためには必要なものであった。

本学においては、帳簿を1996年12月からデータベースに置き換えて提供サービスを個別に管理してきたが、データへのアクセスコントロールを細かく集中管理し、個人情報保護、情報漏洩対策を行う必要性が増してきたため、提供サービスを一元管理するシステムの設計・構築を行った。また、利用者の利便性の向上と近年のペーパーレス化の流れに伴い、これまでは利用者からの申請を紙をベースに行っていたものをWebベースで行えるよう合わせて設計・構築を行った。

これらはシステムを一度全て停止し、発行済みアカウントもすべて抹消して、新しいシステム

上に新たに申請を受け付ける形であればシステム側をカスタマイズするなどし、統一認証システムに統合し、管理形態を簡単することが可能ではあるが、多くが運用を止めずに動かし続けなくてはならないシステムであり現実的ではない。このため、既存システムとの連携を考慮に入れた基幹となる新データベースシステムの構築が必要であった。

2.2 新一元管理システムの設計と構築

新一元管理システムは、第一に自動化を進め運用側のコストを低減すること、第二に利用者の利便性をはかること、第三にセキュリティを確保できる形にすること、第四にこれらが現実的な形で導入できることが目的である。現実的な導入は、システムを統合しようとした際に理想的な形だけを追い求め、運用の際に統合できないシステムが出てきてしまい、かえってコストが増えてしまうという問題が起こりうるからであり、システム構築の議論では忘れられがちであるが重要な点である。

2.2.1 提供システムの利用アカウントの集約

提供しているシステムの利用者情報を一元的に管理するためには、まずはアカウントとパスワードをできるだけ集約していくのが利用者側から見ても良く、今回の設計と構築で統一認証を導入することとした。しかしながら、前述のように実際に運用しているシステムでは統一認証に向くものと向かないものがあり、分類を行ったところアカウントと利用者の実際の対応関係は大きく3つに分けられた。

1. 1人の利用者に対して1つのアカウントだけを発行して利用
2. 1人の利用者に対して複数のアカウントを発行して利用(例：担当授業科目利用と個人利用)
3. 1つのアカウント(または共同作業領域)を複数の利用者が利用(例：共通授業科目で使用、部署内で共有)

利用形態(1)はシステム利用のアカウントと人物が1対1の対応であるため、統一認証に統合すればよい。利用形態(3)は適切なグループを作って個人のアカウントに対してアクセス権など付与する形が望ましいが、現状で動いているシステムの中にはそのようなことが考慮されていないものもある。そのため、システム利用アカウントと人物

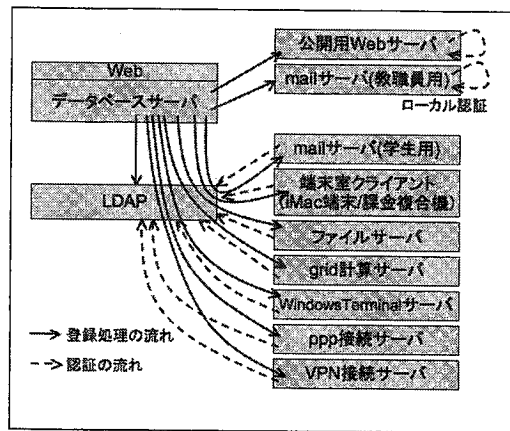


図1 構築システム全体図

が1対1の対応ではない利用形態(2)、(3)には統一認証を使わず、従来のアカウントとパスワードの組を発行する方が現実的である。ただしこの場合には、その利用アカウントの責任者を紐付けしておく必要がある。本学の場合、どの利用アカウントでも発行申請を行った人を責任者として管理する。特に利用形態(3)の場合、誰とアカウントを共有しているかはその責任者となった人が管理することとし、本メディアセンター側では関与しない形として管理責任の分解点を明確にした。

これらを踏まえ、管理用の基幹データベースを新規構築し、利用者情報の管理、アカウント情報の管理を行った。各システムと基幹データベースの連携の全体像を図1に示す。本稿の設計・構築で構築する統一認証システムはLDAPを基幹とする。ただし、LDAPに対応していないシステムは、LDAPサーバ上に連携用のコマンドを置き、LDAPサーバの変更を各システムに自動送信する。その他の統一認証を用いないシステムは、基幹データベースからアカウント名・パスワードのデータをそれぞれのシステムに出力し、認証はそれぞれのシステム内部の認証機構を用いる。本メディアセンターは、公開用Webサーバ、mailサーバ(教職員用)は統一認証を用いないが、それ以外のmailサーバ(学生用)、端末室、ファイルサーバ(端末室、メールサーバで利用)、grid計算サーバ、高速計算機サーバ、WindowsTerminalサーバ、ppp接続サーバ、VPN接続サーバは統一認証を用いる。

2.2.2 IP アドレス・ファイアウォール管理の集約

これまで本メディアセンターでは、IP アドレス・ファイアウォールのルールは何かログインするためのものではないため、利用アカウントとは別々に管理を行っていた。しかしながら、1つのIP アドレス自体をアカウント名と考えれば、前述の「1人の利用者に対して複数のアカウントを発行して利用」の形態と一致する。個々のIP アドレスに対するファイアウォールのルールを、それぞれのIP アドレスの付属情報として持たせることにより、利用者アカウントと同様に管理する。

2.2.3 Web による利用者申請と実システム反映までの自動化

今回の設計・構築では、一元管理するシステムを構築するが、単純なアカウント等の統合だけでは、管理コストの低減、利用者の利便性の向上にはつながらない。利用者がシステムを利用するためには申請等を行う必要があるが、その申請もオンライン上で常に受け付けられるようにし、申請を確認した後、実システムへの反映が自動化できれば管理コスト、ユーザの利便性も向上する。

利用受付に関しては、本人からの申請かどうかを確認する必要がある、いたずらで申請が行われないかを判断する必要がある。また、長期出張期間中に利用申請を代理で行う、採用予定のアルバイト等にシステムを利用させたい、採用予定の人に代わり申請を行う等、大学での実際の運用ではこれまで必ずしも利用者本人が自ら申請をしていないことがあった。それらを想定した流れをシステム構築前にあらかじめ考えておく必要がある、ネットを利用した申請・変更申請を行う場合にはいたずらの防止のためにも特に本人認証を簡単に行うことができる必要がある。

今回の設計・構築での利用者の申請から実システムへ反映するまでの流れを図2に示す。まず利用者はWeb 上から各システムの利用申請を個人の識別記号（職員番号・学生番号ベース）を入力して行う（図2(1)）。データベース上にはあらかじめ大学事務部門で把握している個人の識別番号と本人の連絡先（メールアドレス）の組が格納されており、申請の際に入力された値とデータベースに格納されている値の組が一致した場合のみ登録処理を続けることができるようにし、いたずらを防止する。ただしこれだけでは万全ではないため、

Web 上での申請処理が終わり次第連絡先のアドレスへ申請内容の確認メールを送信する（図2(2)）。

メールには申請内容とワントime用に自動生成したページへのURL が記載されており、メール内のURL をクリックしてWeb ページを表示し、表示されたページ内の確認ボタンを押すことで本人確認と申請内容の確定をする。確定されると自動的に受付承認待ちデータベースへその情報が登録される（図2(3)）。即座に実システムへの登録を行うことも技術的には可能であるが、異常な量の利用申請や機器トラブルなどのトラブルに対応するため、メディアセンター側のシステム管理者が一度申請内容一覧を管理者用Web ページからチェックする。チェックし終えたものは実システムへ情報を反映させるため自動的に処理待ちテーブルへ情報を格納される（図2(4)）。処理待ちテーブルを用意し、システムの実登録を直接行わない理由は主に3つある。第一に自動化できないシステムに対応するため、第二に一定の時間帯にまとめて反映をするため、第三に実システムが応答しないなどのエラーに対応するためである。実システムに変更を反映させる時にシステムに負荷がかかったり、サービスの停止を伴ったりするものがある場合に、利用者のいない、または少ない一定の時間帯にまとめてシステムへの反映を行うことは必要である。また、実システムが応答しないなどのエラーに対応することは、管理用のデータベースと実システムで不整合が起きないようにするために必要である。したがって、各段階で待ち受けのためのデータベーステーブルを用意し、申請、実システムへの反映を管理する。

利用者の登録・変更・削除申請はすべてWeb ページを通して行い、クライアントOS に依存しない形にするため、同じ利用アカウントに対して複数の（変更）申請を同時に出される可能性がある。変更が実システムに反映される前に次の申請を受け付けてしまうとデータ整合性がとれなくなる可能性があるため、同一システムの同一利用アカウントに対して一つでも申請が処理中の場合は、その処理が実システムに反映されるまでは申請を受け付けられないようロックする仕組みを一元管理システムに持たせた。

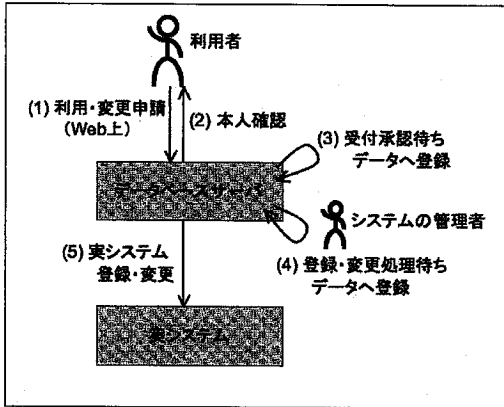


図 2 登録処理の流れ

2.2.4 パスワードの再発行の自動化

メディアセンターの窓口対応で一番多いのは、パスワード忘れによる再発行処理である。さらに本学ではリプレースの関係で2006年4月に端末室の入れ替えがあり、端末室用のパスワードの新規発行も必要であった。そこでこの機会に統一認証に移行することとし、パスワード再発行の自動化の設計・構築も合わせて行った。従来は学生証や教職員証 (IDカード) の提示を求め、パスワード再発行専用用紙に必要事項を記入してもらい受け付けを行っていた。

本構築では、IDカードに記載されている人物識別記号 (学籍番号や教職員番号など) を読み取り、パスワードを新規にランダム発行し、レシートプリンタ等から出力する。その情報は自動的に実システム登録・変更待ちデータへ登録し (図2(4))、定期的に実システムに反映する。

統一認証のパスワード再発行のソフトウェアは、IDカードを機械的に読み取り、別途暗号コードを付与し、データベースサーバのWebサービスに接続する。Webサービスからの戻りをレシートプリンタに印字し、ユーザはそれを持ち帰る形とした。レシートには、新規パスワード、アカウント名の一部、発行日時が記入されている。パスワード変更希望者が殺到した場合の混乱に備え、アカウント名を一部表示する。一部表示としているのはそのレシート紛失の際にパスワードが漏れることを防ぐためである。IDカードの読み取りは、現在はIDカードに記載のバーコードを読み取っているが、

ICカード (Felica)、磁気ストライプの読み取りにも対応している。実システムへの再発行パスワードの反映は一定間隔 (15~30分間隔) で自動実行している。

統一認証ではないシステムのパスワード再発行は、後述のWebによる管理インタフェースを窓口対応員が操作することでランダムパスワードを発行してレシートプリンタから印刷し、利用者へ手渡す。

前述の利用形態 (2),(3) の場合は実際には「申請者=利用者」とならないことがありうる。パスワード忘れでは利用者が窓口を利用者が訪れることになるが、個々のアカウントに関して利用者が誰かまでは管理できないため、データベースでは申請者情報でアカウントを管理している。パスワード再発行に来た方が申請者と一致しない場合にはパスワードを再発行してレシートを渡すが即座にシステムには反映せず、申請者に電子メールでパスワード再発行申請があったことをワнтаイムWebページのURLとともに通知する。アカウントの申請者はその電子メール内のワнтаイムURLにアクセスし、そのパスワード初期化を承認するかしないかをデータベースサーバに送信する。承認された場合、一定時間後に実システムに反映される。いたずらで申請された場合には承認しないことで、そのパスワード再発行申請自体が破棄される。また一定期間ワнтаイムURLへアクセスがない場合には、同様に申請を破棄する。

2.2.5 Webによる管理側インタフェース

本メディアセンター側の管理インタフェースでもデータベース操作をWeb画面を用いてクライアントOSに依存しないようにした。システム管理者はWeb画面上からデータベースの状態の他、図2の受付承認待ちの状態確認・承認等を行う。段階に応じてApache等のパスワード機能を使って閲覧制限をかけている。電話や窓口の対応ではシステムの登録・処理状況の確認が必要であるが、余分な情報を見せるとデータの流出の可能性もあり、それを防ぐために閲覧制限をすることが必要である。また、模擬画面を作成して事前に電話・窓口対応担当からヒアリングを行った結果、画面に表示される情報が多すぎても複雑になり短時間で必要な情報を抽出しにくいという意見が出たため、表示するデータもそれぞれの段階に応じて最低限の

ものとしている。

2.2.6 システムの構築

実運用を考えた場合、数年毎に機器の交換、ソフトウェアのバージョンアップが必要となる。そのため、汎用的でオープンなソフトウェアを使用するのが望ましい。そこで今回の構築では、データベースはSQLを使用するMySQL 5、WebサーバにはApache2を用い、CGIにはPHP4を用いてページ等を構築した。PHPには処理の高速化のためZend optimizer、データベース連携のためpearをインストールしている。

実システムへの変更反映はcronを利用し定期的にperl、PHPで記述のスクリプトを走らせている。各々のバージョンは、セキュリティホールが発見され次第適宜アップデートする。

新一元管理システムのサーバには、ハードウェア・OSにはXserve G5(Dual CPU / Memory 2GB / 80GB HDD x3 / グラフィックカード内蔵 / Gigabitイーサネットボード追加)、Mac OS X Server 10.4を用いた。

2.3 新一元管理システムの運用状況

2008年7月末現在の運用管理状況は、アカウント利用者数8153人、アカウント数27338である。学内LANはDHCPによりIPアドレスを配布しているが、固定IPアドレスとして申請されている数は13880件であった。パスワードの自動発行(新規発行・パスワード忘れの両方を含む)は一日平均約60件行われている状況であり、電子申請は2008年7月末までに8841件行われた。

Xserve G5のメモリは1.7GB使用しており、ほぼMySQLでの利用である。またCPUの負荷率は約1割で、現運用での最大負荷時には5割程度、http接続でのタイムアウトも発生しておらず、Xserve G5で性能上問題はない。

3 Webによる情報サービス利用者確認システムの構築と運用

冒頭の問題点でも述べたように、特に大学では学会開催によるアカウントの作成、利用者の入れ替わりなどがあり、休眠状態のアカウントが発生しやすいが、それを確実に把握することが困難である。このような大学特有の状況を解決するため、利用状況の確認を行う場合がある。アカウント1件ごとに確認の書面やメールを送付し確認を行っ

ても良いが、利用者側が複数システムを使うようになると利用者によくの確認書が届くことになり、利用者の負担が増える。また利用者からの回答をメディアセンター側で集計する際にも手間がかかってしまう。そこで構築・運用している一元管理システムを利用し、回答結果を自動的にシステムに反映するWebを利用した利用者確認のシステムを構築・運用する。

3.1 システムの設計と構築

前述の提供サービスを一元管理するシステムの構築・運用を行ったことにより、利用者がどのシステムを利用しているかの把握が簡単になった。そこでこれまで紙で行ってきた利用者確認の代わりに回答結果を自動的にシステムに反映するWebを利用したシステムを構築・運用することとした。利用者確認調査は、何らかの申請をしたことがあり、現在有効なアカウント、固定IPアドレス申請がある各利用者に対してそれぞれ一つのWebページアドレスを生成(セキュリティ確保、間違い防止のため観点からURLはランダムに重複なく生成)し、それを利用者に対して電子メールで送付する。申請者はこの電子メール内のURLにアクセスし利用者確認調査を行う。利用者一元管理システム側にはWebページを閲覧していない、閲覧済み、確認データ送信済みといったステータスが保持される仕組みをとる。利用者確認回答期間を過ぎると生成したURLは無効とし、利用者確認のとれなかったアカウントの停止処理を行う。利用停止後一定期間で自動的に完全にアカウントを廃止とする。

3.2 利用者確認調査の実施と考察

Webによる利用者確認を2006年から実施した。2006年から2008年までの3年間の実施結果を述べるとともに考察を行う。

確認調査初年度は利用者へ送付した利用者確認Webページから、各システムの利用の継続または廃止を選択してもらった。次年度以降は、廃止の場合だけ別途通常のWebページで廃止申請をしてもらう形とし、電子メール内のURLを確認すれば利用継続処理とした。初年度調査を行った際に利用者側から、多くは継続であり、利用者確認調査のWebページ内と通常のWebからの廃止申請の2つの方法があるのは分かりにくいとの意見が多く寄せられたため、利用者確認調査は次年度以降は確認だけとした。調査対象の利用アカウントに

は統一認証を含んでいないため、端末室の利用アカウントや学生用電子メールアカウントは調査対象となっていない。従って利用者確認の対象は教職員である。

利用者確認調査対象のアカウント数を表1に、回答数の推移を表2に示す。2005年は各個人ごとに利用アカウントの一覧が印刷された調査票（紙）を送付し、回答してもらった。2005年の調査対象は402人、調査期間は14日で、回答が寄せられたのは319人で79%の回収率であった。2006年以降は本稿で述べたシステムを利用し電子的に行った。

経過日ごとの回答数の変化の2006年の部分を見ると、利用者確認調査の電子メールを送付した当日または翌日に利用者確認調査の回答が集中し、それ以降は回答人数が急激に減少していることが分かる。このことから回答の行動に移るのは電子メール開封日かその翌日であると推測し、締め切り日前に回答していない利用者に対して回答を促すため、電子メールを2006年は10日目、2007年は8日目、2008年は7日目にそれぞれ再送付した。回答人数がこの電子メールの再送付時に増えていることから、回答していない利用者に対する電子メールの再送付は効果があったと認められる。また調査期間が長くても回収率はさほど変化しないことが読み取れるため、2008年は調査日数を1日短縮し、電子メールの再送付を早めに行った。2008年は調査締め切り後に未回答者に電子メールを送信し、調査期間終了日の翌日だけ受け付けた結果、駆け込みで回答があった。これは電子メール開封日、翌日に回答が集中する点に加え、締め切りが1日しかないことから、回答行動を起こす効果が大きく現れたと考えられる。このように工夫を行うことで、調査期間中の回答率は2006年約80(83)％、2007年約83(85)％、2008年87(95)％と回答率を年々向上させることに成功した(括弧内は締め切り後の回答数を含んだ率)。特に2008年は調査期間を1日短縮し、終了後に1日だけ受け付ける形式をとったため、全体としての回答受付日数に変わりはないが、調査期間と回答を促す通知を適切に組み合わせることにより回答回収率を大幅に向上できた。

電子化したことにより回答率が向上しており、紙を利用した調査では回答していなかった人がWebを利用した調査では回答をしており、利用者確認調

表2 利用者確認調査の回答人数 [人]

経過日数	2006年	2007年	2008年
1日目	112	225	350
2日目	226	150	65
3日目	31	40	17
4日目	20	12	11
5日目	14	10	1
6日目	3	2	1
7日目	1	0	151
8日目	19	106	42
9日目	8	41	10
10日目	127	12	10
11日目	52	11	5
12日目	28	11	—
締め切り後	18	12	63
回答者/対象者	659/795	662/783	726/765

査の電子化は有効であったと言える。つまりWebを使うことによる回答回収に影響が無い、むしろ回収率が向上することが確認できた。2005年の紙での利用者確認調査で回答をしていない利用者は、電子化されてからも毎年20人程度は回答しておらず、紙の調査の時も含め、全ての年で回答していない人は10人(全体の1.3%)であり、電子化するしないにかかわらず、一定の人数は回答をしないことが改めて確認できた。

4 おわりに

本稿では、情報センター系施設において提供するサービスを一元管理するために構築し、運用しているシステムと、これを利用したWebによる情報サービス利用者確認システムの構築と3年間の運用結果について述べた。Webインタフェースを備えたデータベースを構築して一元管理することにより、これまで分散していた情報を連携して管理することができ、情報サービスの利用・廃止申請をWebベースで行うことも可能となった。Webによる情報サービス利用者確認は、各利用者ごとにURLを自動的に生成してあるため、各利用者が受け取った電子メール内のURLにアクセスするだけでシステム利用者確認が可能なこともあり、紙

表 1 利用者確認調査のアカウント数

システム種別	2005年		2006年			2007年			2008年		
	対象	廃止	対象	廃止	変更	対象	廃止	変更	対象	廃止	変更
教職員用電子メール	2747	662	2396	376	1348	1765	125	48	1792	101	56
メーリングリスト	175	1	214	10	192	261	4	1	302	4	0
www	585	—	554	32	447	567	17	7	521	8	14
サブドメイン	83	4	109	9	96	114	0	0	127	1	0
固定 IP アドレス	1079	42	1214	55	776	1238	31	8	1245	21	4
合計	4084	709	5009	483	2859	3945	177	64	3987	117	72

で回収していた時よりも回収率が上昇した。これにより Web を使うことによる回答回収に影響が無い、むしろ回収率が向上することが確認できた。また、利用者の回答日は電子メール送付日または翌日に集中しており、電子メールを読んでもすぐに回答の行動に移っていることがわかった。このため、未回答者へ回答を促す電子メールの再送信を早めに行うことにより、回答回収率が向上した。

3年間の運用結果を調べると、利用者確認のような調査を電子化し、未回答者へ再度依頼をすることにより回答回収率を向上させることができたが、毎年ほぼ一定数(約2.6%)が回答を行っておらず、Webを利用してもしなくても全く回答しない人数も一定数(約1.3%)いることが分かった。今後はこの回答を行わない一定数がどのような特徴があるかを調べ、対策を考える必要がある。

参考文献

- 1) 徐 浩源, 大山 清, 志村 俊也: *IP アドレス管理システムの開発と運用*, 学術情報処理研究集会, No.8, pp.79-82 (2004).
- 2) 井町 智彦, 車古 正樹, 松平 拓也, 西川 直樹: *ネットワーク管理業務におけるデータベース活用*, 学術情報処理研究, No.8, pp.93-98 (2004).
- 3) 奈古屋広昭, 松村芳樹, 入来院ひさ子, 鈴木令子, 鷹野三千代: *オープンソースによる統合認証系の構築と運用*, 情報処理, 第8回 DSM シンポジウム (2004).
- 4) 内藤久資, 梶田将司, 小尻智子, 平野靖, 間瀬健二: *大学における統一認証基盤としての CAS*

とその拡張, 情報処理, Vol.47 No.4, pp.1127-1135(2006).

- 5) 奥村勝, 本山聡, 三河邦夫: *福岡大学における統合認証システムの構築と運用について*, 情報処理, 分散システム/インターネット運用技術研究会報告, Vol.2006 No.38(2006).
- 6) 江藤博文, 渡辺健次, 只木進一, 渡辺義明: *大学における情報基盤整備の中核となる統合認証システム*, DSM シンポジウム 2002(2002).
- 7) 広島大学全学電子認証システム, 広 大 フォーラム 2003 年 8 月号 (No.377), <http://home.hiroshima-u.ac.jp/forum/2003-8/>