# 可変秘匿 ID 方式を用いた図書館向け RFID プライバシ保護プロトコル

諸橋　玄武　　木下　真吾　　星野　文学

NTT 情報流通プラットフォーム研究所
〒 239-0847 神奈川県横須賀市光の丘 1-1

{gembu,kinosita,fhoshino}@isl.ntt.co.jp

**あらまし**　近年流通業界を中心に業務に RFID を取り入れる動きが進んでいる．一方で RFID が付随したモノが消費者の手に渡ることから生じるプライバシの侵害が深刻な問題になっており，RFID の導入に対する障害の一因になっている．こうした問題に対し，我々はこれまでに低コストでプライバシ問題を解決する基盤技術として可変秘匿 ID 方式を開発してきた．本論文では，所有者／利用者，利用期間といった点において，いわゆる消費財と異なる特性をもつレンタル分野，特に図書館分野におけるプライバシ問題の考察するとともに，可変秘匿 ID 方式の適用プロトコルを提案する．提案プロトコルでは，可変秘匿 ID 方式の ID 再暗号化方法（再暗号化を行う端末や契機）や復号方法などを図書館業務プロセスに最適となるように具体化している．また，図書館以外のレンタル分野への適用性についても考察する．

# RFID Privacy Protection Protocol for Libraries with the Unidentifiable Anonymous ID Scheme

Gembu MOROHASHI　　Shingo KINOSHITA　　Fumitaka HOSHINO

NTT Infomation Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka
Kanagawa, 239-0847 Japan

{gembu,kinosita,fhoshino}@isl.ntt.co.jp

**Abstract**　RFID technologies become to be used in the supply chain. However tagged items bring privacy risks for consumers.

This paper presents consideration about privacy issue related to RFID in libraries, concerning users, borrowers and loan periods. Moreover we propose an application of the unidentifiable anonymous-ID scheme which we have developped. This application provides the re-encryption process in the anonymous-ID scheme. Then we discuss the triggers for re-encrypting, the placement of the re-encryption terminals, and decryption process in the anonymous-ID scheme. Furthermore we discuss applicabilities to other rental services.

## 1　はじめに

RFID（Radio Frequency IDentification）とは無線通信を用いた自動認識技術であり，最近特に注目されているのが RFID タグである．これは IC チップとアンテナを内蔵した荷札で，無線タグ，IC タグなどとも呼ばれ，流通業界を中心に導入への動きが盛んになっている．また，ユビキタスサービスの基盤技術として様々な応用が考えられており [5]，例えば書籍業界では流通・在庫管理から店頭での万引き防止，さらに古本市場への盗品の流出防止に利用する計画もあり，導入に向けた実証実験なども盛んに行われている．図書館においても，RFID の特性が業務の効率化につながると期待され，すでに各地の図書館で導入が進んでいる．

一方で，RFID タグが貼り付けられたモノが利用

者の手に渡ったとき，利用者のプライバシが侵害されることが深刻な問題になっている．RFID 導入に反対する動きも目立っており，RFID 普及に向けた課題のひとつになっている．我々は RFID によって侵害される利用者のプライバシを保護する技術を開発し，基盤技術として可変秘匿 ID 方式 [1] および Hash-Chain 方式 [4] を提案してきた．

本論文では，図書館に RFID を導入した場合に生じるプライバシ問題について議論し，ひとつの解決策として，可変秘匿 ID 方式の適用プロトコルを提案し，その適用性について考察する．

## 2 図書館への RFID 導入とプライバシ問題

現在多くの図書館では業務の効率化を目指してシステムの電子化を進めている．具体的には，蔵書をバーコードを用いて管理する方法が多くとられている．RFID タグを導入することによって，貸出・返却業務，蔵書点検作業の効率化，蔵書検索サービスの向上などが期待される．例えば，貸出・返却処理においてバーコードでは 1 冊ずつ読み取らなければならなかったが，複数の本を重ねたままの読み取りが可能となり，処理時間・作業の手間が大幅に削減される．また，出入口にゲートを設置することで貸出処理がされていない蔵書を持ち出された場合に検知できたり，書架にリーダを置くことで蔵書の位置確認や閲覧状況の確認も可能である．

図書館での利用も国内外で拡がってきている．すでに米・カリフォルニア州のサンタ・クララ市立図書館，ネバダ大学ラスベガス図書館，オレゴン公立図書館などではすべての蔵書，CD などに RFID タグが貼り付けられている [2]．国内では宮崎県北方町立図書館，島根県斐川町立図書館，千葉県富里市立図書館，福岡県筑穂町立ちくほ図書館，九州大学附属図書館筑紫分館，国立広島原爆死没者追悼平和祈念館，アド・ミュージアム東京などですでに導入されている [3]．

**図書館におけるプライバシ問題**　図書館ではその公共性から利用者のプライバシ情報の取り扱いについて，十分に考慮する必要がある．特に書籍という特殊な物品を扱っていることから，図書館が持ちうる情報にはプライバシに直接結びつくものが非常に多い．例えば利用者の貸出・閲覧等の履歴情報は，その利用者自身の趣味・思想を色濃く反映している．また，同じ本を借りているのが誰かといった情報を調べると，何冊か調べていくうちに思想等の他に交友関係[1]なども類推されてしまう恐れがある．

**RFID によるプライバシ問題**　RFID 導入によって多くの利点が生まれる一方で，利用者のプライバシが侵害される恐れがあるということが問題視されている．RFID タグのメモリに書籍のタイトル，サブタイトル，著者名，発行年等の書誌データが入力されていれば，鞄に入れていたり，ブックカバーをかけていても，無線通信によって知らない間に所持している本に関する情報が他人に知られてしまう恐れがある．図書館では蔵書管理をする上で，同じ本を複数所蔵することが多々あるので，蔵書 1 冊ずつにそれぞれ個別の ID を割り振って管理する必要がある．RFID タグにもそのような個別の ID 情報が入力される．RFID タグに個別の ID 情報だけを入力する方式も考えられる．しかし攻撃者があらかじめ ID と書誌データの対応表を作っておけば，ID 情報のみからでも本に関する情報を知られてしまう恐れがある．

また，この ID 情報が利用者と結びついた場合，すなわち蔵書の ID 情報を逐次追跡していけば，この蔵書を持った人が何時にどこへ行った，というような行動履歴を取ることが可能である．この問題は図書館に限った話ではなく，一般に RFID を利用した場合に生じうる問題であり，RFID 普及への大きな課題のひとつである．

**取り上げる問題**　本論文では，ここに挙げたような図書館での RFID 利用によるプラバイシ問題のうち，

(1) 所持している本に関する情報の漏洩の問題，
(2) 図書館データベース情報に関連する問題（本の ID 情報と貸出状況などを管理する図書館のデータベースの情報が結びついて生じるプライバシ情報の漏洩の問題），
(3) 図書館内外での利用者の行動追跡の問題

について注目し，その解決方法を探る．

**対策**　プライバシ保護の観点から，プライバシ保護のために RFID タグの読み取りができないようにする方法や，RFID タグの機能無効化といった方法

[1] 例えば，知人に推薦されて本を借りることが多い場合等．

(kill コマンド) が提案されている．また，RFID タグを運用する際のガイドライン [6] が策定されている．図書館では書籍は繰り返し利用されるため，貸出処理ごとに RFID タグを無効化する（返却時に新しいタグに貼りかえる）といった方法はふさわしくない．貸出処理の際 kill したものを返却時に復活させる（re-activate）といった方法も考えられるが，re-activate 処理をタグの方で制御できない，すなわち攻撃者に勝手にタグの機能を復活させられる恐れがある．攻撃者によるタグの読み取りを防ぐにためは，タグに読み取りのアクセス制御の仕組みを取り入れる方法もある．例えばパスワードによる保護が考えられるが，タグごとに異なるパスワードを設定できないため，その安全性や RFID タグのパスワード更新等の運用コストが問題となる．そこで，本論文ではプライバシ保護技術として NTT が開発してきた可変秘匿 ID 方式 [1] の適用を考えてみる．この方式ではメモリの書換機能を持つ単純なタグ利用することでタグにかかるコストを低く抑えられ，かつある一定のプライバシを保護することができる．

# 3 可変秘匿 ID 方式 [1]

RFID 特有のプライバシ問題として先に述べたように書名等の書誌情報の漏洩と，ID の追跡の問題がある．これらの問題を解決するために必要となるのが ID 情報の秘匿性と同定不能性であるが，それらを実現する方式のひとつに，可変秘匿 ID 方式がある．可変秘匿 ID 方式では，元の情報を暗号化（秘匿化）し，ある一定の機会で暗号文の更新（再秘匿化）を行うことで同定不能性を実現している．暗号化や再秘匿化の処理（計算）はタグ内で行うのが理想的だが，タグに暗号処理回路もしくは CPU の搭載が必要でコスト面から実現は難しいため，これらの処理は外部コンピュータで行い，タグには複数回書き換えが可能な EEPROM 等の ROM を搭載したタグを利用することで実現性を得ている．秘匿化の方法として，ランダム化，共通鍵暗号化，公開鍵暗号化の 3 つの方法が提案されているが，それぞれ特徴があり，例えば公開鍵を用いると秘匿化後の暗号文が大きくなり，ランダム化の方法では暗号処理を行う際サーバ側の負担の大きくなる．

可変秘匿 ID 方式であっても以下にあげるような問題がある．まず，RFID タグの存在自体は隠すことができない．攻撃者にはタグの付いた何かを持っていることが把握されてしまう．また，再秘匿化処理のタイミングの問題がある．再秘匿化は自動的に行われないため，ある一定の機会で再秘匿化処理を行う必要がある．再秘匿化を可能にするためにタグは書き換えが可能な性質を持つが，書換処理を行う装置を認証することができないため，任意の値を書き込まれてしまう恐れがある．(改竄検出の方法は [1] で検討されている.) 他にも（再）秘匿化や復号化を行う際必要となる鍵の（サーバ側での）管理の問題がある．再秘匿化処理の機会について，図書館等のレンタル業の分野では短い貸出期間の前後に貸出・返却処理を必ず行うため，この機会に再秘匿化を行うことで，問題点を補完できるものと考えられる．

# 4 可変秘匿 ID 方式の適用プロトコル

## 4.1 図書館業務システムのモデル化

ここでは，図書館業務に利用されるシステムを貸出業務に注目してモデル化する．まず，貸出業務に関わる装置として，貸出管理 DB，蔵書 DB，本に割り当てられた ID の暗号化・復号化・再暗号化等を行うセキュリティサーバおよび受付カウンタで貸出手続きの際にタグの読み取り，書き込みを行う端末（貸出端末）を用意する．また，貸出処理を行ってない蔵書が持ち出されないよう，図書館の出入口にチェックゲートを設置する．一般に図書館業務を行うには，さらに利用者登録情報 DB，蔵書検索システム，書籍・雑誌購入システム等が必要となるだろう [7]．図書館の利用者にはそれぞれ個別の ID（ユーザ ID）が与えられているものとする．利用者（登録）証は RFID に限定しない．RFID によるプライバシ脅威を考えると，磁気カードやバーコード等 RFID 以外の方式のほうが扱いやすいかもしれない．一方，図書館の蔵書には RFID タグが貼付され，それぞれ個別の ID が与えられているものとする．[2]

[2] RFID タグの容量の大きさによっては，個別 ID の他に書誌データや最終利用日等の情報をタグに入力しておく方法も考えられる．

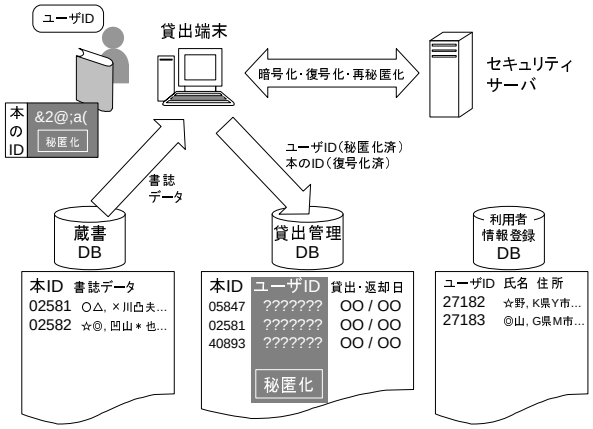


図: 可変秘匿 ID 方式の適用プロトコル（貸出処理）

### 4.2 各業務への可変秘匿 ID 方式の適用プロトコル

**貸出** 貸出処理では，利用者が借りたい本を貸出端末まで持参し，以下のような手順で貸出手続きを行う．

1) 貸出端末にユーザ ID と借りたい本の（暗号化された）ID を読み取らせる．
2) 貸出端末は読み取った（暗号化された）本の ID をセキュリティサーバを介して復号化する．また読み取ったユーザ ID をセキュリティサーバを介して暗号化する．ここで，ユーザ ID を暗号化する際には確率暗号（同じ平文を暗号化しても異なる暗号文を得られるような暗号）を用いるものとする．すなわち，同じユーザ ID を暗号化したものどうしから関連性を見出すことは難しい．
3) 復号化した本の ID と暗号化されたユーザ ID を貸出管理 DB に送る．
4) 貸出管理 DB は，本の ID をキーとして貸し出しに関係する情報を管理する．ここでは，送られてきた本の ID，暗号化されたユーザ ID に加え，貸出日と返却期限日を貸出リストに蓄積する．
5) 貸出管理 DB の処理が無事終わったら，貸出端末はセキュリティサーバを介して本の ID の再秘匿化を行い，本の RFID タグに書かれた ID を再秘匿化したものに書き換える．

**返却** 返却処理では，返却された本を返却端末で以下のような手順で返却手続きを行う．

1) 利用者は返却端末に返却する本の（暗号化された）ID を読み取らせる．
2) 返却端末は読み取った本の（暗号化された）ID をセキュリティサーバを介して復号化し，本の ID を貸出管理 DB へ送る．
3) 貸出管理 DB は受け取った本の ID と合致する情報を貸出リストから検索し，該当する項目の情報を削除することで貸出登録を抹消する．
4) 貸出管理 DB の処理が無事終わったら，返却端末はここでセキュリティサーバを介して本の ID の再秘匿化を行い，本の RFID タグに書かれた ID を再秘匿化したものに書き換える．

**不正持ち出し検出** チェックゲートでは貸出処理されないまま蔵書が持ち出されないかチェックをする．ゲート通過時に（暗号化された）本の ID を読み取り，セキュリティサーバを介して復号化し，得られた本の ID を貸出管理 DB に照会し，貸出中かどうか調べる．

**返却遅滞の検出** 返却が滞っているものについては，貸出管理 DB から該当する（返却遅滞の）本の貸出情報を検索し，そこに含まれる暗号化されたユーザ ID をセキュリティサーバを介して復号化することで，利用者 ID を得て，それを元に利用者情報登録 DB から返却が滞っているユーザを特定し，返却を催促する．

## 5 考察

前述のプロトコルでは可変秘匿 ID 方式を用いることで，低コストで実現可能ながらもプライバシを保護できる方式を提案した．ここでは 2 節で注目した 3 つの問題を中心に考察をすすめる．このプロトコルに対して様々な攻撃が考えられるが，前提としてセキュリティサーバは頑強であり認証を受けたものでないと復号化依頼はできないものと仮定し，暗号化（秘匿化）された情報はセキュリティサーバによる復号化を受けない限り復号化できないものと仮定する．

**(1) 所持している本に関する情報の漏洩**　まず本に付けられたRFIDタグの情報について考える．RFIDタグには本のIDが常に秘匿化された状態で記憶されているため，RFIDタグから読み取れる情報そのものからは，その本に関する情報は得られない．

また，あらかじめ図書館の書架に収められた蔵書の（暗号化された）IDを読み取り，(それを新たな“ID”とみなすことで）書名などの書誌データと対応付け，ID情報から書誌データを得るという攻撃が考えられる．しかしこのプロトコルでは貸出・返却時にIDの再秘匿化処理を行っているため，図書館内で読み取った蔵書の“ID”と結び付けておいても，同じ蔵書の“ID”を図書館の外で読み取ると別の“ID”に見える．(ゆえに書誌データと対応付けできない.)

**(2) DB情報に関連する問題**　次に，DBの情報が漏洩した場合を考える．このプロトコルで登場するDBのうち，主に利用者の情報が関係する（ユーザIDが含まれる）のは利用者情報登録DB，貸出管理DBである．

まず貸出管理DBの情報が漏洩した場合を考える．貸出管理DBには貸出中の本のID，それを借りている利用者の暗号化されたユーザID，貸出・返却日である．ユーザIDは確率暗号によって暗号化されているため，ここで利用者情報登録DBの情報が知られていたとしても，同じユーザIDを暗号化したもの同士に関連性は見つけられないため，該当の本を誰が借りたかといった情報はわからない．また，どの本が借りられているかという情報だけは知られてしまうが，そもそもこの情報は通常のサービスとして提供されるものである．貸出管理DBは現在の貸出状況のみを蓄積しているため，過去にどのような本を借りたのか，といった情報も知られない．実際に貸し出されている本のRFIDタグには，ここに記録された本のIDを暗号化したものが記憶されているため，(暗号化されたユーザID等の）貸出情報と実際の本とは結びつかない．

利用者情報登録DBについては蓄積されている情報そのものが個人情報にあたるため，この情報が漏洩すること自体大きな問題であるが，ここでは特にユーザIDと個人情報が結びついてしまうことに注目する．4.1節で述べたようにユーザIDの情報が書き込まれる利用者証にRFIDを用いなければ，利用者証所持者の同意なしにユーザIDを読み取ることは難しく，どこの誰かといった情報がすぐにはわからない．

**(3) 利用者の行動追跡**　本のRFIDタグに入力されたIDは暗号化されているが，この暗号化データを新たなIDとみなして追跡することが考えられる．これについては貸出・返却処理で必ず再秘匿化処理を行うため，前後の関連性は断たれ，追跡から逃れることができる．本提案では貸出から返却までの間（すなわち図書館の外では），再秘匿化処理は行われないため，固定されたIDによる行動の追跡はそのままでは対応できない．図書の貸出期間は短く，(2)で考察したように図書館のDBから個人情報に結びつく情報が取られにくいこと，また返却後の貸出履歴がまったく残らないことから，消費財などと比較すると危険性は低い．根本的にこの問題を回避するには，ある一定の間隔で再秘匿化処理を行う必要があるため，図書館の受付等で再秘匿化するか，信頼できる再秘匿化端末を（コンビニや駅等街中に）設置し，利用者にたびたび再秘匿化してもらわなければならない．あるいは，Hash-Chain方式で提案しているようなタグ内部で再秘匿化処理を行うようにすれば（タグにかかるコストが高くなるが）回避できる．

**その他の問題点**　今回のプロトコルでは図書館内にある蔵書のRFIDタグの情報も秘匿化しているが，復号化の手間を考えると図書館内では本のIDをそのまま記憶させるという方法も考えられる．例えば，書架に読取装置を設置し，本の位置や閲覧状況などを常時監視するようなシステムでは，IDを秘匿化しておくよりも（復号化の手間が省けて）効率が良いのではないか，と考えられる．復号処理の負担については，現状の読取性能（読取処理にかかる時間）と比較して考えよう．現状として読取装置が高価なため図書館内全体に設置するには限度があり，アンテナを多重化する等の対策をとることが考えられる．このときの読取性能は（IDの衝突回避の処理等により）あまり良くないため，読取処理にかかる時間に比べると秘匿化IDの復号処理にかかる時間はそれほど影響しないと考えられる．

復号化・再秘匿化処理において，セキュリティサーバは与えられた暗号化されたIDに対応する鍵がどれであるか知る必要がある[3]．単純にすべての鍵で

[3] これは3章で述べた秘匿化の方式の選び方にも依存する．

処理を試みる方法も考えられるが，蔵書が何万冊にも及ぶような図書館では，その処理にかかる時間も大きい．このため，暗号化された ID には対応する鍵の情報を付与しなければならない．最も簡単な方法として，すべて同じ鍵を用いる方法も考えられるが，鍵が知られてしまった場合の影響が大きく，鍵の変更作業もすべての蔵書に対して行う必要があるためリスクが大きい．逆にすべて異なる鍵を用いると，前述のような鍵の情報を付与しなければならない．しかし，この鍵の情報はまさに個別の ID を与えていることに他ならない．以上のことから，蔵書をいくつかの鍵で管理することが最良と考えられるが，このとき，同じ鍵を使う蔵書にはなるべく関連性がないようにしなければならない．本の ID は，管理上の利便性から十進分類法等に沿った番号付けをすることが考えられるため，ID をベースにグループ分けを行うには十分注意が必要である．例えば，よくあるコード体系では末尾に近い数字にシリアル番号が振られていることが多いので，末尾の番号ごとにグループ分けする，あるいは図書館に納品された日付でグループ分けする等といった方法が考えられる．

また，本に付けられた RFID タグは書き換えが可能であるため，記憶された情報が改竄されてしまう恐れがある．改竄された情報は正しいものに書き換えなければならないが，例えば本に RFID タグとは別にバーコード等で ID を印字しておき，書換時に利用することで運用上の手間を削減することも可能である．

図書館業務を合理化するため貸出・返却処理をセルフサービス化することも可能であるが，ここで注意すべきところは貸出・返却処理が正しく行われるかどうかである．例えば貸出の際，貸出管理 DB への登録は終了したが，再秘匿化処理が終わらないうちに端末から離されてしまうと，先に述べたような ID の追跡や，書誌データの漏洩につながってしまう．再秘匿化処理を終了する前に本が取り除かれた場合は警告を出す，あるいは端末に扉をつけ，処理が終わるまで取り出せないようにする等一連の処理が確実に実行されるような工夫が必要である．

**レンタル業への適用**　本提案の適用先として図書館と同じような業務形態であるレンタル業，例えばレンタルビデオ，観光地などでのレンタサイクルや手漕ぎボート等への適用も可能である．レンタル業では，貸出・返却の処理にレンタル料金の徴収という重要なセッションがあるため，図書館に比べて貸出・返却処理が確実に行われると考えられる．

## 6　おわりに

本論文では図書館で RFID を利用したときに生じるプライバシ問題を挙げ，低コストで実現可能なプライバシ保護技術である可変秘匿 ID 方式を用いて，いくつかの問題を解決するプロトコルを提案した．RFID タグそのものにはあまり機能を求めない方式であるため，実現性の高いプライバシ保護方式として有効であると考える．今後の課題としては，図書館外での再秘匿化処理が挙げられるが，例えば複数の図書館が連携し，近くのコンビニなどで貸出・返却が行われるようになれば，再秘匿化の機会についても改善されると考えられる．

## 参考文献


[1] 木下 真吾, 星野 文学, 小室 智之, 藤村 明子, 大久保 美也子, “ローコスト RFID プライバシ保護方法,” 情処学論, vol.45, no.8, pp.2007–2021, Aug. 2004.

[2] D. Molnar, D. Wagner, “Privacy and Security in Library RFID Issues, Practices, and Architectures,” http://www.cs.berkeley.edu/~dmolnar/library.pdf, Jun. 2004.

[3] NTT Comware, “IC タグを導入した図書館の未来形,” Comzine, 2004. 2 月号, http://www.nttcom.co.jp/comzine/no009/dragnet/index.html, Feb. 2004.

[4] M. Ohkubo, K. Suzuki, S. Kinoshita, “Cryptographic Approach to a Privacy Friendly Tag,” RFID Privacy Workshop@MIT, http://www.rfidprivacy.org, Nov. 2003.

[5] 総務省 ユビキタスネットワーク時代における電子タグの高度利活用に関する調査研究会, “「ユビキタスネットワーク時代における電子タグの高度利活用に関する調査研究会」最終報告,” 総務省, http://www.soumu.go.jp/s-news/2004/040330_6.html, Mar. 2004.

[6] 総務省, 経済産業省, “電子タグに関するプライバシー保護ガイドライン,” 総務省, 経済産業省, http://www.soumu.go.jp/s-news/2004/040608_4.html, Jun. 2004.

[7] 図書館情報学ハンドブック編集委員会, “図書館情報学ハンドブック,” 丸善, Mar. 1988.