可変秘匿ID方式を用いたRFID電子カルテシステムの提案

菅原康太†　高橋修†

公立はこだて未来大学システム情報科学部†

1 背景

RFID(Radio Frequency IDentification)タグはリーダからの電力供給能力を持ち，無線通信によって非接触で自動認証を行える電子デバイスである．タグには電力の供給方法から 2 種類に分けられる．1 つは電源を内蔵せず，リーダとの相互誘導によって発生する微弱電波によって電力をまかない通信を行うパッシブタグであり，もう 1 つはボタン電池などの電源を内蔵し，タグ自ら電波を発してリーダと通信を行うアクティブタグである．これらタグは，バーコードの認証率が 70%程度なのに対して 99%以上と言われる高い認証率が特徴である[1]．また，タグはバーコードや QR コードとは異なり以下のような利点が存在する．

1) データの書き込み，追記が出来る
2) 汚れ，磨耗に強い
3) データの暗号化が出来る

このような利点から RFID は FeliCa や Edy などの電子通貨の認証作業や家畜にタグを取り付け個体情報の管理などを行うトレーサビリティの領域を中心に利用が広まっている．

2 研究の目的

本研究では，RFID の高い認証率などの利点を様々な分野へ導入を促す第一歩として普及率が低い電子カルテへの RFID の認証システムの設計を目的とする．具体的には以下の2つである．

1) 患者カルテ作成時における暗号化作業にタグのデータを暗号化の種として用いて行い，カルテへのアクセス権の制限を施す
2) 作成後のカルテに対する追記処理の認証作業をタグを用いて行い，不正アクセス・改竄を防ぐ

また，本研究に対する医療現場を想定した要件定義を行い，プロトタイプシステムにより実装・評価を行うことを目標とする．目標に対する達成の評価は，実際に病院でプレゼンテーションやシュミレーションなどを行い，病院側からの評価をしてもらう．更にアプリケーションの性能面から実行時間などの評価を加え，最終的な評価とする．

3 研究課題

3. 1 従来の研究状況

関連研究として医療面ではインシデント(うっかりミス)対策のシステム構築が挙げられる．代表的な例として看護師が PDA などの端末機器を携帯し，点滴，採血時などに患者の腕に取り付けられた個人 ID などが書き込まれたタグと点滴パックのタグの情報を読み取り，比較することで患者や薬品の取り違いなどのミスを未然に防ぐシステムである[2]．また，暗号化に関する従来の研究では，RSA 暗号を用いる方式[3]と ID ベース署名を用いて RSA 暗号で行う場合より署名の長さを短くし，同等の強度を持たせる方式[4]が提案されている．以上のように，電子カルテでの利用が少ないことで総合的な導入が出来ないことが問題となる．そのため，電子カルテにも RFID を利用できるシステムを構築することが必要となる．

3. 2 要件と課題

本研究で満たさなければならない電子カルテに求められる要件は「保存義務のある情報の真正性の確保」[5]である．これは他者のカルテとの混同や改竄などを防ぎ，作成の責任所在を明確に出来ることが必要となる．この要件を満たし，従来の電子署名，暗号化と比較した際に煩わしさやセキュリティの不安を感じないような工夫を施すことと，限定された小さなメモリ資源しか有しない RFID への適切な実装方法の検討が課題となる．

4 RFID 電子カルテシステムの提案

4. 1 提案システムの概要

本研究では，以下の2つのシステムを想定して上記の電子カルテの要件「真正性の確保」を主として検討する．

1) 暗号化システム

このシステムはカルテ作成時に患者，医師，看護師の3者が揃っている状況を想定する．この3者の個人タグを揃え，リーダに通すことでカルテの暗号化を行うシステムである(図1)．このシステムでは3者の内一人でも欠けた場合，カルテの暗号化は成立しないものとし，これによって真正性を実現する．生成される秘密鍵は秘密分散法(後述)を用いて分割し，分割情報を3者に対応付ける．

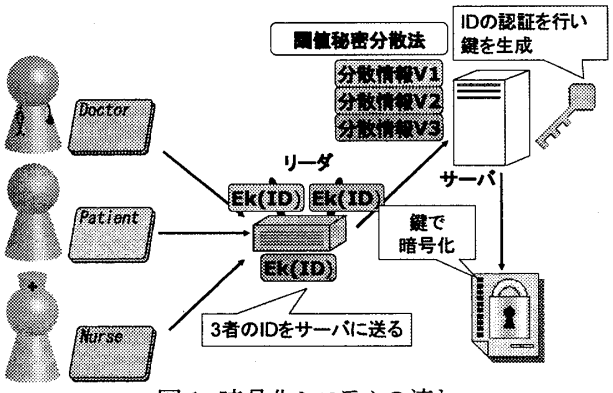

図1 暗号化システムの流れ

Proposal RFID Electronic Medical Chart System using Unidentifiable Anonymous ID Scheme

† Kouta Sugawara ・Future University-Hakodate
† Osamu Takahashi ・Future University-Hakodate

2) アクセスロックシステム

このシステムはカルテ作成後の追記処理を行う場合で患者がいない状況を想定する. 追記を行う役職の人の分割情報ともう一方の役職の人の分割情報の2つをもとに秘密鍵を作り, 作成済みのカルテの変更は行わずに追記カルテに追記可能となるアクセスロックシステムとする(図2).

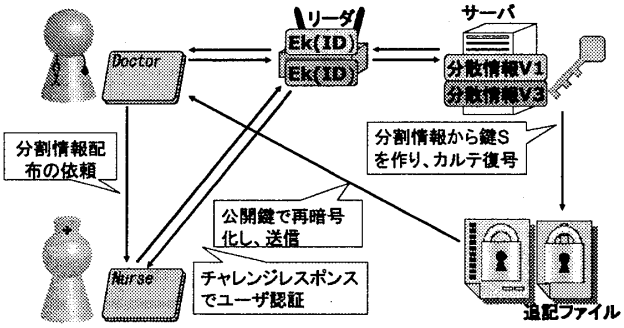

図2 アクセスロックシステムの流れ

上記提案方式における実現方式を 4.2, 4.3 節に示す.

4. 2 暗号化システムの実現方法

ID(暗号化の種)の再暗号化の際, リーダ, タグに加えてセキュリティサーバを設ける可変秘匿 ID 方式[6]を採用する. この方式ではタグの中には暗号化された ID である秘匿 ID のみを保有し, リーダが秘匿 ID に対応する ID の取得要求をセキュリティサーバに依頼することでタグの消費メモリとコストを抑えている.

本提案方式では秘匿 ID に位置するものを暗号化の種に置き換えることでタグの少量のメモリ資源の消費を抑え, タグ内の情報は ID そのものではないため, 紛失時の情報漏洩, ID 追跡問題を防ぐことができる.

4. 3 アクセスロックシステムの実現方法

秘密情報 S からn個の分割情報を生成し, n 個全てを収集することで S が復元可能な秘密分散法[7]を採用する. 本提案方式では, 秘密分散法の中でも 2-out-of-3 方式を用いる. この方式は通常 n 個全ての分割情報が必要であったのに対して n 個の分割情報に対して k 個の分割情報の収集で S が復元可能な方式である. この方式を用いることで個々の分割情報が漏洩しても S が守ることが可能となる. 本提案方式では秘密鍵が秘密情報 S に相当する.

5 基本実験システムの構築と評価

基本評価実験は以下の表 1. の開発環境で構築した.

表1 モバイル PC 用開発環境

OS	WindowsXP Home Edition sp2
CPU	GenuineIntel(R) CPU T2300 1.66GHz
RFID	Philips 社 I-CODE-SLI
リーダ/ライタ	Omron 社 V720S-HMF01
プログラミングツール	Microsoft Visual C# 2005 Express Edition

基本評価実験におけるシステム構成を図 3 に示す.

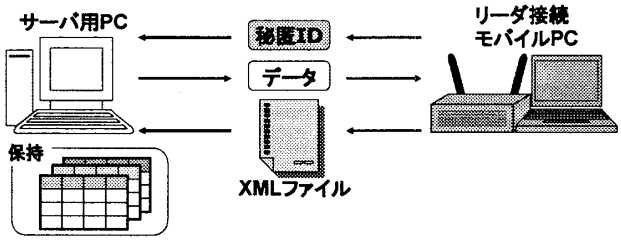

図3 基本評価実験用システム構成

プロトタイプとしてモバイル PC に接続したリーダにかざしたタグから読み出した情報をもとに外部サーバのデータベースへアクセスし, 対応するデータの取得を行った. その後, このデータからカルテフォームを作成, 保存を行うシステムとした. テーブルでは ID と個人情報の対応付けと ID と分散情報対応付けを行っている. また, 秘匿 ID の読み出し, 書き込みは RFID が個別の動作しか出来ないため, 0.5ms のインターバルによって擬似的に一連の動作を実現している. そのため, Suica 使用時などと比較して長く感じられる.

今後の課題としてスケーラビリティの低下に関してテーブル構成の工夫と可変秘匿 ID 方式によって随時, 秘匿 ID が更新されるため, 秘匿 ID 更新頻度の適当な設定によるアクセス量の制限が必要となる.

参考文献

[1]国土交通省「RFID 技術応用による航空手荷物管理システムに関する調査研究報告書」
(http://www.mlit.go.jp/kisha/kisha02/15/150402/150402_2.pdf)
[2]株式会社オリンパスメディカルシステム
Solemio NURSE
(http://www.olympus.co.jp/jp/lineup/index2.cfm)
[3]寺西, 佐古, 野田, 田口
署名長が署名者数に比例しない RSA ベース Sequential Aggregate 署名方式
(CSEC2005 pp.393-398)
[4]P. Ith, Y. OYAMA, A. INOMATA, E. OKAMOTO
Implementation of ID-Based Signature In RFID System
(DICOMO2007 pp.1243-1248)
[5]株式会社 BML 電子カルテ導入の手引き
(http://www.bml.co.jp/medical_station/guidance/index.html)
[6]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
(情報処理学会論文誌 2004 pp.2007-2021)
[7]與那嶺裕, 與那嶺寛庸, 長田智和, 玉城史朗
閾値秘密分散法に基づく広域ネットワークストレージに関する研究
(電子情報通信学会 ISEC2005-81)