RFID システムのビジネス適用におけるプライバシー保護に関する考察

神戸 雅一　桑田 喜隆　山本 修一郎

株式会社 NTT データ
技術開発本部

東京都江東区豊洲 3-3-9 豊洲センタービルアネックス

e-mail:{kanbems, kuwatay, yamamotosui}@nttdata.co.jp

A Discussion on the Privacy Protection in RFID System for Business Use

Masakazu KANBE, Yoshitaka KUWATA, Shuichiro YAMAMOTO

Research and Development Headquarters
NTT DATA CORPORATION

3-3-9 Toyosu Koutou-ku Tokyo Japan

e-mail:{kanbems, kuwatay, yamamotosui}@nttdata.co.jp

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の分野で，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，それら属性を管理することを目的としている．RFID タグの非接触・複数同時読み取りという特性で，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．RFID システムとは，RFID タグを利用し，現実世界からの大量の情報を取得し，人間にこれまでよりも広範囲なドメインで緻密な活動を支援するシステムである．RFID ビジネスは，RFID システムを利用したビジネス形態のことを指す．

しかし，この RFID の特性と複数の事業者が同じ RFID タグを読み取る相互運用性が実現されることで，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 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収集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緩和することである．技術的・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．

個人情報保護の観点から，企業が業務上必要とするプライバシー情報の不適切な管理体制も企業活動上の多大なリスクとなる可能性が高い．さらに情報科学による安心な電子社会の実現に関する研究も着手され[1)]，RFID システムを運用するために技術面と社会面を包括した対策を検討する下地ができつつある．

本稿では，RFID システムの運用に関するプライバシー保護に関する課題を体系的に分析し，解決方法の検討を行う．これを踏まえて技術的，社会的なプライバシー保護対策を包括した RFID システムのためのプライバシー保護フレームワークの提案を行う．

2. RFID システムの特徴と課題

本章では個人や組織の活動に対し，RFID システムがどのように貢献するかを例示し，その課題を紹介する．RFID システムとは，RFID システム利用者のプライバシー情報を，個人認証用，商品管理用等の RFID タグを用いデータを収集・分析し，RFID 事業者と RFID 利用者との関係性を高めることを目的としたシステムである．代表的な RFID システムとは，図 1 に示したように，決済時に，商品に添付した RFID タグの ID を読み取る．この際，RFID リーダの ID 等により商品の購入場所を特定し，端末を通じ事業者サーバ内のデータベースに，どの商品がどの店舗で，いつ購入されたかという情報を配信する．事業者サーバのデータベース内に蓄積された情報は，後に消費者が来店した際に，個々の消費者の基本情報や購買履歴などからそれぞれの消費者に適したプロモーションを行う材料となる．このプロモーションは FSP (Frequency Shoppers Program）と呼ばれ，企業にとっての消費者価値を最大化し，利益を向上させることを目的として行われている [2)].

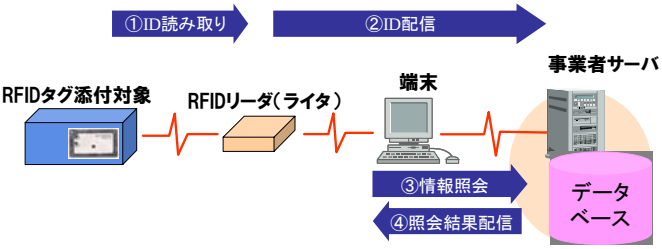

図1：RFIDシステムの処理モデル

RFID を用いた CRM (Customer Relationship Management)システムのなかには, 消費者が購入した商品の利用頻度や利用方法を企業が管理し，プロモーションやマーケティングに役立てるほか，使用後のリサイクル状況の把握など社会的利益を確保するものも考案されている．

オフィス内における就業者の位置管理を行う RFID システムも考案されている [3]. このシステムでは, RFID リーダは一定周期で人物が保持する RFID タグの読み取りを行う. RFID リーダはオフィス内で数メートル間隔に配置され，人物の所有する RFID タグがどの RFID リーダに読み込まれたかをサーバのデータベースに格納する．システムによりデータベースに記録された人物の位置をあらかじめ用意したオフィスマップに表示することが可能となる．オフィス内での就業者の遭遇履歴や動線分析に利用し，オフィスレイアウトの変更時の有効な情報となる．

商品購入後に消費者だけでなく企業や社会全体が RFID タグで取得された情報を利用しビジネスに用いることや，オフィス内での就業者の移動履歴等をビジネスに用いることについては，プライバシー保護を中心としたさまざまな懸念が存在する. RFID システムでは, RFID 利用者のプライバシー情報を扱うことが多く, システム構築時に注意が必要である． RFID システムにおけるプライバシー情報に関する脅威は，図 1 に示した情報処理過程に従い，以下の 4 点に大別される．

1. ID 読み取り：RFID リーダを所有する悪意をもった第三者が不正な ID 読み取りを行う
2. ID 配信：読み取られた ID を正当な事業者以外が盗聴し閲覧する
3. 情報照会：不正な情報照会要求やクラッキングによりサーバ等に蓄積されたプライバシー情報が不正に利用される
4. 照会結果配信：照会結果の盗聴により ID とプライバシー情報の不正な照合が行われる

こうしたプライバシー情報への脅威に向けた対策を, RFID 技術ベンダは複数提案している．しかし RFID システムの構築・運用に対しては技術的対策だけでは不十分であり，社会的な対策も不可欠である．よって，RFID システムにおけるプライバシー情報保護に対して，技術的な対策と社会的な対策を考慮し検討する．

3.RFID システムのプライバシー保護対策の現状

現存する RFID システムの技術的および社会的なプライバシー保護対策の整理を行う．

3.1 RFID システムにおけるプライバシー保護の技術的対策

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 [4][5]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 の項目は図 1 中の① ID 読み取りに関するプライバシー保護技術である．1 から 3 の技術は RFID タグ内の情報を利用者の意志で読み取りを禁止する RFID 不活性化技術である. 4 から 8 は RFID タグ内の情報の暗号化や擬似 ID の発生を施し，第三者による不正な読み取りを防止する技術である．RFID ベンダは，これらに最も最も注力している．

表 1 中の 9 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．10 は蓄積された RFID 情報を持つデータベースのアクセスを管理する一般的な方法が適用される．11 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の改ざんを防止する一般的手法の適用が現実的な解決である．12 の照合結果参照については，データベースのアクセスログを監視するなどして, 消費者の ID と所有製品などのプライバシー情報を不正に照合する行為などを監視する．販売店従業員やシステム管理者等の正当な権限を持った人物が正規のアクセス手段で情報を取得し，不正に利用するといった問題の解決方法もアクセスログの監視などが有効である．

それぞれのプライバシー保護技術に対して効果と課題があり単一の技術的対策だけでは十分なプライバシー保護は困難である．複数の技術的対策の組み合わせだけでなく，社会的な対策の併用が，RFID システムの安全な運用に必要である．

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	技術名	説明	課題
1	ID読み取り	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	ID読み取り	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
3	ID読み取り	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
4	ID読み取り	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
5	ID読み取り	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
6	ID読み取り	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
7	ID読み取り	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
8	ID読み取り	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	ID配信	SSL	RFIDリーダ（ライタ），端末，サーバ間の通信を暗号化して行う	通常のWebサービスの通信の暗号化と同様
10	情報照会	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
11	情報照会	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
12	照会結果参照	DB Access Audit	RFIDデータのDBに対するアクセスを監査し、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

3.2 RFID システムにおけるプライバシー保護の社会的対策

RFID システムの運用については, 複数のガイドラインが公開されており, RFID 事業者はそれらガイドラインを参照し，RFID システムへの適切な運用を実施する．本稿では，代表的な RFID ガイドラインとして，以下の 4 つのガイドラインを整理し, RFID システムに対する社会的対策を分析する．

A. 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) [6]

B. Guidelines on EPC for Consumer Products (EPC Global) [7]

C. Guidelines on Commercial Use of RFID Technology (EPIC: ELECTRONIC PRIVACY INFORMATION CENTER) [8]

D. An RFID Bill of Rights (Girfinkel) [9][10]

A は日本の総務省，経済産業省が公表した文書であり, B は国際 EAN 協会とアメリカの流通コード機関である UCC が共同で所有する非営利法人で，EPC システムの運用管理を行う EPC Global の提示したガイドラインである．C はサイバースペース内のプライバシーについて情報を提供している消費者団体である EPIC が公開したガイドラインであり，D は RFID システム研究者 Girfinkel が公開した RFID に関する見解である．なおガイドライン中には，個人情報とプライバシー情報が区別されているものがある．本稿では， RFID システム内の個人やプライバシーに関わる情報の表記をプライバシー情報に統一する．

4 つのガイドラインを分析し, 19 の項目を抽出した．このガイドラインの規定事項を, RFID システム実現の

ためのプランとした．19 項目を整理し，a から g の 7 つ目標(ゴール)にまとめた．表 2 にガイドラインから抽出したゴールとプランをまとめた結果を示す．以下に RFID ビジネス実現のための目標について説明する．

a .RFID システムの啓発活動

RFID 利用者に対して RFID システムの説明と情報提供を行うことが必要である. RFID システムに対する偏見や誤解を取り除き，RFID システムの効果や脅威を，RFID 利用者に広く伝えることは重要である. 啓発活動により，RFID システムの認知を向上させることは，即効性は期待できないが, RFID システムの普及には不可欠である．ガイドラインでは，特に RFID システムの社会的利益に関する情報提供を規定している. RFID タグ利用者に対して, RFID システムによる管理が生じることを説明するとともに，製品の適切な廃棄やリサイクル状況の管理による社会的利益などを説明することが，RFID システムの啓発活動となる．

b. RFID システムの存在明示

RFID 利用者に対して RFID システムの存在を明示することは重要である．ガイドラインでは，RFID タグの存在や読み取られる可能性を RFID タグ自体や RFID タグ添付商品等に明示することを規定している．このほかに RFID リーダの存在の明示やどのタイミングで RFID タグが読み込まれたかという動作状態を明らかにすることを規定するガイドラインもある．

また, RFID タグ内に記録されている情報を利用者も参照可能とすることを規定しているガイドラインもある. RFID システムの存在を利用者に対して明らかにすることは，利用者に，いつ，どこで，どのような情報が，RFID システムに読み込まれる可能性があるのか，また読み込まれたのかを認知させることになり，RFID システムに対する合意なきプライバシー情報の取得という懸念を緩和することができる．

c. プライバシー情報の利用承諾

総務省・経済産業省のガイドラインでは，個人情報保護法に則し利用目的の本人通知と目的外利用の承諾を規定している．総務省・経済産業省のガイドラインでは利用承諾に関する明確な方法は規定されていないが，EPIC ガイドラインでは，プライバシー情報の利用範囲の承諾を書面で行うことを規定している．プライバシー情報の利用承諾は，プライバシー情報を扱う RFID システムの利用者と事業者の信頼関係に関わる課題である．

d. RFID システムへの参加選択権付与

利用者が入手した商品や配布された RFID タグを不活性化する等の方法で, RFID システムから離脱する権利をすべてのガイドラインで規定している. EPIC ガイドラインでは． RFID 利用者となる可能性がある人に対して，事業者が RFID システムの利用を強要することを禁止している．Girfinkel は RFID システムを利用しないことを選択した人にも, RFID システムの利用者が得られる利益を享受できる措置をとるよう主張している．RFID システムへの参加の選択権を，利用者に与えることで，「RFID システムに参加をしない」という究極的な選択肢が確保される．

e. プライバシー情報のセキュリティ確保

プライバシー情報の正確性の確保は，3 つのガイドラインで規定されている. RFID システム内の利用者のプライバシー情報を正確かつ迅速に維持することは重要である．プライバシー情報の損失，毀損，改竄，漏洩を防止することも重要である．プライバシー情報のセキュリティ確保については, RFID タグの読み取り防

表2：RFIDガイドライン分析による目標（ゴール）とプランの抽出

番号	RFIDビジネス実現のための目標	目標を実現するプラン	総務省・経済産業省ガイドライン	EPC Global ガイドライン	EPIC ガイドライン	Girfinkelの RFID 権利宣言
1	a. RFIDシステムの啓発活動	利用者に対する説明及び情報提供	○	○		
2		RFIDタグの社会的利益に関する情報提供	○	○	○	
3	b. RFIDシステムの存在明示	RFIDタグ装着の明示	○	○	○	○
4		RFIDリーダの存在の明示			○	
5		RFIDリーダの動作状況の明示			○	
6		利用者によるRFID内情報の確認				○
7	c. プライバシー情報の利用承諾	プライバシー情報利用目的の本人通知	○		○	
8		プライバシー情報の目的外利用の承諾	○		○	
9		利用者の同意のない追跡の禁止			○	
10	d. RFIDシステムへの参加選択権付与	RFIDタグの不活性化の選択権付与	○	○	○	○
11		利用者へのRFID利用強要の禁止			○	
12		RFID不利用による機会損失の禁止				○
13	e. プライバシー情報のセキュリティ確保	プライバシー情報の正確性確保	○	○	○	
14		プライバシー情報の損失，毀損，改竄，漏洩の防止	○	○	○	
15	f. プライバシー情報の適切な管理	プライバシー情報の第三者開示禁止			○	
16		情報管理者の設置	○		○	
17		利用者へのプライバシー情報の開示	○	○	○	○
18	g. プライバシー情報の濫用禁止	消費者の要求以外の条件でのプライバシー情報照会の禁止			○	
19		RFIDタグ情報とプライバシー情報DBとの照会規制	○			

止や暗号通信などの技術的な対策が複数提案されているが，技術的な対策だけでなく，事業者の行動監視などといった技術や社会制度的な対策が必要である．

f. プライバシー情報の適切な管理

要求のあった利用者に対し RFID システムが管理するプライバシー情報を開示することが，すべてのガイドラインで規定されている．これは利用者からの情報開示要求が抑止力として働き，事業者が不要なプライバシー情報を保持しないことや適切な管理を厳格に実施することを目的としている．また，情報管理者の設置を規定するガイドラインも存在している．

EPIC ガイドラインでは，プライバシー情報の第三者への開示を禁止するよう規定している．しかし RFID システム内のデータを共同で利用するビジネスモデルも考案されており，実現にあたっては議論が必要である．

g. プライバシー情報の濫用禁止

総務省・経済産業省ガイドラインでは，RFID タグの内部に含まれるプライバシー情報のほか，RFID タグ内の ID と関連するデータベースとの照合に関しても規制している．これは個人情報保護法に合致したガイドラインの項目であり，従業員等の役割に基づいたデータベースのアクセスコントロールで実現される．また EPIC ガイドラインでは，プライバシー情報照会は緊急時を除き禁止し，利用者の同意が得られた場合のみ可とすることで，事業者による利用者のプライバシー情報の安易な利用を規制している．

このように，政府機関，業界団体，消費者団体，学術研究者がガイドラインを公表し，RFID システムの普及に尽力している．ガイドライン公表の目的は，消費者に対して RFID システムの存在，取得情報の明確化，適切なセキュリティ確保をアピールすることである．

4. RFID システムのためのプライバシー保護フレームワーク

3 章で RFID システムの技術的，社会的対策を説明した．本章では，3 章で紹介した RFID プライバシー保護対策をソフトゴール分析 [11] の手法を用いて整理した RFID システムのためのプライバシー保護フレームワークを説明する．

4.1 RFID システムのためのプライバシー保護フレームワーク

図 2 に RFID システムのためのプライバシー保護フレームワークを示す．本フレームワークは，ゴールレイヤ，プランレイヤ，アクションレイヤからなる 3 階層で構成される．ゴールレイヤの構築には，要求工学における主なゴール分析手法のうち，NFR フレームワーク（Non-Functional Requirement Framework）を用いた [12]．NFR フレームワークでは，非機能要求（NFR)の構造を NFR 型と定義しておき，具体的なシステム要求の分析で再利用することが可能となる．ゴールレイヤを表現する目的は，「プライバシーを保護した RFID ビジネスの実現」という最終目標(ゴール)に対して，RFID 事業者の目標を細分化することである．

図 2 のゴールレイヤの最下位に位置する a から g までの 7 つの非機能要求は，表 2 中の RFID ビジネス実現のための目標に相当する．ゴールレイヤはこの最下位のサブゴールを，最上位の「プライバシーを保護した RFID ビジネスの実現」とのあいだで構造化を行ったものである．最下位のサブゴールと最上位のゴールとの関連付けのために，両者のあいだに複数のサブゴールを設定した．その結果が図 2 のゴールレイヤとなる．

図 2 の中段にはプランレイヤが位置する．プランレイヤには，表 2 中の「目標を実現するためのプラン」があり，ゴールレイヤの最下位のサブゴールと対応す

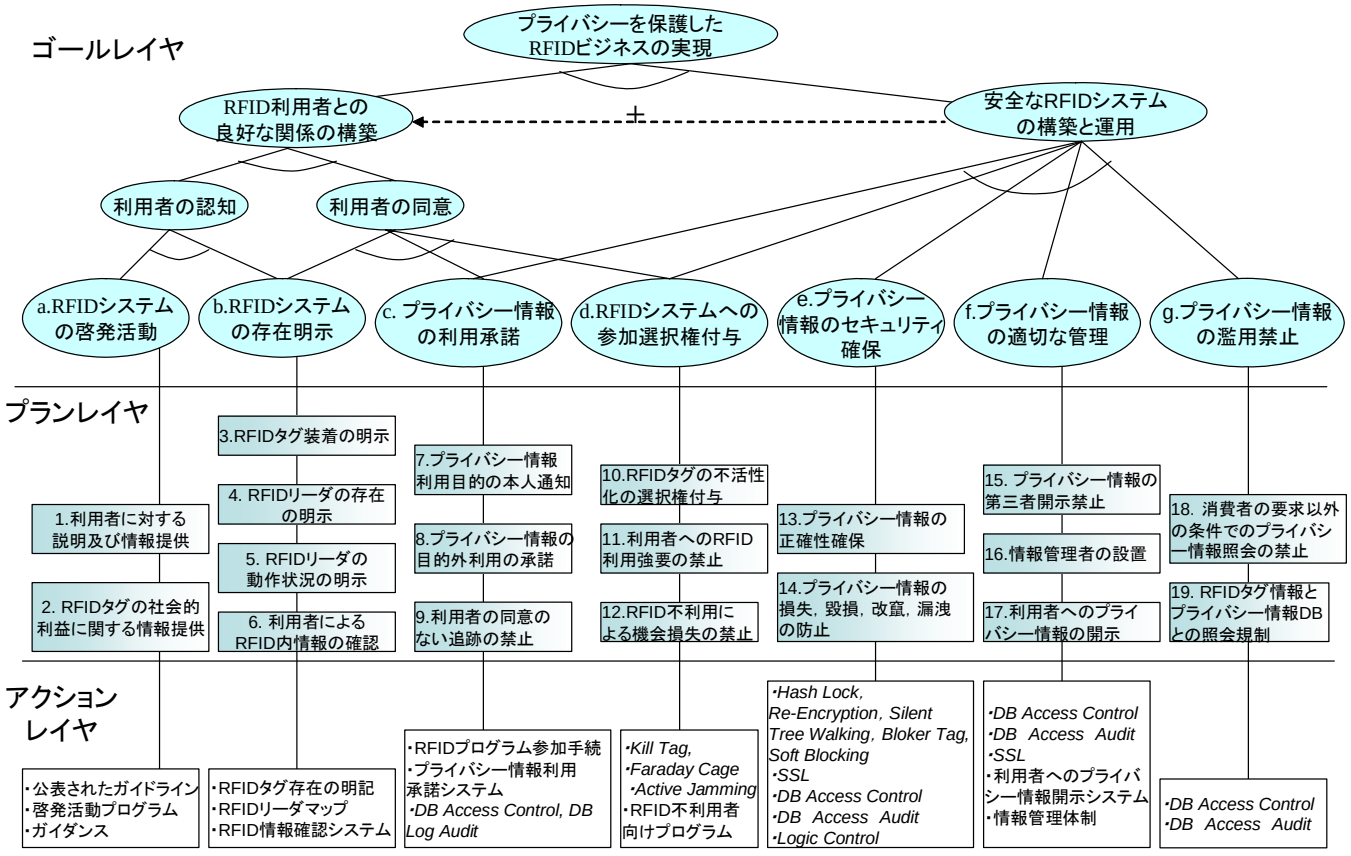

図2：RFIDシステムのためのプライバシー保護フレームワーク

る．プランレイヤを表現する目的は，RFID 事業者が採用すべきプランが十分であるかを確認することである．

図 2 の最下段には，アクションレイヤが位置する．アクションレイヤには，プランを実現するための具体的な手段をあげる．図 2 中のアクションレイヤ内のアクションのなかには，表 1 で説明した RFID システムのプライバシー保護技術が存在する．表 1 中の保護技術を図 2 では斜字体で表現している．それ以外にも，3.2 で紹介したプライバシー保護の社会的対策のうち，事業者の取りうる社会的プログラムや利用者の同意を取るためのシステムなどを実現手段としてあげる．数ある実現手段のなかから，RFID システムの費用対効果やゴールやプランの重要度などにより，実現手段の決定に利用できる．次に三階層の説明を詳細に行う．

①ゴールレイヤ

技術的，社会的プライバシー保護対策を含めた RFID ビジネスを検討する場合に，RFID 事業者は「プライバシーを保護した RFID ビジネスの実現」を最終的なゴールとして設定する．「プライバシーを保護した RFID ビジネスの実現」のために，RFID システムの技術的特徴や社会的受容状態を分析しなければならない．分析の結果，「プライバシーを保護した RFID ビジネスの実現」には，「RFID 利用者との良好な関係の構築」および「安全な RFID システムの構築と運用」が必要である．この両者は AND 条件で存在している．安全な RFID システムの構築と運用があり，RFID 利用者との良好な関係を構築することができる．この 2 つのサブゴールの関係を図 2 中の「＋」マークつきの矢印で表現している．

RFID 利用者との良好な関係を RFID 事業者が構築する場合には．「利用者の認知」と「利用者の同意」を得ることが必要である．この 2 つを，「RFID 利用者との良好な関係」の構築のサブゴールとした．利用者の認知と同意は AND 条件で存在している．「利用者の認知」を高めるために「RFID システムの啓発活動」と「RFID システムの存在明示」の 2 つのサブゴールが AND 条件で存在する．「利用者の同意」については，「RFID システムの存在明示」，「プライバシー情報の利用承諾」，「RFID システムへの参加選択権付与」の 3 つのサブゴールを AND 条件で設定した．

一方，安全な RFID システムの構築については，「プライバシー情報のセキュリティ確保」，「プライバシー情報の適切な管理」，「プライバシー情報の濫用禁止」，「プライバシー情報の利用承諾」，「RFID システムへの参加選択権付与」の 5 つが最下位のサブゴールとなり AND 条件で存在する．

②プランレイヤ

図 2 のプランレイヤは，ゴールレイヤの最下位の a から g までと，表 2 に示した 1 から 17 までの目標を実現するプランを対応付けて表現している．最下位のゴールは，ガイドラインを整理した結果をまとめることで抽出した．よって，最下位のゴールを実現するためにはプランレイヤで示したプランを実現することが必要となる．

③アクションレイヤ

図 2 のアクションレイヤには RFID 事業者が企画する社会的プログラムやシステム，RFID システムのプライバシー保護技術，Web サービスで使われるセキュリティ保護技術，RFID 事業者が取り得る社会的プログラムなどが存在する．これらアクションの選択には，ゴールレイヤの構造やプランレイヤとの関係を分析することが手助けとなる．

RFID システムのためのプライバシー保護フレームワークは，RFID ビジネスの企画時にシステムの開発，運用の要件定義を行う際に，統合的なプライバシー保護対策検討に有効である．ゴールレイヤは，複数のガイドラインを整理し導出されたものであり，これらのゴールを無視し，RFID ビジネスを実施することはガイドラインからの逸脱を意味する．よって，ゴールレイヤを意識しビジネスプランを策定する必要がある．

4.2 RFID システムのためのプライバシー保護フレームワークの有効性

RFID システムのためのプライバシー保護フレームワークとプライバシー保護対策，RFID システムの関係とその有効性を図 3 に示す．

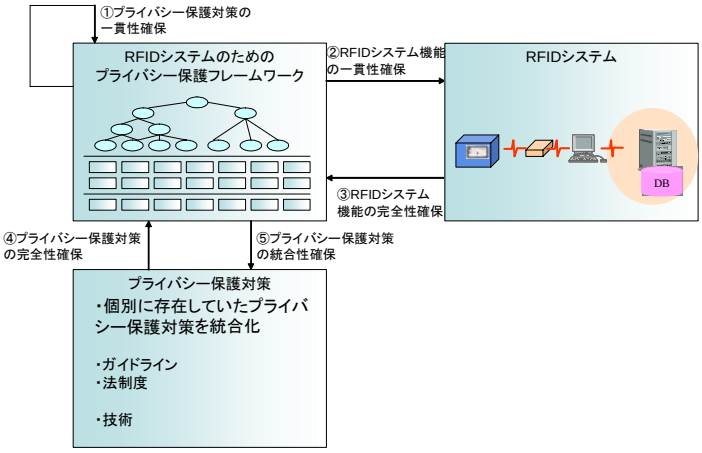

図3：RFIDシステムのためのプライバシー保護フレームワークの有効性

① プライバシー保護対策の一貫性確保

RFID ビジネスの企画時のプライバシー保護対策の一貫性を確保する際に，本稿で提案するフレームワークは有効に作用する．ゴールレイヤ，プランレイヤに従い，ビジネス領域に応じたアクション項目をアクションレイヤに記述することで，RFID システムにおけるプライバシー保護対策を決定することができる．しかし，この際に，プランまたはアクション項目間で競合が発生する場合がある．例えば，プランレイヤの「2.RFID タグの社会的利益に関する情報提供」というプランのアクションである「啓発活動プログラム」に，「RFID 利用者に対するインセンティブの用意」が具体的なアクション項目としてあるとする．このアクションは，プランレイヤの「12.RFID 不利用による機会損失の禁止」の具体的アクションである「RFID 不利用者向けプログラム」と競合する．RFID 不利用者に対し，インセンティブを提供することは，RFID システムの啓発活動の効果を薄めることにつながるからである．RFID 事業者は，それぞれの上位ゴールである「a. RFID システムの啓発活動」と「d. RFID システムへの参加選択権付与」の双方のゴールを検討し，「d. RFID システムへの参加選択権付与」に関連するプランである「10.RFID タグの不活性化の選択権付与」，「11.利用者への RFID 利用強要の禁止」を実施し，双方のゴールを満たすことを検討する．本フレームワークの利用で実現プラン間の競合を上位のサブゴールの分岐構造まで遡ることや，複数のプランから必要なものを選択することで，システムの目標を逸脱せず適切にアクションの競合を解消することが可能となる．

② RFID システム機能の一貫性確保

①と同様に RFID システムの設計段階においても，本フレームワークがアクション項目の競合解消に有効である．たとえば RFID システム内のデータベースに対する厳格なアクセスコントロールを実現するアクション項目を選択し，RFID 利用者の要望に応じたプライバシー情報を提示するアクション項目を選択する場合に，両者は競合することもある．

③ RFID システム機能の完全性確保

本フレームワークは，運用中の RFID システムの評価にも有効である．本フレームワークを利用することで，運用中の RFID システムのプライバシー保護対策がガイドラインに沿った完全なものであるかを確認することが可能である．

④ プライバシー保護対策の完全性確保

本フレームワークは，RFID ビジネス企画時に利用するプライバシー保護対策の完全性を確保することに有効である．RFID ビジネス企画時に，ゴールやプランに合致した現存するプライバシー保護対策を検討する際に，プライバシー保護ガイドラインや法制度，プライバシー保護技術といったプライバシー保護対策アクションの完全性を検討することに利用できる．

⑤プライバシー保護対策の統合性確保

本フレームワークは，現存するプライバシー保護対策の統合性を確保することに有効である．RFID ビジネスを企画した際の内容によっては，現存するプライバシー保護対策ガイドラインを統合して扱うことや，法制度化して拘束力を高めることなども視野に入れる必要がある．統合化によりプライバシー保護対策の能力を向上させることに本フレームワークは有効である．同様に RFID システムのプライバシー保護技術に対して，新規に検討するものがあれば，新技術開発などを提案し，技術的なプライバシー保護対策を向上することもできる．また，ガイドラインや法制度といった社会的対策と RFID システム構築に利用する技術的な対策の組み合わせ方を，フレームワークをベースに検討することで統合性の確保が実現できる．

個別の企業が公開するプライバシー条項の内容を比較・分析し，その傾向をまとめ標準化を狙った研究は存在する [13]．しかしプライバシーを保護したビジネスシステムの導入に向けて，技術的・社会的対策を網羅的に分析することされていない．RFID システムの構築やプライバシー対策全般に対して有効性を発揮する本稿のフレームワークは存在せず新規な取り組みである．

5. RFID ビジネスのためプライバシー保護フレームワークの評価

フレームワークの有効性について評価を実施する．5.1 では，CRM システム企画に関するケーススタディを題材にし，5.2 では就業者位置管理システムを題材に評価を行う．

5.1 CRM システム企画時の評価

本項では，HBR 誌のケーススタディで紹介されたコメントを RFID ビジネスのためのプライバシー保護フレームワークに対応させ，必要な情報を追記し評価を行う．HBR 誌で紹介された CRM システムのケーススタディは，FSP を積極的に導入する意向を持ったアパレルブランドの依頼を受けて，RFID ベンダが RFID の導入を推進するか，プライバシー情報保護を主張するかについてコメントを求めるものであった．この事例を本稿で取り上げた理由は，RFID を用いた CRM ビジネスに対し，多面的なコメントが挙げられていたからである．ケーススタディで取り上げられた事例の要点を以下に記す．

■ ティーン向けのアパレルブランドの視点
- 物流管理に RFID タグを利用している．
- 更なる事業の効率化を目指し，人気商品に RFID タグを装着することの検討を開始した．
- 商品への RFID タグの装着が実現すれば需給計画，在庫調整，商品開発を効果的に実施できる．
- さらに消費者に適切な商品を推薦することができ，適切な顧客管理が実施できる．

■ RFID ベンダの視点
- アパレルブランドのアイデアを実現できれば業界内の評価を高められ魅力的である．
- 法律面，倫理面でかなりの不安を感じている．

■ ケーススタディの要求事項
- RFID ベンダはアパレルブランドの要求にどう対応すべきかについて，4 名の識者にコメントを求めている．

4 章で紹介した図 2 の RFID ビジネスのためのプライバシー保護フレームワークに，CRM システムの事例を当てはめ説明する．表 3 は RFID ビジネスのプライバシー保護フレームワークにより，CRM システムに必要なプライバシー保護機能をアクションとして規定したものである．表 3 のアクションのうち，*印が付いているものは HBR 誌のケーススタディのコメントで紹介されていたものである．それ以外は，著者らが CRM システムの構築に必要であるものを追記した．CRM システムを RFID システムとして実現するためには，さまざまなアクションを選択することになる．RFID 事業者が選択するアクションは，社会的なプログラムから RFID タグの不正読み取り技術の防止などさまざまなプライバシー保護対策が含まれる．表 3 をもとに，RFID ビジネスのためのプライバシー保護フレームワークの有効性の評価を行う．

①プライバシー保護対策の一貫性確保

表 3 中の具体的アクションである 2 の「奨学金などの公的インセンティブシステム」と 12 の「RFID 不利用消費者へのインセンティブ確保」は，RFID 不利用者に対する奨学金プログラムの提供により，RFID 利用者への奨学金プログラムの効果との差別化ができないことから，競合するアクションとなる．導入に際しては，事業者の判断が必要である．判断の際には，図 2 のフレームワーク内のゴールレイヤまで遡り，サブゴールである利用者の認知と利用者の同意のバランスについて検討する必要がある．社会全体での認知度を徹底的に向上させるのであれば，奨学金プログラムを徹底的に実施する必要があるが，RFID 不利用者まで奨学金プログラムの対象にしてしまうのであれば利用者の認知に対するアクションの効果が薄れる．RFID 事業者は，CRM プログラムを企画する段階で本フレームワークを利用し，アクション間での競合関係を見つけ，競合に対する対策をサブゴール間での調整を行うことができる．よって本フレームワークはプライバシー保護対策の一貫性確保という点で有効である．

② RFID システム機能の一貫性確保

CRM システムを実現する上でのプライバシー保護

機能は，表 3 に体系的に記載した．さらに，表 3 中の 14 の暗号通信技術の採用, RFID の不正読み取り技術，データベースへのアクセス制御と 17 の利用者へのプライバシー情報開示機能は，利用者の認証手段にセキュリティ上の問題がある場合に，プライバシー情報の漏洩につながり，機能の一貫性確保に不合理が生じることとなる．本フレームワークの利用により，CRM システムの利用者認証に対して強固な対策を用いなければ CRM システム機能の一貫性確保が十分に行えないことが示される．

③ RFID システム機能の完全性確保

フレームワークに基づき，実装されたシステムの機能が十分であるかどうかを評価することができる．本稿で扱う CRM 事例は，HBR 誌のケーススタディの範囲を出ていないため，実際の CRM システムが機能を十分に満たしているかを判断することはできない．しかし，実際に構築されたシステムの機能完全性の評価に，本フレームワークを用いることは可能である．詳細は 5.2 項で説明する．

④ プライバシー保護対策の完全性確保

表 3 中の具体的なアクションには，フレームワークのアクションレイヤに記述されている技術的・社会的対策に分類される項目が記載されており，プライバシー保護対策の完全性が確保されていることが確認された．しかし，技術面・社会面を含む新たなプライバシー保護対策が提案された場合には，フレームワークの変更を行う必要がある．プライバシー保護対策の完全性確保という点においても，フレームワークは固定的なものではなく, 常に進化し続けることが必要となる．

⑤ プライバシー保護対策の統合性確保

本フレームワークに基づき，プライバシー保護対策の統合性確保を行うことが可能となる．フレームワークには既存の RFID システムに関する主要なガイドラインや, RFID システムのプライバシー保護技術が含まれており, 現時点での統合性の確保は検証できている．統合性の確保とは，個別に存在している RFID システムのプライバシー保護対策を統合することである．

5.2 就業者位置管理システムの評価

オフィス内の就業者位置管理システムを題材にした③RFID システム機能の完全性確保を行った結果を表 4 に示す. 6 の利用者による RFID タグ内の情報の確認，13 のプライバシー情報の正確性確保，17 の利用者へのプライバシー情報の開示のアクションが, RFID システムとしてフレームワークに対して十分な対応ができていない点が判明した．フレームワークによりシステム機能の不足を抽出することが可能と言える．本フレームワーク中に存在しない機能を RFID システムが有している場合には，フレームワークの変更を行う必要がある．フレームワークは固定的なものではなく，常に進化し続けることで, RFID システム機能の完全性を確保できることとなる．

6. まとめと今後の課題

本稿では, RFID システムのプライバシー保護対策の技術面，社会面を体系的に調査し，RFID システムのためのプライバシー保護フレームワークの提案を行った．RFID システムのうち CRM システム，オフィスにおける就業者位置管理システムに対し評価を行い提案したフレームワークの評価を行った．その結果，CRM システム企画時の①プライバシー保護対策の一貫性確保，②RFID システム機能の一貫性確保, ④プライバシー保護対策の完全性確保，⑤プライバシー保護対策の統合性確保についての確認を行った. ③RFID システム機能の完全性確保については，実システムを想定したオフィスにおける就業者位置管理システムに対して実施した．この結果，RFID システムの機能の完全性確保に対し，複数の機能に関する不足事項を確認することができた．

本稿で提案したフレームワークは，プライバシー保護を考慮した RFID システムの構築に対して有効であ

表3：RFIDガイドライン分析によるプライバシー保護フレームワークの評価（CRMシステム）

番号	RFIDビジネス実現のための目標	目標を実現するプラン	具体的なアクション
1	a. RFIDシステムの啓発活動	利用者に対する説明及び情報提供	消費者のRFID理解度チェックシステム*、業界内での自主基準の策定と公表*
2		RFIDタグの社会的利益に関する情報提供	奨学金などの公的インセンティブシステム*
3	b. RFIDシステムの存在明示	RFIDタグ装着の明示	商品への電子タグ装着の明記*
4		RFIDリーダの存在の明示	店内でのRFIDリーダ設置箇所および読み取り範囲の明示
5		RFIDリーダの動作状況の明示	店内でのRFID読み取り音や読み取りインジケータ表示機器
6		利用者によるRFIDタグ内情報の確認	消費者宅などでのRFID情報確認システム、消費者向けRFIDリーダの配布
7	c. プライバシー情報の利用承諾	プライバシー情報利用目的の本人通知	販売時におけるプライバシー情報の利用目的通知
8		プライバシー情報の目的外利用の承諾	プライバシー情報の目的外利用に対する承諾確認システム
9		利用者の同意のない追跡の禁止	事業者のプライバシー情報利用監視機能*
10	d. RFIDシステムのへの参加の選択権付与	RFIDタグの不活性化の選択権付与	商品から簡単に除去できるRFIDタグの使用、KILL Tagなどの RFID不活性化技術
11		利用者へのRFID利用強要の禁止	RFID不添付商品の販売*
12		RFID不利用による機会損失の禁止	RFID不利用消費者へのインセンティブ確保*
13	e. プライバシー情報のセキュリティ確保	プライバシー情報の正確性確保	データベースへのアクセス制御、事業者のプライバシー情報利用監視*
14		プライバシー情報の損失，毀損，改竄，漏洩の防止	暗号通信技術の採用、RFIDの不正読み取り技術，データベースへのアクセス制御
15	f. プライバシー情報の適切な管理	プライバシー情報の第三者開示禁止	事業者のプライバシー情報利用監視機能*
16		情報管理者の設置	情報管理者の設置、データベースへのアクセス制御
17		利用者へのプライバシー情報の開示	消費者へのプライバシー情報開示機能
18	g. プライバシー情報の濫用禁止	消費者の要求以外の条件でのプライバシー情報照会の禁止	事業者のプライバシー情報利用監視機能*
19		RFIDタグ情報とプライバシー情報DBとの照会規制	CRMシステムの利用制限機能

るが，実システムの機能の完全性確保を実施する点今後の課題である．提案したフレームワークについて，そのベースとなった RFID システムにおけるプライバシー保護技術および RFID システムのためのプライバシー保護に関するガイドラインは進化する．それらの進化に応じてフレームワークも変化することが重要である．

[引用文献]

1) 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，Vol.46, No.5, pp.515-512 (2005).
2) 助田浩子，大関一博，堀井洋一：Anonymous CRM ー顧客匿名性を考慮した顧客情報分析システムー，情報処理学会論文誌，Vol.47, No.3, pp658-665 (2006).
3)白樫和明，桑田喜隆，相原 理，藤本 浩，本条啓史：ユビキタスで新しいライフスタイルを創造する「ユビスタイル」, 第 19 回日本人工知能学会全国大会, 2C3-06 (2005).
4) A. Juels, R.L.Rivest, and M. Szydlo:The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy, In Computer and Communications Security, pp103–111, ACM Press, (2003).
5) 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).
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,
http://www.soumu.go.jp/s-news/2004/pdf/040608_4_b.pdf (2004).
7) EPC global：Guidelines on EPC for Consumer Products, http://www.epcglobalinc.org/public/ppsc_guide/ (2005).
8) EPIC: Guidelines on Commercial Use of RFID Technology, http://www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf (2004).
9) S. Garfinkel and B. Rosenberg, RFID: Applications, Security, and Privacy, Addison-Wesley, 2005.
10) S. Girfinkel: An RFID Bill of Rights, Technology Review, pp35, October 2005.
11) L.Chung, B.Nixon, E.Yu, J.Mylopoulos: Non-Functional Requirements in Software Engineering, Kluwer Academic Publishers (2000).
12) 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, pp 152-156, (2005).
13) A. I. Anton, J. B. Earp, Q. He, W. Stufflebeam, D. Bolchini and C. Jensen: Financial Privacy Policies and the Need for Standardization, IEEE SECURITY & PRIVACY, pp36-45, IEEE COMPUTER SOCIETY (2004).
14) DAIAMONDO　ハーバード・ビジネス・レビュー：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, pp121-133.ダイヤモンド社.2005 年 6 月.

表4：RFIDガイドライン分析によるプライバシー保護フレームワークの評価（就業者位置管理システム）

番号	RFIDビジネス実現のための目標	目標を実現するプラン	具体的なアクション
1	a. RFIDシステムの啓発活動	利用者に対する説明及び情報提供	就業規則への記述、就労者に対するガイダンスの実施
2		RFIDタグの社会的利益に関する情報提供	ガイダンスにおける想定する利用効果の説明
3	b. RFIDシステムの存在明示	RFIDタグ装着の明示	就労者が装着するタグの性能の説明
4		RFIDリーダの存在の明示	オフィスマップ内におけるRFIDリーダの存在明示
5		RFIDリーダの動作状況の明示	リーダの読み取り時間間隔の説明
6		利用者によるRFIDタグ内情報の確認	*未実施*
7	c. プライバシー情報の利用承諾	プライバシー情報利用目的の本人通知	システム参加時におけるプライバシー情報の利用目的通知
8		プライバシー情報の目的外利用の承諾	プライバシー情報の目的外利用に対する承諾確認ルールの設定
9		利用者の同意のない追跡の禁止	オフィスや会議室内のみでのタグの読み取りの遵守
10	d. RFIDシステムのへの参加の選択権付与	RFIDタグの不活性化の選択権付与	位置情報を知られたくない場合の方法の説明
11		利用者へのRFID利用強要の禁止	不参加ルールの策定と運用
12		RFID不利用による機会損失の禁止	RFID不利用就労者への他の就労者の位置情報提示
13	e. プライバシー情報のセキュリティ確保	プライバシー情報の正確性確保	*データベースの性能でリアルタイム表示が行えない場合がある*
14		プライバシー情報の損失，毀損，改竄，漏洩の防止	暗号通信技術の採用、RFIDの不正読み取り技術
15	f. プライバシー情報の適切な管理	プライバシー情報の第三者開示禁止	事業者のプライバシー情報利用監視機能
16		情報管理者の設置	情報管理者の設置、データベースへのアクセス制御
17		利用者へのプライバシー情報の開示	就業者のオフィス内での位置情報の提示、*就業者の位置情報ログの提示（未実施）*
18	g. プライバシー情報の濫用禁止	消費者の要求以外の条件でのプライバシー情報照会の禁止	事業者のプライバシー情報利用監視機能
19		RFIDタグ情報とプライバシー情報DBとの照会規制	データベースへのアクセス制御、運用者のプライバシー情報利用監視