病院情報システムの職員属性とその履歴を取得解釈して アクセス権を制御する診療情報参照システム

○廣瀬 康行[1] 柴田 学[2] 勝本 威男[3] 野原 広[4] 稲嶺 盛彦[4] 山里 泰三[4] 屋宜 勲[4]

琉球大学 医学部附属病院 医療情報部[1]
日本電気株式会社 第一システム事業本部 第二公共システム開発事業部[2]
システムリサーチ株式会社 システム部[3]
日本電気ソフトウエア沖縄株式会社 ソリューションビジネス部[4]

The medical data warehouse system that automatically controls access right according to staff roles and its histories in the HIS

Yasuyuki Hirose[1] Manabu Shibata[2] Takeo Katsumoto[3] Hiroshi Nohara[4]
Morihiko Inamine[4] Taizo Yamazato[4] Isao Yagi[4]

Medical Informatics, University of the Ryukyus Hospital[1]
NEC Corporation[2]
System Research Corporation[3]
NEC Software Okinawa Ltd[4]

Abstract: The authors have developed the medical data warehouse(DWH) system that automatically controls access right according to staff roles and its histories in the hospital information system(HIS). Each access right is also configurable finely so that this DWH system can be easily controlled to satisfy the security policy, which differs from HIS.

Keywords: data warehouse, hospital information system, role, history, access right

緒 言

病院情報システムに蓄積された各種の診療情報は，当該患者の cure と care はもとより，privacy を保護し confidentiality を維持しつつ臨床研究や経営分析にも活用できるよう，種々の努力が為されているところである．これを真に実現するためには，

A) 病院情報システムにおいては，いつ・どこで・誰が・誰の・どの情報に・なぜ（診療現場でのアクセス理由と動的な役割）・どのようにアクセスしたのか，が精確に管理記録され，アクセスに関する追跡性を確保せねばならず，かつ

B) 職員マスタにおいては，主所属科や副所属科（静的な役割）に関する期間と履歴を管理記録でき，その遡及性を確保する環境が必要となる [1〜3]．そのうえで

C) 診療情報の後利用参照システムでは前者の履歴情報に基づきつつも，さらにセキュリティ・ポリシーに基づいたアクセス制御やマスクを施しつつ，参照を許可しなければならない．というのも，診療業務における診療情報へのアクセス権と・研究教育業務等における診療情報へのアクセス権とは，たとえ同一職員の同一患者に対するアクセスであったとしても，通常，自ずと異なることになるからである．

筆頭発表者は，オープンシステム系病院情報システムについては，(A) と (B) のほとんどを満たすシステムを東京医科歯科大学歯学部附属病院において設計実装したが [4〜7]，(C) の段階にまでは至っていなかった．

一方，本邦においては依然として多くの汎用機系の病院情報システムが実稼動しており，さ

らにこのようなシステムの職員マスタの多くは,平板な構造しか有していない．このため，特定職員に関する所属診療科の履歴を保存できないことは言うに及ばず，複数の役割（＝副診療科）は統一的に管理されておらず，さらに，同一職員か否かの同定さえままならないことがある.

このようなシステム環境を改善して，職員の多様な役割とその履歴に応じつつ・コンフィデンシャリティを重んじ・アクセス自由度を保持し・管理コストを極小化した・診療情報参照システムの構築を設計実装するに至ったので，これを報告する.

環 境

琉球大学医学部附属病院は病院情報システム（THISUR）に日本電気社製の IBARS-T と PC-ORDERING（52PC）を ACOS PX 7500（COBOL）にて稼動している．一方，オープン系サーバとして EWS 4800（UX），EXPRESS 5800（Windows NT）を有している.前者にはperl による変換処理とOracle によるＤＢサーバを担わせ,後者はＮＥＣソフトウェア九州製の Simple Data Gateway（asp）をベースにＡＰサーバとした（https）.

設 計 戦 略

旧式な病院情報システムのため，種々の制約条件は極めて強い.よって（A）を追求することは非現実的ゆえ，これは割愛した．ただし職員マスタの構造を再設計改善し,かつ過去15年間3000 件程の職員レコードを整理して（B）の要件は完全に満たすよう改善し [8]，汎用機からオープン系サーバまで１職員あたり１アカウント１パスワードで，かつ所属科等の履歴を全てオープン系サーバへ自動的に反映できるようにした．そのうえでＡＰサーバには，以下のアクセス制御機能を有するよう設計した：

i. 職員属性とその履歴に応じてアクセス制御できること
ii. 診療業務系とは完全に独立した管理設定もできること
iii. 特定の病名やデータを必要に応じてマスクできること
iv. オンライン検索結果を端末にＣＳＶで転送できること
v. 転送も含めた全てのアクセスログを記録保存すること

成 果

ＡＰサーバのデフォルト設定では，現在の所属診療科に関わる患者情報のうち・特にマスクされていない事項のみを閲覧できるようにしている．この方針のみ適応すればよいなら，管理コストは殆ど皆無で妥当なアクセス権を自動的に付与でき，エンドユーザにはその範囲内での高いアクセス自由度を確保できることとなった.

また「診療以外の目的で診療情報を再利用する際のセキュリティ・ポリシー」に基づいて厳密にアクセス制御したい場合などには，デフォルト設定をオーバーライドするだけで実現することができるようになった.

使い勝手の快適さについては，ハイパーデモで実感してほしい.

考 察

はじめに挙げた（B），（C）の要件を満たした診療情報参照サーバを構築した．現時点では病院情報システム自体の制約から（A）を満たしていないが，これは病院情報システムの更新時に実現する予定としている.

なお高い自由度と利便性とが得られることから，セキュリティ・ポリシーを再検討・明文化した後に院内へ公開することとした.

文 献

[1] CEN. Health informatics -Electronic healthcare record communication -Part 3: Distribution rules. DD ENV 13606-3:2000, May/2000.

[2] US Government. HIPPA. 2001.

[3] 文部省, 厚生省, 通商産業省, 科学技術庁. ヒトゲノム・遺伝子解析研究に関する倫理指針（案）. 平成 12 年 12 月 20 日. http://www.mext.go.jp/b_menu/houdou/12/12/001238.htm, 2001.

[4] 廣瀬康行, 佐々木好幸, 木下淳博, 水口俊介, 竹田淳志, 大林尚人.「関係と状況」と閲覧内容ログ. 医療情報学連合大会論文集 vol.16：86-87, 1996.

[5] Yasuyuki Hirose. Access Control and System Audit Based on "Patient-Doctor Relation and Clinical Situation" Model. Medinfo '98, vol.2：1151-1155, 1998.

[6] 佐々木好幸, 水口俊介, 木下淳博, 竹田淳志, 大林尚人, 依田哲也, 廣瀬康行, 侯木志朗. 電子診療録における診療グループの構成とセキュリティについて. 医療情報学 20 (Suppl. 2)：440-441, 2000.

[7] Yasuyuki Hirose, Yoshiyuki Sasaki, Atsuhiro Kinoshita. Human Resource Assignment and Role Representation Mechanism with the "Cascading Staff-Group Authoring" and "Relation / Situation" Model. Medinfo '2001, in printing, 2001.

[8] 廣瀬康行, 稲嶺盛彦, 野原広, 伊良波朝賞. 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～. 第 18 回医療情報学連合大会論文集. p.248-249, 1988.