

# RFID システム運用上のプライバシーについての考察

## A Discussion on Privacy in RFID System

神戸 雅一\*<sup>1</sup>  
Masakazu KANBE

桑田 喜隆\*<sup>1</sup>  
Yoshitaka KUWATA

山本 修一郎\*<sup>1</sup>  
Shuichiro YAMAMOTO

\*<sup>1</sup> 株式会社 NTT データ

NTT DATA CCORPORATION

Because of its technical feature "Contact less", RFID system cannot sweep away the apprehension that the system can be used to collect and use the privacy information wrongly. This apprehension comes to social movement of privacy protection and some problems about adoption of RFID system. In this paper, we order the social and technical problems of RFID system, and discuss on the Privacy Problems in RFID system.

### 1. はじめに

RFID の登場以来、製造業における工程の管理や工場から量販店までの物流管理、オフィス内における人物の位置特定などさまざまな分野において、その応用が実現されつつある。RFID システムの多くは、管理対象とする物品や人物に対しユニークな ID を持つ RFID タグ (電子タグ) を付与し、管理対象に関するさまざまな属性を管理することを目的としている。RFID システムは、RFID タグの物理的な非接触性による複数同時読み取りという特性により、これまでにない大量の情報を実世界から取得することが可能となった。その大量の情報を利用し、人間はこれまでより先緻密な知的活動を実施することができる。

しかしこの RFID の特性により、RFID システム利用者のプライバシー情報が、悪意のある第三者に不正に取得、使用される可能性がある。RFID 関連企業も、プライバシー保護についてはさまざまな技術を提案し、RFID による情報の不正収集防止と、収集された情報の不正利用防止に取り組んでいる。また、政府も「電子タグに関するプライバシー保護ガイドライン」を発表し、RFID タグを用いた情報システムにおけるプライバシー保護基準を明文化している。

しかし、こうした技術的や社会的な取り組みにも関わらず、プライバシー情報のビジネス利用に関する問題は、欧米を中心に現実のものとなっている。RFID の課題は、技術的課題と社会的課題の 2 つがある。技術的課題は、RFID により収集されたプライバシー情報の悪意を持った取得と利用を防ぐことである。社会的課題は、プライバシーの適切な管理を実施しアピールすることで、普及の障害となる不安感を払拭することである。これら課題を解決することが RFID システムの安全な利用と普及には不可欠である。日本では片山による情報科学による安心な電子社会の実現についての研究が進められている。

本稿では、RFID システムの運用に関するプライバシー保護の課題を、知的インフラという観点で RFID システムを分析し、現時点での技術的対策とガイドラインの示す社会的対策を包括して整理し、考察する。

### 2. 知的インフラとしての RFID システムとプライバシー保護技術

本章では個人や組織の知的生産活動に対し、RFID システムがどのように貢献するかを例示し分析すること、RFID システムにおけるプライバシー保護技術の紹介を行う。

#### 2.1 知的インフラとしての RFID システム

図 1 に知的インフラとしての RFID システムを示す。RFID システムも一般的な情報システムと同様に、

- (1) システムに対する情報の入力
- (2) システム内での情報の蓄積
- (3) システム内での情報の処理
- (4) システム内での情報の提示

といったプロセスを経て、人間社会の知的活動の支援を行っている。RFID タグを用いた CRM システムを例にあげると、消費者の商品購入履歴や利用履歴を、RFID タグを利用し収集し、DB に蓄積し、購入履歴等に応じ、消費者に対して新商品のリコメンドを行うことが可能となる。消費者の行動を自動的に収集し、システム側で処理することで、商品リコメンドという知的活動を支援するという点で、RFID タグを用いた CRM システムは知的インフラと呼ぶことができる。本項では RFID を用いた CRM システムを例示し、プライバシー保護に関する課題を整理する。

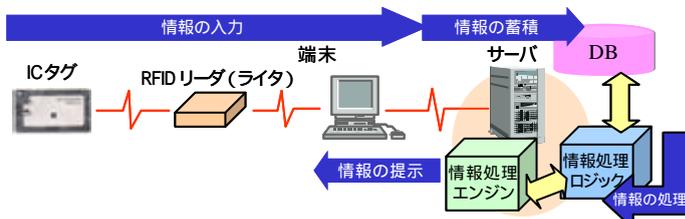


図1 知的インフラとしてのRFIDシステム

#### (1) システムに対する情報の入力

RFID システムにおいては、これまでの情報システムと比較し圧倒的に大量の情報をシステムに対して入力することが可能となる。RFID タグを用いた CRM システムは、RFID タグ付きの商品を購入した際に、購入者、購入商品、購入場所、購入時間などの情報をシステムに入力することも可能となる。さらにシステム設計によっては、家庭内での保管場所、他の商品と組み合わせ利用履歴などもシステムに入力可能となる。こうして RFID システムに入力された情報は、多大なプライバシー情報として扱わ

連絡先 神戸雅一, 株式会社 NTT データ 技術開発本部 システム科学研究所, 〒104-0033 東京都中央区新川 1-21-2 茅場町タワービル, TEL :03-3523-8052, FAX :03-3523-6227, kanbems@nttdata.co.jp

れるため、悪意のある第三者によるプライバシー情報の不正取得への対策が必要となる。

(2) システム内での情報の蓄積

(1)で説明したように RFID システムは、大量の情報を読み取ることが可能である。RFID タグを用いた CRM システムには、大量に入力された情報が蓄積される。RFID システム内の DB に蓄積された情報は、システム的设计によっては、個人を特定する情報と結び付けることができる。ある特定の消費者について紺色のスーツに青いシャツ、グレーのネクタイを合わせることが多いなどといった事実が、システム内に蓄積された情報から判明してしまう可能性がある。悪意を持った第三者によるシステム内に蓄積されたプライバシー情報へのアクセスを防ぐことが必要となる。

(3) システム内での情報の処理

(2)により蓄積された情報を処理し、システムは消費者に対して新商品をリコメンドすることができる。新商品をリコメンドする際に、ユーザが決定したリコメンドのためのロジックや、システム登録ユーザの 20% 以上が購入した商品を推薦するなど、同じシステムを利用しているユーザの挙動などを収集して実行されるロジックが存在する場合もある。消費者がどのようなロジックやパラメータを設定しているかなども、その個人の行動を特定するためのプライバシー情報となる可能性もあるため、第三者からの不正アクセス対策が必要となる。

(4) システム内での情報の提示

システム内での情報処理に応じ、システムは適切な権限を持った利用者に対して情報を提示しなければならない。このため第三者からの不正なアクセスによるプライバシー情報の提示を回避する必要がある。

2.2 RFID システムのプライバシー保護技術

上述したように、RFID システムの運用にはプライバシーの保護を実践するための技術が必要となる。本項では RFID システムにおける具体的なプライバシー保護技術の整理を行う。表 1 は Juels らのまとめた RFID プライバシー保護技術の分類に追

記を行ったものである。表 1 中の 1 から 8 の項目は RFID タグの情報入力に関するプライバシー情報保護技術である。具体的には、RFID タグ内の情報の暗号化や擬似 ID の発生などの技術であり、RFID ベンダが最も注力している不正対策が、RFID タグ情報の不正読取への対策である。

表 1 中 9, 11 は蓄積された RFID 情報を管理するデータベースのアクセスを管理する方法であり、ユーザの権限に基づきデータへのアクセスコントロールをする手法であり、一般的なアクセスコントロールの手法が用いられることが多い。表 1 中の 10 の情報処理ロジックの保護も、第三者による不正な情報処理ロジックへのアクセスを防止する一般的な情報システム手法の利用が現実的であると考えられる。また、RFID リーダ、端末、サーバ間の通信については SSL などの Web サービスの暗号通信技術が適用可能である。

3. ガイドラインに対するソフトゴール分析

3 章では RFID システムを利用する際の、社会的な保護施策の分析を行う。

3.1 政府による電子タグに関するプライバシー保護ガイドライン

平成 16 年 6 月 8 日に総務省と経済産業省から「電子タグに関するプライバシー保護ガイドライン」という文書が公表されている。文書のなかでは、プライバシー保護の必要性が記されており、その必要性の概要を以下にまとめる。

- ・ 個人情報の保護の問題については、電子タグを取り扱う場合においても個人情報保護法の規制を受けることになる
- ・ 個人情報とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他記述等により特定の個人を識別できるものであり、特定の個人に結びつかない情報は個人情報には該当しない
- ・ 個人情報には、他の情報と容易に照合することができ、それにより個人を識別することができることとなるものを含む
- ・ 電子タグについては、その固有の性質が、未だ消費者に十分に認知されている状態でないことから、消費者が保有

表1 :RFIDシステムにおけるプライバシー保護技術

番号	保護ポイント	方法	説明	課題
1	情報入力	Kill Tag	消費者の手に渡る前にKillコマンドでタグを読めないようにする	販売後の商品情報入手が不可
2	情報入力	Hash-lock	RFIDに鍵をかけることで情報を保護する	暗号処理のためのコスト増大
3	情報入力	Re-Encryption	プライバシー強化装置を用いてID番号を暗号化してRFIDに書き込む	コスト増大と外部装置での暗号化による煩雑さ
4	情報入力	Silent Tree Walking	RFIDからID情報を盗聴できないよう暗号化する	暗号処理のためのコスト増大
5	情報入力	Blocker Tag	RFID内のID番号以外の擬似IDを発信し、正当な権限のないリーダにタグを読み取らせない	特殊なリーダのコストが大きい
6	情報入力	Faraday Cage	金属性の籠やホイルで覆い無線信号を遮断する	商品を包み込む形になるため、その用途は限定
7	情報入力	Active Jamming	RFIDリーダに対して妨害電波を発信する	近接するRFIDシステムへの障害
8	情報入力	Soft Blocking	RFIDのモードを、リーダ側から変更することで、局面ごとにタグが発信する情報を変化させる	特殊なリーダのコストが大きい
9	情報蓄積	DB Access Control	RFIDデータが蓄積されたDBへのアクセス制御	正当な利用者の不正への対応が困難
10	情報処理	Logic Control	RFIDシステム内の情報処理ロジックを保護する	正当な利用者の不正への対応が困難
11	情報提示	DB Access Log Audit	RFIDデータのDBに対するアクセスログを監査し、正当な利用者の不正に対応する	不正への即時対応などが困難



果を認知させることに重きを置くことが現実的である。R6 については、RFID タグと個人情報を保存している DB の適切な管理技術が要求されている。また R6 では 2 章で説明した情報処理ロジックの保護を含む対策が要求されていると整理できる。

R7 については、RFID システムに情報を入力する場合の制限として、RFID タグの読み取り保護技術とその適切な運用があげられる。さらに、利用に関する制限も規定されていることから、情報蓄積、情報処理や情報提示に関する技術とその適切な運用も対象となる。R8 については、第三者による RFID タグへの不正書き込み対策技術が対応する。R9 については、情報管理者の設置と適切な運用が対応し、R10 については消費者に対する RFID タグの啓蒙活動が対応している。

RFID におけるプライバシー保護技術の多くは、タグの不正読み取りに対するものであり、RFID タグ内の情報と個人情報を格納する DB との対応付けに関しては、既存の Web システムの情報管理方式を適切に利用することが現時点では現実的である。

## 5. まとめと今後の課題

本稿では、RFID システムを知的インフラとして捉え、情報の入力、蓄積、処理、提示の観点でプライバシー情報保護のポイントを整理した。次に「電子タグに関するプライバシー保護ガイドライン」の分析を行い、プライバシー保護に対するガイドラインを分析し、その概念を整理した。最後にプライバシー保護対策とガイドラインの関係を整理し、プライバシー保護とガイドラインの現状と今後の展開を考察した。今後は一般的な情報システムで利用される DB 上の情報管理とは異なる、RFID システム固有の情報管理方式の提案により、画期的に情報管理効率が向上する可能性について検討する。

また、本稿で例示した消費者のプライバシー保護の観点だけでなく、オフィス内の就業者の行動管理も RFID の重要な応用であると考えられる。これまでオフィス内における RFID の主だった応用は RFID を認証デバイスとして用いた情報へのアクセス制御であった。RFID のアクセス制御利用のほかに就業者の移動履歴などの行動情報管理などを検討し、RFID を用いたオフィス情報のあり方を明確にしていく。この際、就業者の行動情報とプ

ライバシー情報の関係を整理していく予定である。

### 参考文献

- [総務省・経済産業省 2004 年] 電子タグに関するプライバシー保護ガイドライン, [http://www.soumu.go.jp/s-news/2004/pdf/040608\\_4\\_b.pdf](http://www.soumu.go.jp/s-news/2004/pdf/040608_4_b.pdf), 2004 年
- [HBR CASE STUDY 2005 年] HBR CASE STUDY: IC タグを導入すべきか、個人情報の保護に回るべきか, Diamond Harvard Business Review, page121-133. ダイヤモンド社.2005 年 6 月.
- [Juels 2005 年] A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In Computer and Communications Security, pages 103–111. ACM Press, 2003.
- [Juels 2004 年] A. Juels and J. Brainard: Soft Blocking: Flexible Blocker Tag on the Cheap, Proceedings of the 2004 ACM workshop on Privacy in the electronic society, ACM Press, October 2004.
- [Garfinkel 2005 年] S. Garfinkel and B. Rosenberg, RFID: Applications, Security, and Privacy, Addison-Wesley, 2005.
- [Garfinkel 2002 年] S. Garfinkel: An RFID Bill of Rights. Technology Review, page35, October 2002.
- [山本 2005 年] 山本修一郎:「連載 要求工学 第 14 回ゴール分析」, ビジネスコミュニケーション Vol.42, No.12, page 152-156, 2005 年. <http://www.bcm.co.jp/site/2005/2005-12/05-yokyu-12/05-yokyu-12.html>
- [山本 2006 年] 山本修一郎:「連載 要求工学 第 17 回 ゴール分析 応用編」, ビジネスコミュニケーション Vol.43, No.3, page 68-72 2006 年 <http://www.bcm.co.jp/site/youkyu/youkyu17.html>
- [神戸 2006 年] 神戸雅一, 山本修一郎 RFID システム運用におけるプライバシー保護知識の考察, 信学技報, KBSE2005-22, page 7-12, 電子情報通信学会, 2006 年
- [片山 2005 年] 片山卓也, 検証進化可能電子社会-情報科学による安心な電子社会の実現 情報処理, 46 巻 5 号, page 516-521, 情報処理学会, 2005 年

表2 :ガイドラインの概要とプライバシー保護対策

	概要	プライバシー保護対策
R1	電子タグに関するプライバシーを保護する	-
R2	消費者に物品を手交した後も物品に電子タグを装着しておく場合に消費者のプライバシーを保護する	-
R3	物品に電子タグが装着されていることを消費者が認識できる	商品への電子タグ添付の明記
R4	消費者の選択により、物品に装着された電子タグの読取をできないようにする	表1中1-8の情報入力を制限する技術
R5	電子タグの社会的利益等に関する情報提供	消費者に対する読み取り不可能としない条件の認知向上活動
R6	電子タグに対応しDBに記録された個人情報を保護する	表1中9-11の情報処理 蓄積 提示に関する技術
R7	電子タグ内に記録された個人情報に関して情報収集および利用を制限する	表1中1-8の情報入力を制限する技術とその適切な運用 表1中9-11の情報蓄積 処理 提示に対する適切な運用
R8	電子タグ内に記録された個人情報の正確性を確保する	表1中2のRFID内の情報を保護する技術
R9	電子タグ情報を責任者が管理する	情報管理者の設置と適切な運用
R10	消費者が電子タグを適切に取り扱うことができるようにする	消費者に対する電子タグの啓蒙活動