メインフレーム／オープンシステムサーバ間でのアカウント一元管理
―システムＩＤと個人同定情報との結びつけ―

○ 廣瀬 康行[1)]　稲嶺 盛彦[2)]　野原 広[2)]　伊良波 朝賞
琉球大学 医学部附属病院 医療情報部[1)]
NEC ソフトウエア沖縄[2)]

Account Management between Mainframe and Open System Servers
- Practical Binding of System ID and Personal ID with his/her “role” -

Yasuyuki Hirose[1)]　Morihiko Inamine[2)]　Hiroshi Nohara[2)]　Chosho Iraha
Medical Informatics, Ryukyus University Hospital[1)]　(hirose@hosp.u-ryukyu.ac.jp)
NEC Software Okinawa[2)]

Abstract: We have improved the account management system between mainframe and open sysytem servers in the hospital information system in order to minimize its cost. We clearly separated the “internal” staff identifier for the system(SID) and the personal identifier of the real world(PID), and we also prepared “external” staff identifier for the system(CID). A pair of PID and CID is controlled to be unique, and this pair is able to have some “roles” according to staff’s role in the hospital. Then, each PID/CID pair with its “role” is bound on SID. These mechanism satisfy both the representation of the real world and the necessity of uniqueness of SID in natural way. Conquecently, the account file becomes to provide enough information (i) for the access control and the resource management in a hospital information system and (ii) for the system generation of account files for the open sysytem servers.

Keywords: account management, host and open system server, system identifier, real world identifier, role

---

1 緒言

日本の大規模病院情報システムでは，いまだにその中核にメインフレーム（MF）をおく施設が多い．MF では処理レスポンスの向上や・巨大な実稼働環境と COBOL の言語仕様に起因して，種々のレコード構造やファイル関係は柔軟性を欠き，現実世界のモデル化からはほど遠い状態となっている．よって臨床研究や経営分析のデータベースとしては不適であり，参照系サーバ（UNIX，NT など）に DataWareHouse（DWH）等を設ける傾向にある．

しかしこれにより，アカウント管理に費やす人的時間的コストの急激な増大が問題となる．また個別管理ではアクセス権の統括が難しく，思わぬセキュリティホールを生じせしめる危険性がある．

これらのリスクを回避するには，診療情報システムに関わる MF／サーバ間でのアカウントの一元管理，しかも（半）自動的な一元管理が必要となる．しかし単に MF からサーバへと情報を配信するだけでは充分ではない．というのも，診療スタッフは様々な立場や役割のもとに診療業務を遂行するが，これまでの職員マスタレコード構造は，それらを充分に反映できてはいなかったからである．

よって個人識別子（PID）とシステムハンドリングの対象となるＩＤ（SID）との分離，PID と SID との再連結と ROLE（資格や所属や立場）管理の工夫と改善が必要となった．この過程は処理指向のパラダイムでは為しえず，現実世界のモデリングが不可欠である．

この様なモデリングの反映はセキュリティ管理や病院経営の分析にも，極めて重要である．

我々は現行システムへの影響を最小に抑え，現有の情報を有効活用し，管理作業量を軽減する手法を考案したので，これを概説する．

2 手法

2.1 現状分析

琉球大学医学部附属病院では NEC 社製の IBARS と ORDERING を用いている．この職員マスタとその運用は，以下の意図をもって設計されたと思われる：

- CID（磁気カード番号：非公開）と操作者番号（通常の account に相当）の分離による認証能の向上
- SID（病院番号＋CID＋操作者番号＋通番）によるシステム内部での一意性の確保
- 操作者番号の任意性による使い勝手の向上
- 「氏名＋性別＋生年月日」による個人の特定

しかし次のような設計もしくは運用上の問題点が

あった：

1) システムは内的識別子と外的識別子とを持たずかつ一つのレコードは唯一の ROLE のみ保有
   SID と PID との関連や連結管理には無頓着
2) SID と個人識別子は分離されず結果的に同一視
   同一人物が複数の SID を持つことがある
   同一人物が複数の CID を持つことがある
3) 真の個人識別子がない(性別や生年月日は未入力かつ職員番号等のフィールドがない)
   同姓同名や結婚後等の氏姓変更は判別不能
4) システム運用の都合で「無名」の職員レコードが存在する（例：内科医師）
5) 操作者番号（通常の account に相当）の重複

これらはいづれも同定性【唯一性と一貫性，遡及性と追跡性】を損なう要因となっている．

2.2 目標

1) システムからの要求である ID の唯一性と，現実世界からの要求である同一人物の多様な ROLE の反映とを，同時に満たすこと．
2) 個人の同定に関して，明示的な一貫性，遡及性や追跡性を確保すること．
3) 時間的金銭的コストに関し現実的な措置のこと．

2.3 戦略と構造設計

レコード構造とその意義は以下の通り：

1) 予備領域に「個人識別番号区分フラグ」「個人識別番号」と「部署主副判別フラグ」を追加
   PID＝個人識別番号区分フラグ＋個人識別番号
   生年月日等は個人特定の補足情報とする[1]
2) PID と CID との組（ペア）の唯一性の確保
   この組が現実世界とシステム世界との界面
   CID の重複は該当レコード間の chain にて整理
3) 「PID と CID との組」に複数の ROLE を付与
   ROLE の多元管理から一元管理へ
   フラグによる優先度の判別（ただし静的）

これらにより一つの PID すなわち「PID/CID 組」は，現実世界に即した多様な ROLE を保持する．その組は CID を介して SID と連結されるが，SID の唯一性は ROLE 情報を反映した操作者番号によって確保される．見かけ上は複数レコード（＝複数 SID）による管理だが，意味的には統一的かつ明示的な管理であり（＝PID/CID 組の唯一性），改造に伴うインパクトも極めて小さく現実的である．

なおシステムにとっては CID を外的識別子あるいは結合子，SID を内的識別子と捉えることもできよう．

2.4 整理と準備

- 運用ルールの改善（無名性の可及的排除）
- 職員マスタに補助ファイルを追加；PID/CID 組
- 職員マスタ操作用の JOB/JCL の改造
- サーバ側プログラム（perl 等）の作成
- 過去約 15 年間の追跡調査そのほか

2.5 運用

1) サーバへの配信の際には，職員マスタが保持する情報を根拠にして，可及的にプログラムにて整形補足する（＝充分ではないにしても）．
   MF／サーバ間における一元管理
2) DWH では，唯一の「PID と CID の組」すなわち唯一の PID にアカウントを発行し，その ROLE に応じたアクセス権を付与する．
3) ジョブや perl 等の起動等は半自動での対応だが，年間 300 時間以上の人件費節減と予測している．

3 結語

職員マスタは病院情報システムにおけるアクセス管理とリソース管理を実現するための根幹をなしている．今回の改善は今後のセキュリティ管理や病院経営戦略への貢献の礎となりうると期待される．なぜならリソース管理（人・物・場所・時間）の基礎情報を，柔軟かつ統一的に提供可能な構造を持つからである．

ただし動的なアクセス権の制御やリソースの管理については，この手法には限界がある．というのも，従来のレコード構造等の事情により識別子の固定点あるいは「ピボット」を CID としているため，操作者番号が SID の唯一性と ROLE の切替との両方を担っており，分離と統合が不完全だからである．

今後は「関係と状況」（Relation / Situation）[2][3]による動的管理にも対応できる設計が必要となろう．