社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (5)
2009－CSEC－ 44 (5)
2009／3／5

医療分野における RFID タグシステムの情報セキュリティの確保

澤田 忍†‡ 田中 英彦‡

†株式会社 NTT データ
135-6033 江東区豊洲 3-3-3
sawadasnb@nttdata.co.jp

‡情報セキュリティ大学院大学
221-0835 横浜市神奈川区鶴屋町 2-14-1
tanaka@iisec.ac.jp

概要 RFID タグは、利便性や正確性の向上を目的として様々な実証実験が行われているが、RFID タグに格納された情報保護について課題となっている。本研究においては、医療分野を RFID タグ適用の対象として、いくつか典型的な利用シーンを洗い出し、その際に扱う情報やプロセスについて検討して具体的なシーンを確定する。さらに、拡張ミスユースケースを用いて、STRIDE の観点で情報漏洩や改ざんなどの脅威の洗い出しを行う。そして、タグの情報への脅威に対する有効な対策手法を分析・検討し、セキュアなシステム構成を具体化する。最終的には、対策がどのように有効に機能しているかについて、ミスユースアクティビティの手法を用いて検証する。

Research of Information Security Countermeasures of RFID Systems for Medical Applications

Shinobu Sawada †‡ Hidehiko Tanaka ‡

†NTT DATA CORPORATION
Toyosu 3-3-3, Koto-ku, Tokyo 135-6033, Japan
sawadasnb@nttdata.co.jp
‡ Institute of Information Security
Tsuruyacho 2-14-1, Kanagawa-ku, Yokohama, 221-0835 Japan
tanaka@iisec.ac.jp

Abstract There are some problems with information leakage of privacy data in applying RFID tags. In this paper, we show a secure method which protects confidential data for applying RFID tags to medical use. At first we propose some proper medical use case scenarios. Then, we apply the extended misuse case approach and 'STRIDE' threat analysis in order to protect confidential data. And then we detail an effective Information Security Countermeasures for protecting data in RFID tags, and design Secure RFID System. We apply Misuse activities method for verifying how the Secure RFID System's Countermeasure effect on the Threat.

1 はじめに

本研究は、RFID タグの適用先として、医療分野を対象とし、医療分野に RFID タグを適用した際の情報セキュリティに関する脅威と対策を検討し、セキュアなシステムデザインを提案して検証することを目的とする。

まずは医療分野の業務プロセスや前提条件を明確にし、そこで現れる典型的な利用シーンにおいて扱う情報やプロセスについて検討

し、拡張ミスユースケースを用いて、脅威の洗い出しを行う[6][10]。さらに対策の検討を行い、対策を実現するためのセキュアなシステムデザインを提案する。脅威から導出した対策の検討結果に基づきセキュアなRFIDシステムデザインを行い、その効果を、ミスユースアクティビティを用いて検証する[14]。

2 関連研究

RFIDタグに関する医療分野の取り組みと、情報セキュリティに関する取り組みについて関連研究を挙げる。

2.1 医療分野へのRFIDタグ適用事例

患者の病状の情報蓄積・活用・管理、薬品・医療用物資・医療用器材、手術用器材への適用による物品管理など、RFIDタグを用いて様々な実証実験が進められている[2][3]。

2.2 プライバシー保護に関する課題

RFIDタグの流通を見据えて、RFIDタグ自体の情報に対するプライバシー保護対策が必要であると提唱されている[5][8][9]。

また、プライバシー情報の保護に関するガイドラインとして、平成16年に、経済産業省と総務省により、「電子タグに関するプライバシー保護ガイドライン」が公表されている[5]。しかし、運用的な対処が主であり、タグの使用中のプライバシー情報に対する脅威に対しての具体的な対策が挙げられていない。

2.3 情報セキュリティ技術的な取り組み

RFIDタグの使用中におけるプライバシー情報に対する脅威を解決する取り組みとして、経済産業省は研究開発委託事業「UHF帯電子タグの技術開発事業（通称：セキュア電子タグプロジェクト）」（平成18年8月～平成19年3月）を実施し、その成果として「セキュアRFIDプロトコル」が開発された[7]。

また、文部科学省の次世代IT基盤構築のための研究開発として、「安全なユビキタス社会を支える基盤技術の研究開発プロジェクト」（平成17年～平成19年）を実施した[11]。RFIDタグの情報をアプリケーションごとにアクセス制御されるという提案が挙げられている。

2.4 関連研究のまとめ

医療分野のRFIDタグの適用や、情報セキュリティの確保に向けた取り組みは、近年ガイドライン策定や先進的な実証実験として実施されている。しかし、具体的な実利用に向けては技術的にも運用的にも十分に検討されているとは言えず、医療分野において取り扱う情報やプロセスまで検討して情報セキュリティの確保ができるモデルには至っていない。

3 医療分野における利用シーンの特定

まず医療分野にRFIDタグを適用する際、日本の医療機関や関係者について整理し、典型的な利用シーンについて整理する必要がある。そして脅威と対策を分析して、要件を定めなければならない。

3.1 医療分野の概要

医療とは、医療法（昭和23年7月30日法律第205号-最終改正平成20年5月2日法律第30号）において、病院、診療所、介護老人保健施設、調剤を実施する薬局その他の医療を提供する施設を医療提供施設として定義されている。本研究においては、「病院」をターゲットとする。

3.2 病院の関係者

医療分野における関係者としては、医療法においては、医療従事者として医師、歯科医師、薬剤師、看護師その他の医療の担い手が定義されている。本研究においては病院を対象とし、上記から歯科医師を除いた医師、薬剤師、看護師その他の医療の担い手を関係者として挙げる。また、RFIDシステムを導入する上で、システム構築や運用を実施するシ

ステム管理者を加えてこれらを関係者とする。

3.3 一般的な医療業務と医療事故

厚生労働省が実施した「医療安全対策ネットワーク整備事業（ヒヤリ・ハット事例収集事業）」により一般的な医療業務において、どのような業務において医療事故につながる「ヒヤリ・ハット」が起こっているか調査され情報提供が行われた[13]。「ヒヤリ・ハット」事例は、多い順に「処方・与薬（22%）」「ドレーン・チューブ類の使用・管理（15%）」「療養上の世話（9.4%）」「検査（5.8%）」「調剤・製剤管理等（2.8%）」となっており、「処方・与薬」が 11,733 件で全体の 22%を占め医療事故の主たる原因となっていると言える。

3.4 本研究で想定する利用シーン

3.3 の調査を基に、脅威分析の対象として、図に示される利用シーンを想定する[15]。

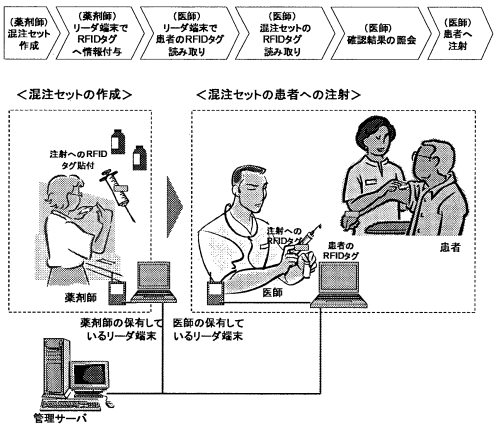

図 1 本研究で想定する利用シーン

4 拡張ミスユースケースを用いた脅威分析・対策立案

ユースケースは通常の開発で使われる標準記法(UML)である。本研究においては、Sindre らがセキュリティ向けに改良したミスユースケースを更に大久保らが拡張した拡張ミスユースケースを用いた[6] [10]。

その検討結果が[15]において示される。[15]で検討された対策に対して、想定脅威やコストを鑑みて、検討する対策を選択した。

まず「タグには ID のみを格納する」という対策についてについて、タグに ID のみを格納した場合と、そうでない場合について分けて検討したい。

「識別認証、アクセス制御を実施する」「信頼できるアクターの認証を加えるなどの二要素認証を行う」「タグーリーダライタ間で認証を行う」という対策に着眼し、アクセス制御及び二要素認証の観点で検討する。

「RFID タグ、通信経路、リーダライタの物理的破壊からの保護」については、使用する機器の筐体は物理的強度を持つものとし、通信経路について、LAN などは床下敷設されるものとして除外する。「機密情報機密情報は暗号化する」「タグーリーダライタ間、リーダライターサーバ間の通信暗号化」「タグーリーダライタ間の通信距離制限」「該当患者以外が利用すると無効となるタグを使用する」については、対策としては考慮せず、検証結果から必要性を述べる。

また、「Kill コマンドにより機能を停止させる」ことについては、リーダから Kill コマンドをタグに送信することで機能自体を停止させるものであるが、機能を有するタグが必要であり、通常利用時に常に有効に働くものではないため、採用しない。また、「書き込み不可能なタグを採用する」という対策についても、今回の利用シーンにおいては書き込みを行う必要性があるため、採用しない。

5 システムデザインの検討

RFID タグを用いて患者への注射を行う際に、RFID タグを用いることでどのようなシステム構成となるか、どのような脅威に対抗しうるかについて述べる。

5.1 利用シーンとシステム構成

下記の利用シーンに即してシステム構成を検討する。

まずは、「医師の指示の確認」において、看護師が医師の指示内容（混注セットと患者情報との適合性）確認を行い、薬品の副作用や、患者のアレルギー情報と問題がないかのチェックを行う。その際看護師はクライアントPC画面で指示内容の確認を行う。次に、薬剤師が混注セットの作成を行いRFIDタグを添付し、薬剤師の保有しているリーダからIDの付与を行う。付与されたIDはクライアントPCを通して管理サーバにも送付される。そして、混注セットを患者に注射する際、医師の保有しているリーダ端末で医師のICカードを読み取り、患者のRFIDタグのIDと、混注セットのRFIDタグのIDを読み取って照会し、クライアントPCの画面で確認し、問題がなければ注射を行う。そして、混注セットに添付されているRFIDタグを除去し、ゼロ値で上書きし、再利用する。混注セットは廃棄する。

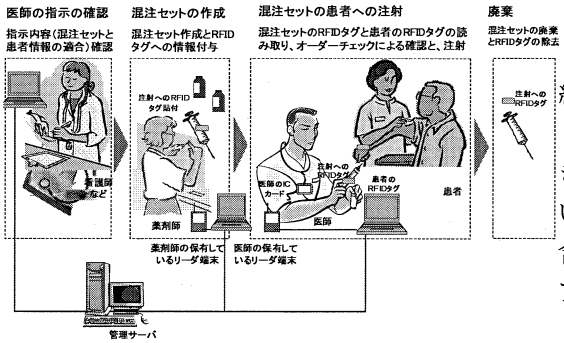

図 2 利用シーンとシステム構成

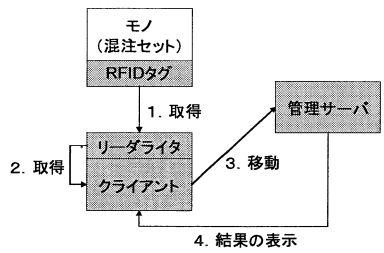

図 3 RFIDタグからサーバへの情報の流れ

なお、誤操作防止を目的とした取り組みはすでに検討されおり、提案されているシステム構成は同様のものである[12]。本研究においては冒頭に述べたように情報セキュリティの観点において検証を行った。

5.2 利用シーンにおける前提条件

システム構築の際、以下を前提条件とする。

- アプリケーションの脆弱性は考慮しない。また、サーバは物理的に安全
- 医師、看護師、薬剤師、システム管理者は、不正または誤操作を行わない
- 対象範囲は病院内部
- 医師、看護師、薬剤師、システム管理者が見ることのできる情報は必要最低限に制限する
- RFIDタグ、リーダライタの筐体は物理的強度を持つものとし、LANなどの通信経路について床下敷設により物理的破壊から保護される

なお、読み書きおよびアクセス制御が可能なRFIDタグを使用することを前提としており、周波数帯や電池の有無を限定しない。そして、IDのみを格納、もしくは複数情報を格納できるメモリを用いる。

また、混注セットのRFIDタグに付与すべき情報を薬品情報、禁忌・副作用情報）については、個人情報などのプライバシー情報は含まれないとみなし、本検討においては特にアクセス制御の対象としていない。

5.3 利用機器

本利用シーンにおいて、利用する機器は以下のものである。

管理サーバ／クライアントPC（医師用、薬剤師用）／リーダ端末（医師用、薬剤師用）／RFIDタグ（患者用、混注セット用）／ICカード（医師用）

5.4 RFIDタグの情報の配置

RFIDタグにIDだけを格納する場合とID以外の情報も格納する場合によって脅威に対

してどのように対抗しているかを比較した結果、RFID タグには ID のみを格納するという条件で情報を配置する。

- RFID タグ（患者用）：患者を識別する「患者識別 ID」
- RFID タグ（混注セット用）：混注セットを識別する「混注セット情報 ID」
- IC カード（医師用）：医師を識別するための「特定使用者識別 ID」
- リーダ：「リーダ ID」
- 電子カルテ・オーダサーバ：アプリケーション ID
  -アクセス制御リスト（図 4）
  -混注セットを識別する「混注セット情報 ID」に紐づいた薬剤の禁忌・副作用情報/患者を識別する「患者識別 ID」に紐づいた個人情報（名前、年齢、病歴など）
  -患者に注射する予定の混注セット ID のリスト/患者に対する薬の禁忌・副作用情報のリスト

「混注セットを患者に注射する」プロセスにおけるアクセス制御リスト

拡張ミスユースケース図におけるアクター		患者RFID		医師・看護師RFID	混注セットRFID		オーダーチェック結果
		アクセス制御情報	患者識別情報	アクター・利用者識別ID	混注セット情報	プロセスID	
医師	担当医師	×	読み取り	×	読み取り	変更	読み取り
	その他の医師	×	×	×	読み取り	×	読み取り
看護師		×	×	×	読み取り	×	読み取り
薬剤師		×	×	×	読み取り	×	読み取り
患者		×	×	×	×	×	読み取り
リーダ	許可	読み取り	読み取り	読み取り	読み取り	読み取り	
	非許可	×	×	×	×	×	
アプリケーション（許可）（電子カルテ オーダサーバ）		読み取り	読み取り	読み取り	読み取り	変更	作成/書き込み

図 4　アクセス制御リスト

6　検証

6.1　ミスユースアクティビティ図を用いた検証

アクティビティ図は、処理の流れを表現する。黒丸で表された開始点からスタートし、アクティビティを順番に実行して終了する。

本検証においては、RFID タグに ID のみを格納した場合を対象とする。リーダの起動を契機として、リーダ ID やアプリケーション ID の読み込みにより各アクターのアクセス制御を行った後に、患者の RFID タグの読み込みを行う流れとなる。

また、ミスユースアクティビティ図は、脅威から発生するミスユースアクティビティで表現されるのが特徴である。検証を分かりやすく表現するために、ミスユースアクティビティを採用して明示する[14]。

6.2　脅威（リーダのなりすまし）の検証

具体的に脅威にどのように対抗するかをミスユースアクティビティで示す。まずは脅威分析においても示した、リーダのなりすましについて検証する。

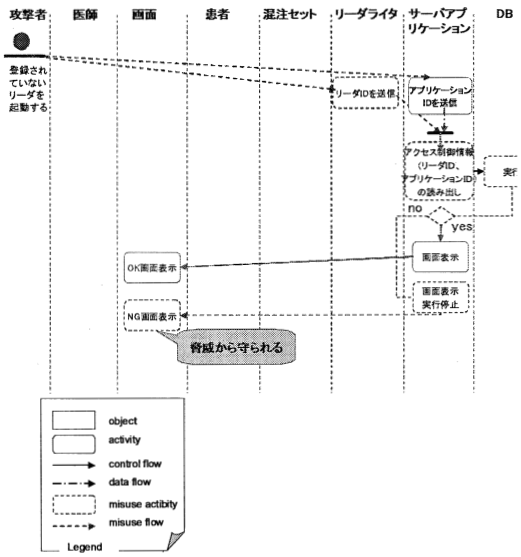

図 5　RFID タグからサーバへの情報の流れ

正規に登録されていないリーダのなりすましに対しては、アクセス制御機能において対抗し、脅威から守られることが分かる。

このようにいくつかのパターンで検証を実施した。

7　まとめ

検証において、患者の RFID タグに格納された情報の読み込み前に、アクセスの可否判断を行うことにより、リーダ、医師のなりすましによる情報漏洩や改竄を防ぐ。また患者

及び混注セットのなりすましについても防御する。そして、アプリケーション、プロセス情報によって利用シーンを細分化して制御することができる。

ただし、自身のRFIDタグやICカードを使用していた場合のなりすましには対抗できるが、別の人物のRFIDタグやICカードを用いてなりすましを行った場合にはシステムの機能だけでは対抗できないため、目視確認を行うなど運用面における対処を考慮すべきである。

RFIDタグやICカードにはIDのみを格納する方が、盗聴された場合の漏洩・改ざんの脅威も軽減する。しかし、トレーサビリティ情報などID情報を追跡する脅威に対抗する場合は、電波を遮断する仕組みや、IDを固定化しない、暗号化の対策などが必要となる。

また、今回のシステム構成においては、チップに格納する情報や通信路の暗号化の対策を行っていないため、特殊な盗聴装置やチップ自体の解析による漏洩・改ざんに対抗することが出来ないことを考慮する必要がある。

参考文献

[1] 情報処理通信機構「組み込みシステムの脅威と対策に関するセキュリティ技術マップの調査報告書」

[2]「ICタグと医療応用特集」、情報処理、2007年4月号

[3]「RFIDを利用した救急トリアージシステムの実証実験」情報処理学会論文誌 Vol.48, No.2(20070215) pp. 802-810

[4] RFID Journal:http://www.rfidjournal.com/

[5] 経済産業省・総務省「電子タグに関するプライバシー保護ガイドライン」(2004年)

[6] 大久保 隆夫, 田中 英彦:「開発の早期段階におけるセキュリティアスペクトの抽出」情報処理学会, コンピュータセキュリティシンポジウム(CSS)2007, 11月 2007年.

[7]セキュアRFIDプロトコル概要 日立製作所
http://www.hitachi.co.jp/Prod/mu-chip/jp/pdf_files/secure_p_0906.pdf

[8]村上康二郎「ユビキタス情報社会におけるプライバシー・個人情報の保護」Mobile Society Review 未来心理 Vol. 5, pp. 6 - 13, 2006年3月

[9] 21世紀COE・次世代ユビキタス情報社会基盤の形成 第五回シンポジウム「ユビキタス情報社会と個人情報保護」(2005年)

[10]G.Sindre and A.L. . Opdahl, "Eliciting security requirements by misusecases," in Proc. TOOLS Pacific 2000, 2000, pp. 120–131.

[11] ㈱横須賀テレコムリサーチパーク 国立大学法人東京大学 平成17～19年度文部科学省次世代ＩＴ基盤構築のための研究開発「安全なユビキタス社会を支える基盤技術の研究開発プロジェクト」Secure Ubiquitous Computing Platform 『事後評価』

[12] 総務省第2回ユビキタス健康医療シンポジウム「医療安全への電子タグ応用」秋田大学医学部附属病院

[13]医療事故情報収集等事業第１３回報告書 平成２０年６月１８日 財団法人日本医療機能評価機構 医療事故防止事業部

[14] Fabricio A. Braz .."Eliciting Security Requirements through Misuse Activities DEXA archive"
Proceedings of the 2008 19th International Conference on Database and Expert Systems Application - Volume 00 table of contents pp. 328-333

[15] 澤田忍, 田中 英彦:「医療分野におけるRFIDタグ活用と情報の機密性・完全性の確保」情報処理学会, コンピュータセキュリティシンポジウム(CSS)2008, 10月 2008年.