センターサービス利用登録システムの再構築
Reconstruction of the Registration system of Center Services

岩沢和男 [1], 宮原俊行 [2], 中川 敦 [3],
岩田則和 [4], 西村浩二 [5], 吉冨健一 [6]

IWASAWA Kazuo[1], MIYAHARA Toshiyuki[2], NAKAGAWA Tsutomu[3],
IWATA Norikazu[4], NISHIMURA Kouji[5], YOSHIDOMI Ken-ichi[6]

{iwasawa[1],tmiyahar[2],nakagawattm[3],norita[4],kouji[5],domi[6]}@hiroshima-u.ac.jp

広島大学情報メディア教育研究センター
〒 739-8526 東広島市鏡山 1-4-2
Tel:082-424-6252, Fax:082-422-7043
Information Media Center, Hiroshima Univ.,
Kagamiyama 1-4-2, Higashi-Hiroshima,Hiroshima 739-8526,JAPAN

概要

広島大学情報メディア教育研究センターでは、2010 年 9 月にシステム更新を完了した。新システムで再構築したセンター・サービスの利用登録システムにおいては、「誰がどの機能を使用できるか」を一元管理するため、サービスの機能単位とユーザーグループで構成するサービス管理表を導入した。これにより、サービス利用条件を可視化でき、且つ、利用条件の変更も容易になった。

事務方とのデータ連携においては、教職員、学生および学外者の ID について、LDAP で連携している。何回か起きた大規模な ID 消失等のトラブルに対して、実害を極力抑制できる仕掛けを構築した。

キーワード

サービス管理, ユーザー管理, トラブル回避

1 はじめに

広島大学情報メディア教育研究センター (以下、センター) では、2010 年 9 月にシステム更新を完了した。2000 年度、2005 年度および 2010 年度という都合三回 (約 11 年間) の全システム更新を経て、センターのサービスは多様化し、提供形態も複雑化してきた。その間、システムトラブルや誤操作等による一括削除等が、何度も発生した。センターのとるべき防御的措置について、その都度、貴重な経験を積んで来た事になる。

今回、再構築したセンター・サービスの利用登録システムにおいては、複雑化し多様化するサービスに関して、「誰がどの機能を使用できるか」を一元的に管理するため、サービスの機能単位とユーザーグループで構成する「サービス管理表」を導入した。これにより、サービス利用条件を可視化でき、且つ、利用条件の変更も容易になった。

また、事務方とのデータ連携に際しては、これまでの大規模な ID 消失等のトラブルを教訓に、トラブルが発生した際の実害を (皆無ではないまでも) 極力抑制する仕掛けを構築した。

本センターの実践とその教訓が、多様で複雑なサービスを提供されている他大学情報センターの参考になれば幸いである。この論文では、第 2 章でセンターを取り巻く情報環境の変遷を概観し、利用登録システム再編への必然性を示す。第 3 章でセンターサービスの概要と、

表- 1: 現在のアカウント体系

種別	期限	用途
個人	ID*	各人がメール等のサービスを利用
グループ	ID*	グループでのホームページ公開等
クラス	あり	講習会の講師、受講生等が利用
ゲスト	あり	来学者が情報コンセントを利用

ID*:期限はないが ID が離籍になると無効化

利用登録システムに実装したサービス管理機能について説明する。第 4 章では、センターと事務方とのデータ連携、防御的措置、及びトラブル再発防止に向けた対応の例を説明し、第 5 章で今後の課題を整理する。

尚、セキュリティ等に配慮し、データ連携やトラブルの詳細、事務担当名称等の記述は、必要最小限に留めさせていただく。

2 センター情報環境の変遷

2.1 アカウントおよび ID 管理の変遷

2000 年度のシステム更新時には、それまで各システム個別に発行していたアカウント群に対して、「情報システム利用には、個人の責任を明確化させる」という基本方針で、新しいアカウント体系を導入した [1, 2]。その後、ネットワーク認証用のゲストアカウントを追加して、現在のアカウント体系としている (表-1 参照)。これまでの運用で、アカウント種別については、現状の体系で十分であると判断している。尚、2000 年当時、センターは非構成員情報を独自に管理していた。即ち、学外者へのアカウント発行は、その ID 作成も含めて、センターで勝手に実施していた。

2005 年度に導入したシステムから、センターがサービス対象とする個人の情報は、全学で統一的に ID 管理する事務方の LDAP サーバーから、利用登録システムに日々取り込むようになっている。その際、教職員・学生はもちろん、学外者の登録および ID 管理も、全学レベルで事務方が担当することとなった。そのため、センターで独自に ID を発行する必要はなくなった。

2007 年度には、アカウントに年度更新制を導入するため、センター利用登録システムに対してのみ、改修を行った。これについては、2.3.1 節に記す。

2010 年度のセンターシステム更新においては、サービスの利用主体を、アカウントから ID に変更することとなった。実際、2005 年度のシステムは、LDAP 連携してはいても、サービスの中心は、個人アカウントであった。即ち「個人アカウントを持つ常勤職員は○○ができる」というのが、サービスを提供する際の考え方であった。しかしながら、全学レベルで LDAP 連携してきたことで、様々な個人の属性情報が LDAP 上に登録されてきた結果、「個人アカウントもセンターが提供するサービスの一つに過ぎず、過度な依存はやめるべき」という考え方が生まれてきた。そこで、サービスを「アカウントに紐付くもの」から「ID に紐付くもの」に方針を転換した。「常勤職員の ID では○○ができる」「○○の管理者はこの ID である」等が、その場合の例になる。

2.2 職種・職名等のコード体系

センターでは「常勤職員がサービス利用の責任を担うべき」と考えている。単純に言えば「常勤職員には提供するが、そうでない者には提供しない」というサービスが、多々ある。つまり「常勤職員」に相当する方がどんな職種・職名で存在するのか、正しく把握しておかなければ、サービスを適切に運用できないことになる。

2.2.1 フルタイム、パートタイム

大学運営業務の実務を担う方々には、非常勤職員の方も数多い。表-2 に、広島大学における職種・職名と常勤・非常勤の区分の例を挙げる。非常勤職員の中には、ほぼフルタイムで働く「パートタイム契約職員」という職種の方がおられる。表-2 に示した、特任教授や特任准教授、契約一般職員の方々がそれにあたる。仮に、この方々の権限を低く設定すると、実務担当者がセンター・サービスを利用できず、非常に多くの問題を引き起こす。例えば、他の常勤職員の ID やパスワードを借用して、センターサービスの利用手続きを行わざるを得ない等。

一方、ティーチングアシスタント (TA)、リサーチアシスタント (RA) は、アルバイトの位置づけであり、権限も責任も非常に小さいものと考えなければならない。

それ故、常勤・非常勤などの名称のみで判断すると、実務上の重要性を見誤ることになる。

今回のシステム更新で、これらの区分の扱いを、センター側で自由に制御できるようにした。

2.2.2 職種・職名の更新頻度

加えて、広島大学においては、非常勤職員の職種・職名等は、かなり頻繁に (ほぼ毎月) 更新される。2005 年度に開発・運用した前利用登録システムにおいては、職名等の人事系コードの更新時には、随時、利用登録システムのマスターを更新する必要があった。取り込みが遅れると、該当するユーザーの情報がエラーで読み込めず、「その人が存在しない」扱いになっていた。つま

表- 2: 職種・職名の例

職種の例	職名の例	区分
大学教員	教授, 准教授	常勤
一般職員	主査, 主任	常勤
パートタイム契約職員	特任教授・准教授	非常勤
パートタイム契約職員	契約一般職員	非常勤
パート職員	TA,RA	非常勤

表- 3: ユーザーが選択するサービス

利用サービス選択の対象
メール, ホームページ, Login サービス, センター端末, HPC, VPN 接続, フレッツ接続

り、前の利用登録システムは、上流工程の異動に追随してメンテナンスする必要があった。

今回のシステム更新で、この点にも対策を施した。

ID についてデータ連携を充実させて置きながら、メンテナンスは手動という中途半端なシステムであったのは、センターがコード体系と実務の関係を充分に理解していなかったためと、今ならば言える。

2.3 セキュリティ対策

2.3.1 遊休アカウント排除等

利便性向上のため、2005 年度に、学内の認証統合 (ID 用パスワード＝個人アカウント用パスワード) が実施された。その後、セキュリティー向上のために、遊休アカウントをロックするべく、2007 年度末から、全アカウントに年度更新制を導入することとなった [3]。その際、「不要サービスは『利用しない』を各ユーザーが選択」できる様に、利用登録システムを改修した (表-3 参照)。

2010 年度からは、更に、セキュリティホール等が放置されやすい学内各部局のサーバー群の巻き取りを意図して、新たにホスティング・サービスを開始することとなった。また、前システムまで別サーバーで運用していたメーリングリストの管理も、今期から利用登録システムに統合された。

こうして、サービスを統合するたびに、利用登録システムの管理機能が追加され、徐々に複雑化していくこととなる。

2.3.2 ID の大量消失事故

一方、大規模なトラブルも度々起きる。

大学においては、学生の卒業・入学、教職員の退職・新規採用等により、大量の離籍・登録が、定期的に起きる。各学生の卒業予定日は不確実であり、教職員の任期制は部分的であり再任もされる。それ故、在籍期限という情報は、あまり一般的ではない。むしろ、学籍データや認証システムとの関係から、「離籍した者の ID は不要」という考え方が、本学の事務方にはある。その結果、「ID の一括削除」という処理が、正常な処理として、センター上流の ID 管理システム上で、定期的に実施される。

従って、センターは、大量の ID が削除されたデータに対しても「正常の状態」として、サービスの利用停止やアカウント削除猶予の通知等、離籍に関連する一連の処理を、実施しなければならない。

その際、上流工程で操作ミスやシステムトラブル等が起きていると (実際に頻発していたが)、まるで天災の如く、被害がセンターユーザー側に発生する。ユーザーからしてみれば、「自分は大学に在籍し続けるのに、なぜ離籍の扱いを受けねばならないのか」と、大量の質問・クレームがメールや電話で、センターに、届く。

実際、数千人規模の教職員 ID の誤削除が、3 年の間隔を経て発生したこともある。「常勤職員が全員離籍、職員は非常勤のみ在籍」という事故もあった。恐らく、人事異動により、それまで特定個人が対応していた危険な処理を、不慣れな新人が作業して発生させたものと、センターでは推測している。

離籍処理を削除ではなく「離籍した日付を記入する処理にしてほしい」と、センターから事務方に要望したが、他システムとの関係もあり、その方法は未だ採用されていない。

暫定措置として、利用登録システム側に「削除された人数が特定の値以上であれば、異常と見なす」という予防的措置を施した場合もあったが、微妙にその数値に届かないケースも起きた。「件数で保険」をかけても無駄である。

今回のシステム更新後の 2011 年 5 月にも、数百件の教職員 ID が離籍になるトラブルが起きた。ただし、今回は、システム更新時に導入した防御的措置のため、復旧に若干の作業は要したが、実害はなく、対処できた。防御的措置については、4.3 節に記す。

3 利用登録システムのサービス管理

3.1 利用登録システムの概要

センターは、広島大学の構成員約 2 万人のユーザーに対して、アカウント、メール、メーリングリスト、ホスティング、HPC 等、数多くのサービスを提供している [4]。そのサービスを管理する利用登録システムは、Web

表- 4: 常勤教職員が利用できる機能

機能
利用サービス選択 (表-3)
使用領域確認
アカウント自主ロック・ロック解除
ML 登録・管理
クラス/ゲスト/グループアカウント登録
ホスティング管理
DB 管理
メール振分・転送設定
メールアドレス変更
メールアドレス引継ぎ
WWW 公開認定試験

ベースの一般利用者機能、センタースタッフが使用する管理者機能、システム管理者機能、および、バッチによる自動処理で、稼働している。

既に 2 章で述べたように、基本となる構成員情報は、事務方が管理する「広島大学統一 ID 管理システム」から、入手している。統一 ID 管理システムでは、教職員、学生、学外者の ID 情報および、所属・職種・職名コードなどの各種データが、統合的に管理されている。

センターで提供するサービスは、システム更新の度に、徐々に増加し続けている。各サービスの利用条件も、複雑化しており、運用を続けるにつれ、その条件の見直しが必要となることもある。

3.2 利用登録システムの基本機能

利用登録システムは、一般のユーザーがログインした場合、アカウントの有無、身分および属性により、表示する情報を選択し、どの機能ボタンを提供するかを管理している。

例えば、常勤職員が個人アカウントでログインした場合、表-4 の機能が使用できる。

学生であれば、グループアカウント、クラスアカウント、ゲストアカウントは作成できない。学外者であれば、ICE 端末を使用できない等、各種の機能制限を、実施している。これは、利便性とセキュリティのバランスを考慮した選択である。

3.3 誰にどのサービスを提供するか

さて「誰にどのサービスを提供するか」は、どのようにして制御するべきか。

例えば名誉教授は、学外者であり、来学されることは少ないが、ネットワーク経由でセンターシステム等を利用されることが多い。留学直前の「日本語研修生」もまた学外者ではあるが、既に来学して日本語を研修中であり、センター端末の必要性は高いと思われる。従って「学外者」という「身分」の情報のみでは、センターがサービス提供を判断するには不十分である。ユーザー毎にサービスの必要性を考慮し、且つ、不要なサービスは提供しないために、「誰にどのサービスを提供するか」を、柔軟に管理できる工夫が必要である。

「誰に」に相当する部分を指定するにあたって、これまでのセンターサービスの利用条件を整理したところ、身分 (職員、学生、学外者) と職種で分類できることがわかった。表-2 に示したような職名 (職種の下の階層) までは不要であった。学外者に対しても「職種」に相当するコードが作成され、管理されている。従って、すべての身分に対して「職種コード」を判断の基準に使用できる。

ところで、運用方針が変更を求められることもある。実際、ML を登録できる者について、前システムでは「個人アカウントを持つ常勤教職員または大学院生」であったが、現システムでは「個人アカウントを持つ常勤教職員」のみと変更することとなった。

前回までのシステムでは、これらの「条件」をプログラムのチェック機能として実装していた。判定に「個人アカウントを持つ常勤職員」等のロジックが入り、同様なチェックが、システム内に多数ばらまかれていた。この方法では、「誰に」の判定部分は、柔軟性に欠け、メンテナンスも難しい。つまり、前システムの方法は、単純な場合では問題なくても、「誰にどんなサービスを提供するか」の詳細度を上げようとすると、いずれ破たんする実装方法であったと言える。

3.4 サービス管理表

上記の問題意識の基づいた対策として、今回の利用登録システムに導入した「サービス管理表」を図-1 に示す。一般利用者が何をできるかを定義したもので、行が機能群を表し、列がユーザーグループを表している。

利用登録システムは、ログインしたユーザーが、どのユーザーグループに属しているかを判定し、どの機能が利用可能かを調べて、対応する「ボタン」をユーザーの Web ページに表示する。

利用可能なサービスには、デフォルトが ON と OFF の区分を用意した。セキュリティリスクの高いものはデフォルト OFF であり、利用開始にはユーザー自身で「利用する」の選択が必要である。

一方、利用開始時に、簡単な試験に合格する必要のあるサービスを設けた。Web ページを作成して学外に開示したい者は、センターが「WWW 公開認定試験」と呼ぶ簡単な試験に、合格しなければならない。

ユーザーグループ / 機能群	個人アカウントなし							個人アカウントあり								その他		
	職員		学生		学外者			職員		学生				学外者				
	常勤等*	パート	正規生*	非正規生	端末利用可*	端末利用不可	無効*	常勤等*	パート	学部生*	大学院生*	専攻科生*	非正規生	端末利用可*	端末利用不可	グループ	クラス	ゲスト
個人アカウント登録申請					○	○												
個人アカウント登録	○	○			○	○												
個人アカウント引継ぎ	○	○			○	○												
アカウント年度更新								○	○	○	○	○	○	○	○	○		
アカウント自主ロック・解除								○	○	○	○	○	○	○	○	○	○	○
グループアカウント管理								○										
クラス・ゲストアカウント管理								○										
メール								○	○	○	○	○	○	○	○	○	○	
メール引継ぎ								○	○	○	○	○	○	○	○	○		
センターメール利用								△	△	△	△	△	△	△	△	△	△	
www公開利用								△	△	△	△	△	△	△	△	△	△	
loginサーバ利用								▲	▲	▲	▲	▲	▲	▲	▲	▲	▲	
ICE(教育用端末)利用								○	○	○	○	○	○	○			○	
HPC利用								▲	▲	▲	▲	▲	▲	▲	▲		▲	
DB利用サービス								○	○	○	○	○	○			○	○	
メーリングリスト登録								○										
メーリングリスト運用								○	○	○	○	○	○	○	○			
セキュリティ試験										○	○	○	○					

○：Default ON(利用する)
▲：Default OFF(利用しない)
△：認定試験合格後、認可属性を与える
空白：利用不可等

図- 1: サービス管理表 (抜粋)。「*」は対応するユーザーグループ定義画面へのリンクを表す。

運用ルールを変更する場合は、利用登録システムのシステム管理者 Web ページで、サービス管理表の情報を更新できる。一般利用者画面は、その更新結果に応じて、自動的にサービス提供内容を変更する。更新されたサービス管理表は、スタッフ用管理者 Web ページで表示でき、センターのスタッフは常に現状を確認できる。

3.5 詳細機能のグループ化

サービスをユーザーに提供するにあたっては、詳細機能レベルで、ユーザーグループ毎に定義することも、一応は可能であろう。だが、例えば、ML を作成する者は、ML を更新・削除できるべきである。つまり「作成・更新・削除」は、詳細機能としては 3 つでも、一組で考えるのが妥当である。これらは一般に「ロール」と呼ばれている。利用登録システムの Web ページにおいて「○○の管理」としてボタンで表示している機能が、これに相当する。

一群の機能を、選択的に特定グループに提供できると、センター管理者にとって便利であり、運用ルールも説明しやすい。「ログインしてみて、ボタンが表示されていれば、その機能は使えます。」というのが最も簡単な説明である。

表- 5: 現在のユーザーグループの分類

身分	グループ		位置づけ
職員	常勤等 パート		デフォルト
学生	正規生	学部生 大学院生 専攻科生	
	非正規生		デフォルト
学外者	端末利用可 端末利用不可 無効		デフォルト

3.6 ユーザーのグループ化

身分に対応するユーザーグループを、表-5 に示す。

3.6.1 個人アカウントを持たないユーザ

個人アカウントを持たないユーザは、基本的に、アカウント登録ができるだけである。学生の個人アカウントは、センター管理者が一括生成させるため、学生の機能としては、使用不能にしている。また、学外者は、アカ

ウント登録の前に、アカウント登録申請が必要であり、許可を得たものがアカウント登録を実施できる。一部の者を除き、一般に学外者には、センター端末を利用させない設定としている。

「無効」と呼ぶユーザーグループは、個人アカウントを持たず、利用登録システム上は、何もできないユーザーである。このグループには、「臨時カード」と呼ぶ認証のみに使用する IC カード用のダミー ID や、「入退室管理が必要だがアカウントは不要な出入り業者」などが、登録してある。様々な ID が登録される様になった結果、全ての ID をサービス対象とする訳には行かなくなっているのも事実である。

3.6.2 ユーザーグループのデフォルト設定

センターに個人アカウントを持つ常勤職員が、利用できるサービスの種類が多い。もっともサービスを利用できないのは、先に述べた「臨時カード用 ID」である。

図-1 および表-5 に示したユーザーグループの名称は、センターが作った勝手な呼称である。2.2 節で述べたように、大学が管理する構成員の種別・名称が、センター業務に直接使用しにくい。例えば、職員を分類するユーザーグループとして「常勤等」とそれ以外にあたる「パート」の 2 種類を作成した。

「常勤等」のユーザーグループに属する者は、「身分が職員」で且つ「職種を明示的に定義」してある。先の述べたように「パートタイム契約職員」という職種は、非常勤ではあるが「常勤等」に登録している。それ以外の職種をもつ「職員」は、デフォルトグループである「パート」として分類する。新規の職種が追加された場合には、例え大学運営上常勤であってもセンターシステムは「パート」として扱う。これは、必要に応じて手動で対応することを意味するが、頻度的に、非常に少ないことが予想される。

これまでの職種・職名コードの改定から、通常でいう常勤職員および正規生は、改定されたことはほとんどない。従って、常勤職員相当のグループあるいは、正規生のグループを明示的に指定しておけば、職員のデフォルト、また、学生のデフォルトは「それ以外」で済ませられる。身分毎にデフォルトのユーザーグループを定義することで、職種・職名コードのメンテナンスの手間を大幅に削減できた。

学外者についても、同様の考え方を適用した。即ち、変化しないものを明示的に指定し、それ以外をデフォルトとする。学外者にはセンター端末（ICE 端末）を利用させない、がデフォルトである。端末利用可とするグループと、何もさせないグループを、例外として明示的に指定した。

尚、今年 3 月までは、学生では大学院生のみに ML の管理権限を与えていたため、学生を 4 つのユーザーグループに分けていた。ルール変更で、大学院生を特別扱いする必要がなくなったので、学生のユーザーグループは、正規生、非正規性の 2 つでも十分ではある。

システム管理者機能により、サービス管理表でのユーザーグループは、適宜、分類を追加できる。

3.7 サービス管理機能の弱点

現システム稼働後の運用から、サービス管理表がルール変更および現状把握にきわめて有効であることは、確認できた。だが、以下の状況では、管理上の問題が発生し易いことも分った。

アカウント引継ぎ 身分等が変わってアカウント所有者の ID が変更された場合に、これまでのアカウント資産を引き継ぐこと。システム的には、アカウント所有者の ID を書き換えることで実現する。

職員から学外者、学生から職員等、身分変更を伴う場合が多いため、利用可能なサービスが異なり、その結果、使えるべき機能が使えなくなる、使えない筈が使えてしまう等の問題が顕在化した。

サービス条件変更 運用ルール変更により、これまで提供していたサービスを使用不能にする、またはその逆。

その結果、管理表では使えない筈の機能を、利用可能な ID・アカウントが発生する。

つまり「サービス管理表」に従えば、利用できない筈のサービスを、アカウントあるいは ID が使用するケースが、発生しえる。その場合、チェック機能不足 (バグ) の場合もあり得るが、ルール変更による「置き去り」の場合もある。尚、管理者機能として、必要な機能が不足する場合、対応に時間を要することになる。

システムの自動的な監視機能 (夜間バッチ等でのチェック) として、サービス管理表からのずれを監視し、管理者に通知する機能は実装済みである。見つかった異常には、個別に対処する必要がある。

4 ID 消失事故への予防的措置

上流工程での ID 管理にトラブルが起きると、センターの利用登録システムには、誤った構成員情報 (ID の大量消失等) が届けられる。受け取ったデータが正常・異常のいずれにしろ、センターの利用登録システムは、消失した ID に対して離籍の処理を行う。

4.1 通常の離籍処理

離籍になったIDがセンターサービスを利用していた場合、離籍処理が走る。即ち、各アカウント所有者宛に「アカウント削除猶予」のメールを発送する。センターでは、IDが離籍になっても、例えば、個人アカウントは90日間削除を猶予する運用を行っている (表-6の「変更前」を参照)。かつて、医学部で卒業後3か月程度してから改めて在籍する研修生が多数いたため、この削除猶予期間を設けた運用としている。

卒業後あるいは離籍後に再度、在籍になった場合を「再在籍」と呼ぶ。この場合「削除猶予解除」のメールを当該アカウント宛てに送信する。

再在籍にならず削除猶予を過ぎたアカウントは、一定期間ロック (利用停止) したのち、削除する。

IDに期限はあっても、個人アカウントおよびグループアカウントには、元々、有効期限はない (表-1の注参照)。所有者のIDが離籍になると個人アカウントに「有効期限＝当日、削除猶予期限＝90日後、利用停止期限＝120日後」を指定し、削除猶予メールを送付する。所有者のIDが再在籍になると、個人アカウントが存在する間であれば、再在籍処理が走り、各期限を無効にして、アカウントを再度有効にしている。

従って、アカウント削除事故と復旧措置が上流で起きた場合、削除猶予および削除猶予解除メールが飛びはするが、個人アカウントおよびグループアカウントは、ファイルを一つも失うことなく、自動的に復旧できる。ここまでは度重なるトラブルを経て、前システムで既に実現していた。

一方、クラスアカウントおよびゲストアカウントは、予め、有効期限を指定したアカウントであり、期日が来たら直ちに削除していた。IDの削除事故が起きた場合、これら期限付きアカウントの扱いが、センターにとっての問題となっていた。

4.2 期限付きアカウントの削除猶予

クラス・ゲストアカウントは期限付きアカウントである。その所有者がアカウントの期限前に離籍した場合、当該アカウントは無効とするのがセンターの方針である。

前システムでは、事故である可能性を考慮して、削除猶予ののち (ロックはせずに) 削除してていた。問題は、ID削除事故からの復旧措置で発生していた。

センターの利用登録システムでは、現システムも前システムも、アカウントの有効期限について日付情報は1つしか用意していない。個人・グループでは、通常、NULLであり、クラス・ゲストでは、申請時に指定した有効期限がセットされている。

表- 6: 離籍時のアカウント運用方針の変更

誤ったID削除を想定し、期限付きアカウントの運用方針を「削除猶予」から「利用停止」に変更した。

種別	変更前		変更後	
	猶予日数	停止日数	猶予日数	停止日数
個人	90	30	90	30
グループ	30	30	30	30
クラス	10	0	0	10
ゲスト	10	0	0	10

前システムでは、「所有者が離籍した日をアカウントの有効期限」としていたため、復旧措置による再在籍処理では、個人・グループは、NULLに戻すだけだが、クラス・ゲストは、元に戻すべき日付が残っていないことになる。

従って、IDの削除事故が起きて、クラス・ゲストアカウントの所有者が巻き込まれた場合、クラス・ゲストアカウントを正常に復帰させるために、センター管理者は以下の手順を実施していた。

- センター管理者が各アカウントの登録申請記録から、該当日付を手動で検索する。
- センター管理者が、手動で、各アカウントに有効期限を設定する。

つまりセンターは、前システムにおいては、「期限付きアカウントの有効期限」という管理情報を、自ら消失させていたことになる。

4.3 期限付きアカウントのロック

今回のシステム改修の際、クラス・ゲストアカウントの有効期限前に所有者が離籍となった場合、当該アカウントは直ちに「利用停止 (ロック)」とすることとした。以下の理由による。

- ID削除事故であった場合の復旧措置は、ロックを解除するだけ済む。
- 「期限付きアカウントの有効期限」を失わずに、アカウントを無効化できる。

表-6に変更内容の日数部分を示す。これ以外にも、前システムで実施していた有効期限を書き換える措置も廃止した。

この場合、アカウント所有者が再在籍処理で復活すると、ロック解除で回復でき、本来の有効期限も失われない。この措置により、これまでの様な、センター管理

者が各アカウントの登録申請をかき集めて手動で再設定する必要がなくなり、復旧措置が自動化できたことになる。

ユーザーから見れば削除猶予メールが届くのは変わらず、「なんで私が離籍なの」というクレーム対応するスタッフの苦労も変わらないが、事故からの復旧が自動化できたことは、センター管理者にとっては、非常に大きなメリットである。ただ、復旧措置が済むまで講習会等での利用に影響が出ることは、覚悟しておかなければならない。

上流工程で事故があっても、「情報を失わない」仕掛けを用意しておけば、ユーザーおよびセンターにとっての実害は最小限に抑えられる、という当然の結論ではある。一般のユーザーにしてみれば、ばたばたした印象を与えているであろうが、実害は極力抑えることができる様になった。

4.4 システムの妥当な振る舞い

因みに、前システムにおいて「削除猶予猶予」を設定したことがある。度々ID の誤削除が起きたことに対応ため、「ID が消えても間違いかもしれので、削除猶予メールの発送を数日間遅らせる」という運用を取ったことがある。その結果は、逆に、正常時に「離籍した ID が所有するアカウントが、直ちに削除猶予にならないのはシステムの異常か？」という疑問を、抱かせることとなった。つまり、削除猶予猶予は忘れられ易く、防衛線として機能するより「自作のトラップ」という位置づけに近くなる。

複雑なシステムには「もぐりの定数」を組み込むべきではない。システムが担う論理に照らして妥当な挙動を維持させることが、当然のことながら、極めて重要である。

4.5 誤操作手順の原因究明と対策の提案

何度も起きる ID の誤削除について、非難することなく、原因を調査した。場合ごとに、トリガーとなる行為が異なっており、優れた教訓を得るのは容易ではない。

その中で、「非常勤職員の ID とパスワードを保存し、書き戻す際に、追加ではなく上書きしてしまい、既存構成員の ID を消去した」というケースがあった。

その行為の理由は、広島大学と一部の非常勤職員との契約で、年度の切り替わり時に数日間契約が切れる場合がある。その結果、ID 管理システム上から ID とパスワードが削除されてしまう。後日、契約完了した場合に、各人は同じ ID で再度登録されるが、パスワード情報がクリアされている。そこで「それらの ID とパスワードを保全し、パスワードの再登録作業を不要とする」ための行為であることが分かった。

この善意に基づく行為は、システム化されておらず、従って、手動で実施する作業として、事務方の現場対応として、行われていた。

センターによる聞き取り調査の結果、統一 ID 管理システムの改修時期でもあり、問題となる作業を、統一 ID 管理システムでのパスワードバックアップ・リストア機能として、実現することを提案し、実装された。これにより、「現場の隠れた作業」をシステムの機能として実現することで、云わば「善意のテロ行為」を排除することができた。

もちろんこれは、単なる例に過ぎず、一般化できるものではない。本来のセンター業務からも踏み出している。だが、上流工程のワークフローに無関心なままでは、結局、センターは事故の被害を垂れ流すしかない。

センターは、ID および各種コードを事務方から受け取り、センターのユーザーにサービスを提供する。既に、身分・職種・職名等のコード体系を適切に理解するには、大学内での現場を把握する必要があることを学んだ。同様に、上流工程での ID 管理等のワークフローについても、ある程度までは把握するべきであり、助言していくべきである、と考えている。

5 まとめと今後の課題

5.1 現システムで実現したこと

センターシステムを更新し、利用登録システムを抜本的に改修した。どのユーザーグループがどのサービスを利用できるかを管理する「サービス管理表」で、利用登録システムが提供する機能 (ボタン群の表示) を、直接、制御している。これにより、誰がどのサービスを利用できるかの把握が容易になり、同時に、ルール変更に伴う条件の変更が、容易になった。

尚、サービス条件を変更した場合、期間を区切った移行措置を実施する必要がある。運用ルール変更が、時に、システムの機能不足 (おもに管理者側) を露呈させる場合もあるので、注意が必要である。

また、度々発生した ID の大量削除というトラブルに対しては、アカウントの猶予期間、利用停止期間を活用して、管理情報を含めて、データの消失を防ぎ、実害が出ないように配慮している。削除猶予メールおよび削除猶予解除メールが大量に飛び、センターに苦情・質問が来る事態に変わりはないが、正常な状態に復帰させるのは、以前よりはるかに容易になった。

5.2 今後の検討課題

かつて、センターの個人アカウントには「サービスを利用する権利」に相当する位置づけがあった。だが、IDで個人を管理する体制が大学として整い、センターがIDに基づきサービスを提供する状況においては、「IDが主たる個人情報」であり、「アカウントはセンターのサービスの一部」に過ぎない。

現状は、センターにとって利用者の権利等の関連付けが、まだアカウント主体のものがあるかもしれない。今後は「サービス利用者の連絡先」程度に扱う必要があるだろう。

ところで、「IDは離籍により失効する」「IDに引き継ぎはない」とするのは、事務方のポリシーである。一方、「アカウントの削除には猶予を設ける」「アカウントは引き継げる」とするのはセンターのポリシーである。これまで、ID失効後も猶予のある(つまり認証可能な)アカウントに各種サービスを紐づけていた。従って、そのアカウントを引き継いでしまえば、すべてのサービスを一括して引き継げていた。IDにサービスを紐づける場合、その「一括引継ぎ機能が消失」しつつある可能性がある。各種サービス停止までの猶予も失われる。今後、この点について、考え方を整理する必要があるだろう。

参考文献

[1] 岩沢和男, 津久間秀彦, 新畑道江, 岸場清悟, 入江治行, 稲垣知宏, 隅谷孝洋, 秋元志美, 勇木義則「大学情報サービス基盤としてのアカウント体系」, 学術情報処理研究 No 4, pp.63-72, 2000.

[2] 岩沢和男, 津久間秀彦, 岸場清悟, 隅谷孝洋,「アカウント体系再編の評価」、学術情報処理研究 No 5, pp.43-48, 2001.

[3] 岩沢和男, 吉冨健一, 宮原俊行,「セキュリティ強化のためのアカウントへの制限」, 平成 20 年度 情報教育研究集会、基盤システム,p491-494,2008.

[4] 広島大学情報メディア教育研究センター Web ページ, http://www.media.hiroshima-u.ac.jp/services