プライバシーを考慮した物探しシステムの実装

野澤 佳世　(指導教員：渡辺 知恵美)

1　はじめに

近年，RFID や QR コードなどの ID タグ技術の発達により，物品の配置や流通の ID タグによる管理が容易に実現できるようになってきた．我々も家庭での ID タグによる物品管理システム「物探しシステム」の開発を進めている．物探しシステムを家族で共有する場合，例えば子供には場所を教えたくない，娘と母のみで共有したいなど公開レベルの管理を行いたい場合がある．

そこで我々はデータベースシステムのアクセス制御機能を利用し，物探しシステムにおける共有レベルの制御を実現する．行・列レベルのアクセス制御を実現するため LBAC を利用し，実世界での物品管理を考慮したアクセス制御の定義を行った。

2　「物探しシステム」とアクセス制御

2.1　物探しシステム

「物探しシステム」とは，物の収納場所をコンピュータに登録し，コンピュータの画面上で物を探すことのできるシステムである．我々が想定する物探しシステムは家族や研究室など小さな集団を対象とする．また，1 つの集団に対して 1 つの物探しシステムがあり，個人の物も共有の物も全て，同じシステムで集中管理するものとする．

本稿で使用する物探しシステムにおける物品または場所の登録の大まかな流れを，図 1 に示す．ユーザは登録の際，バーコードリーダで QR コードを読み取って，しまう物としまった場所の情報を登録する．システムを使うときは，物の情報を検索すると，物の情報がユーザに表示される．

この流れに沿って実際に物の情報を登録すると，作成されるテーブルは図 2 のようになる．登録される情報は物の名前，種類，所有者と公開範囲である．

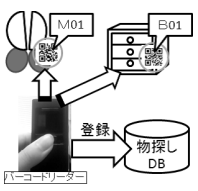

図 1: 登録の流れ

場所ID	場所
1	家
2	娘の部屋
3	娘の机

物ID	物の名前	種類	所有者
1	マグカップ	食器	A
2	グラス	食器	A
3	ボールペン	文房具	B

図 2: 登録されたテーブル

2.2　「物探しシステム」におけるプライバシ

記録された情報が全員に公開される状況である場合，物品を記録する際に，以下のことを意識して記録する必要がある．

(1) その物品があることを、自分だけではなく他人も知ることになる

(2) 検索結果によっては，他人がその物品を使用するかもしれない

(3) 隠しておきたい人のよくアクセスする所に，隠したいものがしまってある

物品のデータがリレーショナルデータベースで管理されているならば，特定のユーザに対してのみ情報を公開したいという (1) の要求は，アクセス制御機能を使えば実現できる．ただしテーブル単位のアクセス制御でなく，行レベル・列レベルの詳細な指定が必要である．

(2) に関して，物品があることは他人に知られても良いが，それを無断で使用して欲しくないときは，物品の格納場所を曖昧にし，使いたい時にその都度所有者に連絡させるようにする．

また，物品が現実世界で収納されていることに関連し，(3) の懸念が生じることがある．これに関しては，検索ログから状況を検知し，記録者に対してメッセージを出すことによって隠したものが他人に見つかることを防げる．

物探しシステムにおけるアクセス制御について考慮・実現すべきこれらの 3 項目について，次節以降詳細を述べる．

2.3　LBAC によるアクセス制御

リレーショナルデータベースシステムにおける基本的なアクセス制御では，テーブル単位でユーザへの閲覧・更新などのアクセスを制御することができる．しかし，テーブル単位のアクセス制御では物品ごとのアクセス制御が実現できない．

そこで本研究では，テーブル単位よりさらに詳細なアクセス制御を実現するために，DB2 [1]に実装されているラベルベースのアクセス制御，LBAC 機能を使う．LBAC を使用すると，アクセス制御権を個々の行および個々の列ごとに決定することができる．ユーザがデータにアクセスするときは，自分の持っているラベルとテーブルについている同じ種類のラベルを照らし合わせ，アクセスの可否を判断する．

LBAC の詳しい説明は図 3 で表す．各個人が所有する A・B・C というラベルがあり，この 3 つは並列の関係である．ある行にアクセスした際に，自分の持っているラベルと行に付いているラベルとを照らし合わせ，一致した場合のみその行にアクセス可能となる．図 3 の場合にラベル同士を比較していくと，各個人に表示される情報は吹き出しの中のようになる．

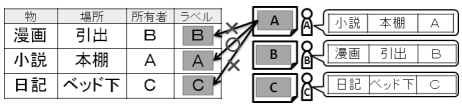

図 3: LBAC の様子

3　ラベルの設計と検索

我々は，LBAC を用いて 2.2 節に述べた物品情報のアクセス制御を実現することにした．まず 3.1 節で，自分が想定した状況において必要なラベルを定義する．

[1]IBM 社

3.2 節，3.3 節にてそれぞれ，2.2 節の (1)，(2) の問い合わせを実現するためのラベル付与について述べる．

物探しシステムは研究室や家など小規模な集団においての使用を前提としているので，ここでは佐藤家の三人 (父・太郎，母・花子，息子・次郎) と，鈴木家の息子 (良夫) が同じ物探しシステムを使う場合を考える．使用者の情報は，図 4 のテーブルで表わされる．

名前	立場	家
太郎	父	佐藤
花子	母	佐藤
次郎	子	佐藤
良夫	子	鈴木

図 4: 使用者の情報テーブル： HITO

我々は個人名を表すラベル，家族内での立場を表すラベル，どこの家の人かを表すの 3 つのグループのラベルを用意した．

ユーザは図 5 で示したように，自身に該当するラベルを所有する．

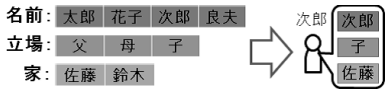

図 5: ラベルを用意し，個人に付与する

3.1 状況 1 ：物を完全に隠す

次郎が日記，参考書，はさみを所有し，共有 DB に物の情報を登録しているとする．次郎はもちろん全ての物のデータを閲覧することができるが，他の人には以下のような情報の見せ方をしたい．

- 日記：誰にも見られない．
- 参考書：子供たちのみ見られる．
- はさみ：同じ家の人のみ見られる．

ここでのプライバシー保護は，単純に行レベルでのアクセス制御を行えば実現する．物のデータが入っているテーブルにおいて，図 6 のように，日記の行には [次郎] のラベル，参考書の行には [子] のラベル，はさみの行には [佐藤] のラベルを張る．[次郎] ラベルが付いている行には [次郎] ラベルを持つユーザ，つまり次郎に本人しかアクセスすることができない．

図 6: 実際のテーブル

このテーブルにアクセスした際日記が自分以外の検索結果には表示されないのに加え，親には参考書，良夫にははさみの情報が表示されていない．よって，データの見え方は次郎の要求通りとなる．

3.2 状況 2 ：ユーザによって場所の見え方を変える

次郎が，机の中に交換日記を入れている．全員に交換日記の存在は教えるが，場所の見せ方はユーザに対して変えたい．

- 良夫には，情報を詳細に表示する．
- 花子には，曖昧な位置を表示する．
- 太郎には，場所は全く見せない．

この場合は，物がしまってある場所のユーザに対する見せ方が設定されている状態である．この場合，単純に行や列のデータを隠しただけでは次郎が望むようなアクセス制御は実現しない．そこで，場所のテーブルを作成する際に工夫をする．

物を表すテーブル，場所を表すテーブルの他に，場所の見え方をユーザによって変える情報選択テーブルを作成し，行にラベルを付ける．実際に良夫が「交換日記」を検索する際の流れを，図 7 を使って説明していく．まず物情報が登録されているテーブルから，交換日記の物 ID を取得する．次に情報選択テーブルにアクセスし，取得した物 ID を使って場所 ID を取得する．情報選択テーブルの行にはラベルが付いているので，自分が持っているラベルによって返される場所 ID が変わる．良夫は子のラベルを持っているので，返される場所 ID は「 p 002」となる．最後に，情報選択テーブルから返された場所 ID を使って場所の名前を検索すると，良夫に返される交換日記の場所情報は「次郎の机」となる．

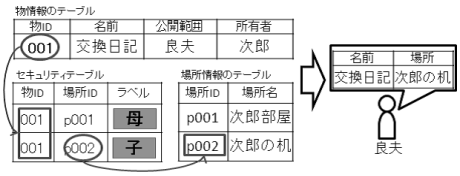

図 7: 場所のテーブル

花子は子のラベルを持っていないので，情報選択テーブルにおいては母のラベルの付いている行にアクセスし，場所情報「次郎部屋」を得る．太郎は情報選択テーブルのどの行にもアクセス出来ないので，詳しい場所が表示されない．よって，次郎のプライバシー保護要求は満たされたことになる．

4 まとめと今後の課題

本稿では，テキストベースの物探しシステムを提案し，様々なアクセス制御をすることによって，最低限のプライバシ保護ができるようなシステムを提案・実装した．

今後はラベルの包含関係を考え，さらに柔軟なシステムを作ることを目標とする．今回解決に至らなかった 2.2 節 (3) の問題についても，検索ログを取るなどして今後解決していきたい．

また，本論文では「情報を隠ぺいする」ことに重点を置いて議論したが,「積極的に情報を開示する」ことによって，結果的にプライバシーが保護される状況についても今後は考えていきたい．

参考文献

[1] 小松崎 瑞穂: “ 2 次元コードと写真を利用した物探し支援システム,” In **お茶の水女子大学** *2008* **年度卒業研究**, febrary 2009.