普及促進・社会受容性検討推進に関する成果報告書

平成１９年 ３月

次世代電子商取引推進協議会

はじめに

電子タグの利活用を普及・促進していくためには、タグの用途開発やコスト削減、ビジネスモデルの開発などもさることながら、来るべき大量普及の時代を念頭に、それを担保するべく、プライバシー問題を中心とした「社会受容性の確保」についての検討が欠かせない。

当 WG としては、メーカーから消費者をつなぐサプライチェーン全体でトレーサビリティ推進をとらえた場合、その中でも電子タグの利活用において、消費者接点以降に発生する様々な課題について、これを社会受容性の問題として捉え、普及促進のためには、どのような施策を講じたらいいのかという点について調査・検討した。

また社会受容性の検討にあたっての基本スタンスとしては、電子タグの普及促進・市場定着のためには、この新技術によって企業が提供する様々なサービスへの消費者からの信頼の確保が重要なテーマとなることを前提にした上で、以下の 2 点を前提とした。

①電子タグの普及阻害要因除去のためには、プライバシーや個人情報の保護を含む全般的な消費者保護と啓発が不可欠である

②消費者の保護・啓発の推進が、社会インフラを変革する可能性を秘めた電子タグという将来有望な新技術・サービスの普及・定着に資する

従って、電子タグの普及促進の進展を目指して、その利活用における消費者保護の方策の検討が当 WG の活動目的である。付け加えるならば、企業側にとっては、電子タグ関連事業推進の一環として、消費者からの素朴な疑問や問い合わせに対応することも大切であり、これを踏まえた「安心安全なサービスの提供」としての電子タグの普及促進も目指している。

本報告書は、電子タグの普及にあたって社会受容性の立場からの検討を行った活動成果をまとめたものである。電子タグの普及に携わる多くの方々の参考となれば幸いである。

平成 19 年 3 月

次世代電子商取引推進協議会

<普及促進・社会受容性検討推進ワーキンググループ名簿(順不同・敬称略)>

(主査)

合原　英次郎	松下電器産業株式会社

(顧問)

松本　恒雄	一橋大学大学院

(有識者)

阿南　久	日本生活協同組合連合会
岩田　修	株式会社オフィスイワタ
原田　由里	有限責任中間法人 EC ネットワーク
内匠　康博	旅行電子商取引促進機構

(委員)

高橋　　衛	株式会社三菱総合研究所
小林　雄一	株式会社日立製作所
赤塚　元	凸版印刷株式会社
岩間　研二	三菱電機株式会社
荒木　吉雄	日本アイ・ビー・エム株式会社
芋生　信一	三菱電機インフォメーションシステムズ株式会社
寺浦　信之	株式会社デンソーウェーブ
川崎　誠一	大日本印刷株式会社
佐藤　治道	東京電力株式会社
湯川　栄治	株式会社 CSK システムズ
森田　浩司	株式会社 CSK システムズ
斉藤　典明	日本電信電話株式会社
榎本　昭彦	JFE システムズ株式会社

(オブザーバー)

遠藤　良樹	経済産業省　商務情報政策局　情報経済課
武田　賢治	日本生活協同組合連合会

(事務局)

松本　孝志	財団法人流通システム開発センター
石川　靖文	次世代電子商取引推進協議会
若泉　和彦	次世代電子商取引推進協議会

<消費者啓発基盤検討タスクフォース名簿(順不同・敬称略)>

(リーダー)

岩田　修	株式会社オフィスイワタ

(サブリーダー)

小林　雄一	株式会社日立製作所

(メンバー)

阿南　久	日本生活協同組合連合会
赤塚　元	凸版印刷株式会社
岩間　研二	三菱電機株式会社
荒木　吉雄	日本アイ・ビー・エム株式会社
芋生　信一	三菱電機インフォメーションシステムズ株式会社
寺浦　信之	株式会社デンソーウェーブ
湯川　栄治	株式会社 CSK システムズ
森田　浩司	株式会社 CSK システムズ
榎本　昭彦	JFE システムズ株式会社

(事務局)

石川　靖文	次世代電子商取引推進協議会
若泉　和彦	次世代電子商取引推進協議会

<消費者啓発 HP 検討タスクフォース名簿(順不同・敬称略)>

(リーダー)

高橋　　衛	株式会社三菱総合研究所

(サブリーダー)

内匠　康博	旅行電子商取引促進機構

(メンバー)

原田　由里	有限責任中間法人 EC ネットワーク
川崎　誠一	大日本印刷株式会社
佐藤　治道	東京電力株式会社
斉藤　典明	日本電信電話株式会社

(事務局)

石川　靖文	次世代電子商取引推進協議会
若泉　和彦	次世代電子商取引推進協議会

目 次

1. WG 活動の背景と内容

1.1 電子タグを取り巻く状況

海外での状況に比べて日本国内では、現在まだ電子タグによる個人情報保護やプライバシー侵害を巡る議論が、それほど表面化していない理由としては、そもそも国民自身の持つプライバシーに対する考え方や消費者意識の違い等が欧米との相違として挙げられる。

また、電子タグの現在の国内における導入パターンが、各業界の実証実験や実際の企業単位における電子タグ稼動システムを主流としており、消費者接点となる店舗フロントでの導入よりも、バックヤードとしての物流・在庫管理の事例がまだまだ多いことが原因として挙げられる。
ただ、これから電子タグを利活用する企業やベンダーといった事業者は欧米で実際に起こった消費者団体の電子タグ装着への反対運動の本質やその影響、それに訴訟や導入中止による経済的な影響力がどれくらいあったか等を十分に認識した上で、電子タグに対する事業展開をする必要がある。

特に最近の傾向としていよいよ、電子タグが消費者と接点を持つ様な場面での使用が本格化するにつけ、つまり電子タグが、社会インフラ全体に対して普及・浸透の局面で、この社会受容性の課題は国内においても少なからず問題になると予測される。

また実際に、国内の消費者団体の方々が、どのように思っているかについては、本年度のこのWG の大きな推進テーマの一つとして取り上げることにした。したがって、各団体へ当ワーキンググループのメンバーが直接訪問して、各団体の抱いている電子タグに対するイメージ・感触・意見等についてヒアリングをすることと、その際に当 WG として考える電子タグの概要説明を行って、それに対する各団体の生の声をお聞きして、後述の電子タグ普及のポータルサイト・ホームページの作成に活用・反映しようとする活動を推進した。

それから最近話題となっている日経コンピュータのニュース記事（2007/02/13）によると、電子タグが消費者と接点を持つ様な場面での顕著な使用例としては、「家電製品の出荷から修理まで」というテーマで、大手の家電量販店が電子タグの公開実験、「電子タグを埋め込んだ書籍を初めて消費者に直接販売する」、出版業界の 4 回目の実証実験実施等が挙げられる。

前者の大手家電量販店の取組内容としては、メーカーの製品出荷時から、製品の販売、消費者の手に渡ったあとの修理業務までの一連の業務で、電子タグを利用する実証実験の模様を公開し、薄型ディスプレイや録画レコーダの製品保証書に電子タグを貼り付け、記録したデータを商品の流通過程で読み取って、各業務を効率化するというもので、同様の実験を、その他の量販店も続いて実施した。

この実験は、大きく二つの観点で実施され、一つ目は、物流における、回収対象品の発見作業を効率化することであるが、消費者接点という観点では、製品修理業務の効率化がポイントである。量販店の店舗で、顧客が持ち込んだ製品の修理を受け付ける際に、これまでは紙の伝票で管理していたが　今回からは保証書に貼った電子タグのデータを読み取ると、製品の型番や、販売時に記録した販売日などが、修理受け付けシステムに自動的に登録されるというものである。

後者の出版業界での実験は、電子タグをコミックスの背表紙の裏に埋め込んで初めて一般に発売した。電子タグに格納した管理番号などにより、カバンに入れている書籍の名前が外から分か

るといったプライバシー上の懸念ため、今回の実験ではプライバシー上の問題が起こらないように十分配慮し、店頭にコミックスを並べる前に、国際規格 Gen 2 対応の電子タグが持つ「キル」機能を使い、すべての電子タグの機能を停止させた。

電子タグを店頭で使う実験は他の書店でも実施している。電子タグリーダーを棚に取り付けたスマートシェルフを使い、店頭で消費者が手に取った回数を書籍ごとに数えて、その数と売り上げの関連を調べるといった実験である。

実は、この実験は、米国においてウォルマートが髭剃りメーカーのジレットと提携して 2003 年に実施した内容と同じものである。米国では、その折、消費者団体の反対を懸念して、ウォルマートが実験を自主的に中止したと言われている、いわく付きの実施内容である。

ただ､今回は今年度で 4 回目となる経済産業省支援の電子タグ実証実験の一環ということもあり、国内では、消費者団体による反対運動などは現状では起こっていない。

1.2　社会受容性検討が必要な背景

ただし、国内の現状がそうであるからといって、それに対して何もせず放置することは、将来の電子タグ本格利用やグローバル展開を考えた場合は得策ではない｡特に消費者保護の立場から、その社会受容性を検討していくことは、その普及促進をめざすためには、最重要な課題である。そもそも、単に企業と比べた場合に消費者が、社会的に弱者となるケースが多いだけでなく、電子タグ関連の事業者・利用者側といった関連する各プレーヤー全般を見渡しても、顧客＝最終エンドユーザーとしての消費者に受け入れてもらわなければ、そのシステム自体が社会的に普及するはずがない。

従って社会受容性・消費者保護という観点から見た場合、第一の課題としては、欧米でも問題となっている、電子タグを付けた商品が流通すると、当該商品に関連する個人情報が盗まれる可能性があるといったプライバシー侵害等を懸念する消費者団体の根深い反対論議があるのは周知の通りである。

そのため、自主規制や保護ガイドライン等のマネジメント上の対策だけでなく、純粋に技術的観点からもさらなる保護方式の検討が必要であり、これについては最新の海外の文献も参照しながら昨年に引き続き、当 WG の活動の柱の一つとして、検討の推進を行った。

ただ電子タグが実際に製品に装着されて、消費者の手にわたる段階では、プライバシー以外にも検討すべき課題が山積みといっても過言ではない。第二の課題として、卑近な例としては、昨年の報告書で、電子タグ利活用の事業者向け指針との取り上げた無線機器の人体及埋め込み医用機器への影響である。またサービス・リサイクルユース場面での普及以外にも環境という観点からは、第三の課題として電子タグが大幅活用されて、大量廃棄されるような時代にはタグ廃棄物そのものの環境面への影響があるとの指摘もある。

以上、このように普及促進のための社会受容性・消費者保護の観点からは、プライバシー問題だけでなく、まだまだ様々な検討課題がある。ただ、当 WG としては、その課題の中でも、主に下記の三点の項目を取り上げて具体的に推進した。また、その内容については、主要な活動状況や成果を、次章以下で述べる。

①電子タグに対する消費者の利用シーンの検討及び各消費者団体のイメージ・感触・意見のヒ

アリングと配布用パンフレットの制作
②電子タグ利活用時の、プライバシーや個人情報の保護に対する技術的対策の掘り下げと検討
③電子タグに対する消費者啓発のための情報発信ホームページのリニューアルと改善

2. 電子タグ普及のための消費者啓発

2.1 電子タグ普及のために必要となる消費者啓発

昨年(平成 17 年度)に引続き、電子タグ普及のために行うべき、消費者への啓発内容に関して WG 内の普及・啓発基盤検討 TF(TF1)として検討を行った。

2.1.1 普及･啓発基盤検討 TF(TF1)の活動

本 TF1 として本年度は次の 3 つの活動を行った。

a．消費者側の電子タグに関する正しい理解への方法の検討とパンフレットの作成

電子タグは来年頃から本格的に日本でも普及していくと予想されており、現在はその準備段階と考えられる。現状では一般消費者の電子タグに対する認知度はまだまだ低く、利活用の実態も理解されているとは言いがたい。

しかし逆に考えれば、今のうちに電子タグに関する正確で公平な知識を広く訴求する事で、多くの消費者が正しく理解し、普及への混乱が減少すると期待される。

ECOM では、昨年度、ECOM ホームページ上に「やさしい IC タグ入門」を構築し消費者への情報提供を開始したが、より広く情報を提供する為に紙媒体のパンフレット「やさしい IC タグ入門」を作成し配布を開始した。

b．電子タグの利活用と消費者メリットの訴求方法の検討と消費者関係有力団体ヒアリング

消費者が正しく理解するためには、具体的な電子タグの利活用のシーンを分かりやすく説明し、それによって消費者にメリットがあることを訴求する必要がある。この為、認知度の低い電子タグに対して、現時点で消費者がどのような理解や期待、懸念を持っているかを知る必要がある。

そこでいくつかの消費者関係有力団体との間で意見交換会や勉強会を開催すると同時に率直な意見や疑問、懸念の項目を調査した。またその調査内容を前述のパンフレット作成において文面やキャラクター表現などに反映させた。

c．消費者のプライバシー確保や医療機器への影響、環境への配慮に関する問題点の考察

電子タグが普及すると共に、プライバシーの確保に対する懸念や、ペースメーカーなどの医療機器への影響、地球環境への負荷など種々の問題点が挙がっており、前述の消費者関係有力団体ヒアリングでの調査内容をもとに、前述のパンフレット内にこれらの項目を記述した。

2.2 消費者関係団体との意見交換会や勉強会の開催

消費者関係団体ヒアリングは、平成 18 年秋に次の 3 団体に対して行った。

・社団法人全国消費生活相談員協会
・日本生活協同組合連合会
・　全国消費者団体連絡会

消費者関係団体の方々との意見交換会や勉強会は、次の次第にて行い、数多くのコメントを頂いた。

・ECOM 活動の紹介
・電子タグ関連で最近の報道事例の紹介

出版関係：NHK 放映、各種の利用シーンとビジネス展開：テレビ東京 WBS 放映

・ECOM HP「やさしい IC タグ入門」の内容紹介

・　意見交換会、勉強会および質疑応答

2.2.1　社団法人全国消費生活相談員協会意見交換会

社団法人全国消費生活相談員協会の意見交換会は、以下の日程にて行った。

・訪問日時：2006/09/15

・参加者：生活相談員協会 13 名、国民生活センター 2 名

・項目

全体的な感想：	4 項目
素朴な反対意見：	5 項目
疑問：	12 項目
要望：	3 項目
提言：	2 項目

【全体的な感想】

(1) 保護の方法も沢山あって目的に応じて使い分ける必要があるということがよく分かりました。

(2) またプライバシーを保護する手段があると知って安心しました

ECOM コメント：

・保護技術については、現在もいろいろな方式が開発中です。

・問題は費用との関係で、運用上、何をどう、どこまで使うかということになります。

(3) ブランドものの真贋判定には電子タグが必要と思われます

ECOM コメント：

・ブランドデザインはイタリアなりフランスなりで行われても、実際の生産地は中国であることが多いため素材も加工者も同じで出口が違うという事態が起こっている。これを防ぐにはタグは有効です。

・宝石などでも使われているケースがあります。

(4) ドイツなどに行っても、食品のトレーサビリティということがいわれていて、店頭で生産者や流通履歴が分かるようになっている。安心・安全ということでは素晴らしいことで、それが電子タグを使うことで実現するのであればとてもよいでしょう

ECOM コメント：

・食品のトレーサビリティは、農林水産省などで行っています。ECOM の「平成 16 年度報告書」でも一部調査を行っています。

・トレーサビリティは、必ずしも電子タグだけでなく、バーコードなどを使っても実現可能でそのような試みもなされています。

・電子タグは機能的には極めて便利ではあるが、タグ自体のコストやシステムコストが嵩むのが大きな課題で、それを吸収するビジネスモデルを考案する必要があります。

【素朴な反対意見】

(1) 自分の知らない内に(企業に)情報を取られてしまうのはいやです

ECOM コメント：

・電子タグを使用することによって取得される個人情報は、クレジットカードを使用した際に取得される内容を超えるものではないとご理解ください。

・現状では、商品につけられた電子タグに個人情報を記載することは先ずないと言ってよいが、むしろクレジットカードの方が商品購入情報と個人情報とが、企業内システムで紐付けされるという意味では危険と考えられます。

・「平成 17 年度報告書」の「プライバシーセンシティブな情報項目」表を提示して説明。

(2) 衣類がリサイクルや廃棄されるまで追跡されるというのはいやです

ECOM コメント：

・電子タグを付けておくか外すかは、飽くまでも消費者が主体的に判断していただくものです。衣類の購入段階でタグを切り離すなり、リサイクルに出す場合にタグを壊すなりすれば、追跡はできなくなります。費用対効果の点からも、衣類をそこまで電子タグで追いかけることは、まずないであろうとお考えください。

・もっとも、自動車に代表される耐久消費財などは、履歴が分かっていた方が、消費者が(中古車などとして)販売する際に、有利になるかも知れません。

(3) それが企業にしろ、個人にしろ、やはり自分の知らない内に情報を取られるのはいやです

ECOM コメント：

・企業に持たれてしまうであろう情報と、個人(悪意の第三者)によって盗み見られるかも知れない情報とは区別してお考えください。

・企業が個人情報を不正使用したとして、それが発覚した場合には社会的制裁を受け、当該企業の存続に係わる問題となります。従って、そのようなことが組織的に行われることは、まずないと考えてよく、実際に、企業から個人情報が漏れる場合の 80%以上は人為的なミスもしくは作為によっています。補足すると、購入時点で企業に取得される情報の管理は、企業の個人情報保護の視点から考えなければなりません。

・電子タグの場合特に問題となるのは、悪意の第三者がターゲットとした個人のプライバシー情報を、電子タグに格納されている情報を読むことで入手してしまう場合ですが、これについては、各種の保護方式が考案され、検討されております。

・「平成 17 年度報告書」の「プライバシー保護方式」の表を提示して説明。

(4) 本の購入は、思想信条に係わることなので、やはりプライバシーのことは気になります

ECOM コメント：

・気になるお気持ちはよく分かるが、電車の中でアダルト誌をカバーも掛けずに読んでいる人もいます。プライバシーの感じ方は人それぞれですが、電子タグとの関連でその侵害が発生する確率をお考えください。

(5) 知らない内にバッグの中身を見られるのはやはりいやです

ECOM コメント：

・高級バッグなどは、アルミの網を内張などすることで、他社製品と差別化を図ることもマーケティング戦略の一つになるかも知れません。

【疑問】

(1) 例えば書籍を購入する場合に、どのような保護措置が取られますか?

ECOM コメント：

・費用対効果の問題があるので、適用出来る保護方式にも限度がありますが、書籍の場合は、電子タグを物理的に壊すか、電波遮蔽シールを貼るのが、最も効果的であると考えられます。このことは、「出版関連業界電子タグ標準化委員会」でも、「私案」として話したことがあります。

・「17 年度報告書」の「電子タグの利用シーンとプライバシー保護方式」の表を提示して説明。

(2) 書籍の購入者は、保護措置を取りうることをどこで知るのですか?

ECOM コメント：

・書店店頭で「クレジットカードでの支払いは一括ですか?」とか訊かれている分けなので、その流れのなかで確認したらよいかと考えられます。また店頭に大きく告知しておくということも必要です。飽くまでも保護措置の選択の主体は購入者であるとお考えください。

(3) プライバシーといっても人によって随分違いますが?

ECOM コメント：

・プライバシーの受け止め方は個人差もあるが地域差もあります。高級ブランドのバッグなら、むしろ読んでもらいたい」という意見もあります。

(4) 書店の店頭に告知をしても、他の告知・広告と紛れてしまいませんか?

ECOM コメント：

・初期の段階では、大きな告知スペースを取ったり、口頭で詳細に伝えたり、マスメディアで派手に告知したりすることも必要です。

(5) 書店での万引き対策には有効であることは分かりますが、誰がその処置をするのですか?

ECOM コメント：

・基本的には事業者(店員)側ですが、購入者の店頭での判断が第一です。措置に関しては、金属シールで遮蔽する単純な方法については、購入者がシールを貰って貼ることもありえます。キル・タグのような特別な装置が必要な場合には、事業者側が対応する事になります。

(6) 電子タグ添付のままの是非は、どのように判断したらよいのですか?

ECOM コメント：

・判断の主体は飽くまでも消費者であることをご認識ください。事業者は消費者の判断に従うことが義務づけられております。

・「17 年度報告書」の「プライバシー保護判断のフローチャート」の図を提示して説明

(7) 価格などの真正性はどこで担保されますか? バーコードの値段と店の値札の値が違ってい

る場合が以前ありました。

ECOM コメント：

・紙の値札とバーコードの価格情報との違いは人為的なミスと思われますが、電子タグを店舗システムと連動させることで、これを防止することができます。例えば、電子広告などと連動させれば、電子タグをスマートラベル化して、システム的に値段の間違いを防止することもできるようになります。

・値段の一括管理も可能なので、時間変わりの一斉価格変更(午後 5 時以降のプライスダウン)なども、瞬時かつ自動的にできるようになります。

(8) 電子タグは捨ててもよいのですか?

ECOM コメント：

・電子タグは、素材的に IC チップとアンテナが金属です。アンテナは銅やアルミニウムなので殆ど心配ないといわれています。IC チップの部分は重金属なので問題がありそうですが、その環境負荷は、世界中の電子タグを併せてもパソコン数十台分に満たないという研究もあり、それほど大きな負荷にはならないと思われます。

・環境へ配慮については現在、各方面で研究中です。

(9) 商品管理の履歴をキチンと書き込んでいるかどうかどういうふうにして確かめるのですか?

ECOM コメント：

・事業者の持っているデータベースとの照合によって可能です。

・データの改竄防止ですが、これには保護方式の内ソフト的な手段が適用できます。

(10) 悪意の第三者が読もうとしたらどういうふうにして防げるのですか?

ECOM コメント：

・Kill タグなり暗号化なり各種の方法がありますが、それらは電子タグ中心の考え方です。

・他方、電子タグの読み書きの装置(R/W)を登録制にするような方法も考えられます。もっとも、携帯電話でも電子タグを読めるようにすることも検討されていますので、登録制もなかなか難しいかも知れません。

・データの改竄防止については、例えば、R/W で書き込みを行う際に R/W の ID も書き込んでしまうようなことをすれば、誰(どの R/W)がデータを改竄したかが分かりやすくなると考えられます。

(11) 電子タグに書き込みが出来る事や消したデータを復活させることが出来る事を初めて知りました。復活させることが出来るなら、誰でも読めてしまうことになるのではないですか?

ECOM コメント：

・復活装置・手段の管理の問題になると思われます。特定の場所、機器でのみ復活可能な状態にしておけば大丈夫と考えられます。

(12) 家庭に、いろいろな電波を使った電子タグ添付商品が入ってくると、R/W も複数必要になりますが、それらを一括して読み取れるような装置(R/W)はないのですか?

ECOM コメント：

・技術的には可能で、いわゆる「マルチリーダー」が考えられていますが、高価になってしまうのが難点です。単一種の電波の「リーダー」との使い分けが行われると思われます。
・国際貿易では、UHF 帯は各国で波長が違うのでマルチリーダーが必要となるかも知れません。ただし、ハード的なマルチリーダーは高価になるので、それを回避するためにミドルウェアを使ったマルチタイプのリーダーが開発されると思われます。

【要望】

(1)質問が来た時の相談窓口が欲しいと思います

ECOM コメント：

・「プライバシー保護指針」にも、相談窓口を置くようになっています。将来的には、ADR 的なものも必要になるかも知れません。ECOM も相談に応じる事を検討しています。

(2) インターネットを見ない人(インターネットを使えない環境にある人、リテラシーが低い人)にも啓発用のツールが欲しいと思います

ECOM コメント：

・そういうことも想定して、今年度は簡易なパンフレットの作成を予定しています。できたら、御意見を頂ければ幸いです。(ご了解を頂きました)
・ECOM HP の図の拡大機能は、老人や弱視者に配慮したものです。

(3) もっと身近な医療とかいったところでのメリットはないのですか?

ECOM コメント：

・医療に関しては、院内物流の合理化や医療過誤の防止で実例があります。調剤などに適用した実証実験では、10 倍にスピードアップしたデータもあり、カルテや医薬品、医療機器・器具の管理にも使われ始めています。他の使用例については、HP の「こんな使われ方」をご覧ください。

【提言】

(1) 具体的にタグをつけたものが世間に出回って感覚的に慣れるまでは、不安感は払拭できないのではないと思います。その意味で、初期の導入の仕方、啓発の仕方が重要であると思います

ECOM コメント：

・関係省庁・団体・企業で統一的かつ斉一的な取り組みを大々的に行う必要があると考えています。

(2) 日頃の相談業務でよく感じますが、新しいものが出た場合には、情報不足による誤解に基づくトラブルが多いです。もっと大々的な啓発・宣伝が必要と思います。特に電子タグの消費者接点投入時には大々的な啓発・知識提供が必要であると思います

ECOM コメント：

・ECOM　HP も、微力ながらそういった趣旨の一環で制作しました。今後どんな情報の掲載を希望するかリクエストしていただければ、WG にて検討し、出来るだけ反映する

ようにいたします。

【訪問結果】

今回の訪問成果として、以下の項目が挙げられる。

(1) IC タグのプライバシー保護および真贋判定やトレーサビリティへの有効性をご理解いただけた

(2) リサイクルで履歴を残すかどうかの懸念があり、消費者が主体的に対応可能であることを告知する必要がある

(3) 本のタイトルやバッグの中身など、個人情報やプライバシーを知らずに読取られる事への懸念もあり、プライバシー保護措置についての告知が必要である

(4) 医療機器への影響や環境への配慮の告知が必要である

(5) IC タグへの書込と復活への対応方法への告知が必要である

(6) 導入時の情報弱者への積極的な啓発活動が必要である

2.2.2 日本生活協同組合連合会ヒアリング

日本生活協同組合連合会のヒアリングは、以下の日程にて行った。

・訪問日時：2006/10/19

・参加者：日本生活協同組合連合会 3 名

・項目

組合員の電子タグに対する意識： 5 項目

電子タグに対する生協のスタンス： 7 項目

当面の消費者接点での電子タグの利用： 2 項目

【組合員の電子タグに対する意識】

(1) 昨年度の実験では、ポイント提供のアンケート(母数 8,000 人強)を実施し、トレーサビリティという用語を知らない人が 67%でした。(別なアンケートでは、トレーサビリティ情報は重要であると回答した方は 53%にのぼる)電子タグについては、さらに認知度は低いと思われます。

(2) URL や二次元バーコードも認識はしていますが、十分には理解されていないのではないでしょうか?

・意識している組合員は 10%もいないと思われます。商品に関する問い合せ連絡先として、包材裏面に表示している組合員サービスセンターの電話番号は比較的認識されています。

(3) JAN コードとバーコードの関係も理解されていません。消費者には JAN コードの意味合いについて知らせていないので当然にもその利用方法はわからないのが一般的です。1 次元バーコード＝JAN コードといった理解が一般的ではないでしょうか。

(4) 組合員「4,000 人を対象としたカードアンケート」では、プライバシー、セキュリティの問題に関しては、磁気カード以外の高機能なカードを希望している組合員が多いです。

(5) 上記の「4,000 人アンケート」のなかでは、電子商取引という意味でのインターネット取引

に関しては、50%弱以上の方が、セキュリティがしっかりしていて安心なものという回答が多かったです。

・インターネットを使うという意味では、組合員の中でも比較的若い方である 30 歳台、40 歳台で利用が高い。

・インターネットの一般のサイトなどで、でクレジット番号や暗証番号を打ち込むのは怖いという意識を持つ方が半数ありました。通常は銀行口座からの引き落としで全てが処理されるので、生協では現在はこちらに慣れている(組合員番号と氏名、住所等は生協のシステム内で管理され、外部にでることがないため安心と感じているためと解釈できます。

・生協の引き落としは銀行と直結しているので組合員と銀行口座の管理がしっかりしているので安心と感じているようです。

【電子タグに対する生協のスタンス】

(1) 電子タグについて物流が中心となっており、消費者接点以降での使用は考えておりません。

・個品への添付は考えていません。添付のコストが高く、費用対効果の問題があります。

(2) レーサビリティなど、食の安全確保のためには、商品一個一個に何らかのコードを添付する必要がありますが、バーコードで十分対応可能です。

(3) 生協の会員 2,000 万人と言っても、独立した単位生協の会員を合計したもの。各生協は、それぞれシステムもデータベースも違うため、(店舗に)電子タグを導入するにしても、事業連合体～単位生協で、ロットを考えなくてはなりません。

・最大組織はコープネット事業連合の 307 万人です。(関東の 7 つの単位生協が加入している)

(4) 情報家電との絡みでいえば、冷蔵庫収納食品の表示は知りたがっている人は確かにいると思いますが、冷蔵庫の在庫管理との係わりでニーズがあると思われます。ただし、現状では食品単価に比べ電子タグの価格が高過ぎます。1 円を切れば広がるのではないでしょうか。

(5) 社会受容性・プライバシー問題は、消費者判断で、どこで切り分けるかですが、(個品単位で電子タグが添付されても)表面化することはないでしょう。(理由は、現在でも店のレジ袋は中が透けて見える程の半透明状態なため)

・独メトロ社の Future Store のキル・タグ装置も殆ど使われていません。

(6) 電子タグとプライバシーの関係が、近い将来大きな課題になるとは考えていません。

(7) 電子タグで何が出来るかに関心があります。

・店舗で商品を購入(販売)するとして、どんな情報を扱うべきか。キラーアプリケーションは何か?

【当面の消費者接点での電子タグの利用】

(1) 商品の仕入れや仕分けはバーコードで管理しています。宅配で使う発泡スチロール製のシッパー(Shipper)には、組合員用のラベルが貼ってありますが、回収する毎に剥がしています。これを電子タグに代えることは検討に値します。

・IC タグとリライタブル印刷技術の組み合わせが重要

(2) シッパーでは冷蔵・冷凍品を配送する際に、温度管理をしていないので、これを電子タグ(センサータグ)によって行うことは検討に値します。

【訪問結果】

今回の訪問成果として、以下の項目が挙げられる。

(1) 電子タグの用語への認知度は低く、啓発が必要である
(2) インターネットでの電子商取引は半数がセキュリティの確保があれば安心と考えている
(3) 費用対効果により物流中心の利用で、消費者接点にはバーコードが利用されている
(4) 単価が下がれば、冷蔵庫在庫管理でのニーズがある
(5) プライバシー問題が将来大きな課題となるとは思えない
(6) 電子タグ利用によるビジネス展開に興味がある
(7) 宅配シッパーなど回収再利用する物への利用が考えられる

2.2.3 全国消費者団体連絡会勉強会

全国消費者団体連絡会での勉強会は、以下の日程にて行った。

・訪問日時：2006/10/20
・参加者：全国消費者団体連絡会 3 名
・項目

質問：	6 項目
懸念：	4 項目
用途への期待：	7 項目
技術的な提案：	2 項目

【質問】

(1) IC カードと電子タグは違うのですか?

ECOM コメント：

・原理的には同じですが、電子タグの読取距離は数十センチから数メートルと長くなります。

・IC カードは人が持って意識的に使いますが、電子タグ(電子荷札)はモノに着けて使い、そのものの存在を積極的には意識しない場合が多いです。

(2) 読まれないようにするためにはどうしたらいいのですか?

ECOM コメント：

・買い物袋で電波を遮断する方法があります。

・Kill タグをしておいて、後から復活させることも可能です。

(3) バーコードはなくなりますか?

ECOM コメント：

・なくならないと思われます。シチュエーションによりますが、電子タグとは相互補完の

関係になると思われます。

(4) 食品にはバーコードレベルで十分に用が足りると思います。

ECOM コメント：

・トレーサビリティ用途でなら足りると思われますが、店舗での高度なサービス提供には電子タグの活用も考えられます。

(5) 牛肉など、大きな塊を切り分けていくと、ドンドン小さな塊になりますが、それにもドンドン電子タグを付けていくのですか?

ECOM コメント：

・原理的にはそうですが、そこまでする必要性と費用対効果が問題となります。

(6) 普及の要因はコストの問題でしょう。

ECOM コメント：

・電子タグ(インレット)1 枚 5 円で製造のメドは立ちましたが、添付のコストが掛かります。将来的には、随分廉価に使うことができるようになると思われます。

[懸念]

(1) 第三者がリーダーを持つことによって、プライバシー情報を取得され、モノを売りつけられる可能性もあるのではないでしょうか?

ECOM コメント：

・対面ならあり得ますが、個人情報との紐付けがなされない限り難しいです。

(2) 個人が電子タグを読み取ることができるようになると、(プライバシー問題が)複雑になるのではないでしょうか?

ECOM コメント：

・その懸念は大いにあり得ます。ある程度の知識があれば、R/W は、秋葉原で部品を購入して組み立てることもできます。

(3) キル・タグは、消費者には余分な作業になるのではないでしょうか?

ECOM コメント：

・Kill タグの選択は消費者ですが、実施は事業者というケースもあり得ます。

・独メトロ社 Future Store のキル・タグ装置は、殆ど使われていません。

(4) 食品用途トレーサビリティに使えると思いますが、食品の平均単価に比してコストが掛かりすぎるのではないでしょうか?

ECOM コメント：

・単にトレーサビリティ用途ならバーコードでも対応が可能です。

[用途開発への期待]

(1) 製品のリコールの問題に有効であると思います。

ECOM コメント：

・所在情報の把握、修理の履歴管理なども可能です。

・経済産業省が昨年 8 月に出した中古家電等の管理に電子タグを使うようにとの通達は、

ガス湯沸器の事故に対応したものです。

(2)電化製品に不具合が発生した場合、取扱説明書、保証書などを電子タグ経由で入手できれば非常に便利です。

(3) リサイクルに使えるのではないでしょうか。

ECOM コメント：

・その方向ですが、費用対効果の問題があり、対象が限定されます。

(4) 捨てられたモノも見つけられないでしょうか。

ECOM コメント：

・GPS タグとは違うので、難しいです。

(5) アレルギー表示など電子タグに書き込んでおけば便利です。

ECOM コメント：

・アレルギーは機微情報なので、プライバシー選択・確保の問題があります。

(6) 病院で貰う紙袋のリサイクルに使えますか? また複数の病院・診療科に跨ると、処方される薬の種類が多くて、どれを服用したら良いのか混乱する場合があるので、そのナビゲーションができないでしょうか?

ECOM コメント：

・可能ですが、個人用の R/W が必要になります。

(7) SCM におけるトレーサビリティで、メーカーから消費者に対する Trace Forward、消費者からメーカーまでの Trace Back の流れは、販社等が入ることで途切れることが往々にしてありますが、電子タグを使って途切れたのを繋ぐことができれば、事故等への対応も速やかに行うことができ便利です。

[技術的な提案]

(1) 長い距離で読み取れない電子タグを作ったらどうでしょうか。

ECOM コメント：

・紙幣などでは、そういったニーズもあると思われます。

・現在、読取距離を短くしてセキュリティやプライバシーを守る事が研究中です。

(2) 携帯電話をリーダーに出来れば便利。また携帯電話やパソコンを電子タグのディスプレイに出来れば非常に便利です。

[訪問結果]

今回の訪問成果として、以下の項目が挙げられる。

(1) Kill タグなどの電波遮断方法の告知が必要

(2) バーコードとの違いの告知が必要

(3) 第三者による読取機利用への懸念があり、その対応策を告知する必要がある

(4) 製品リコールや事故への利用が期待されている

(5) 取扱説明書や保証書などの入手方法として期待されている

(6) SCM におけるトレーサビリティへの利用が期待されている

(7) 読取距離を短くする事で紙幣に利用するなど、プライバシーを守る期待がある
(8) 携帯電話への IC タグ読取機能付加への期待がある

2.2.4 消費者関係団体への訪問･質疑の総括

今回の消費者関係団体訪問での質疑を総括すると次の項目があげられる。

(1)消費者の視点での電子タグ(IC タグ)の機能説明と啓発が必要

・名称として一般的な「IC タグ」を使用する事で理解度が向上する。
・電子タグの用語への認知度は低く啓発が必要であるが、的確な説明を行えば、プライバシー保護および真贋判定やトレーサビリティへの有効性は理解される。
・電子タグ(IC タグ)への書込と復活への対応方法やバーコードとの違い等、導入時の情報弱者への積極的な啓発活動が必要である。

(2)電子タグ(IC タグ)使用によるプライバシー保護や医療機器・環境への配慮が必要

・本のタイトルやバッグの中身など、第三者による読取機利用による個人情報やプライバシーを知らずに読取られる事や、リサイクルで履歴を残すかどうかの懸念があり、消費者が主体的に対応可能であることを告知する必要がある。
・Kill タグなどの電波遮断方法等、プライバシー保護措置についての告知が必要であるが、的確な啓発を行えば、プライバシー問題が将来大きな課題とならずに浸透できると考えられる。
・医療機器への影響や環境への配慮の告知が必要である。

(3)電子タグ（IC タグ）使用具体例や将来像を正しく伝達する必要がある

・電子タグ利用によるビジネス展開として、単価が下がれば、SCM におけるトレーサビリティへの利用ニーズがあるほか、宅配シッパーなど回収再利用する物への利用が考えられる。
・セキュリティ面では、インターネットでの電子商取引へは半数がセキュリティの確保がされれば安心と考えられている。
・生活面での利用に関しても、冷蔵庫在庫管理や、取扱説明書や保証書などの入手方法として、さらに製品リコールや事故への利用、携帯電話に IC タグ読取機能付加しての利用への期待がある。

3. 電子タグ普及のための消費者啓発用パンフレットの制作

3.1 消費者啓発パンフレット「やさしい IC タグ入門」の制作

消費者関係団体の方々との意見交換会や勉強会にて、数多くの貴重なコメント頂いた。その内容をもとに、消費者啓発パンフレット「やさしい IC タグ入門」を制作した。

本パンフレットの主な特徴は、次の通りである。

・消費者の立場を考慮した簡潔で分かりやすい表現
・キャラクターには、生活者としての家族を使用
・表現は「IC タグ」に統一
・消費者の立場を考慮した IC タグの形状・機能を簡潔に説明
・利用シーン事例として、消費者生活に密着した 5 例を説明
・プライバシーや医療・環境への影響を明記
・　携帯性を重視し A4 版 3 つ折で製作

3.2 パンンフレット「やさしい IC タグ入門」の内容

表紙部分には、家族 4 人のキャラクターを用い、家族それぞれが、ラジカセやリンゴパック、本を持ち、消費者の生活の中で電子タグが利活用されている事をアピールした。また用語として IC(アイシー)にルビを付記した。

裏表紙部分には、本 TF での検討結果を元に、プライバシーへの配慮の他、医療機器への影響、環境への配慮、呼称について明記した。また、より詳細な情報を欲しい消費者向けに、ECOM「やさしい IC タグ入門」ホームページ URL を記載し、ホームページへの誘導を行った。なお用語は全て IC タグに統一した。

表紙を開いた最初のページには、IC タグとはと題して、IC タグについての簡潔な説明を行った。主な内容は、一般的な形状、動作原理、IC カードとの違い、IC タグの特長と種類、最大読取距離や無線周波数、電波の広がりによる分類と図解、読取機の種類と一般的な読取機種別の説明とした。

パンフレット内面には、IC タグの利用シーンとして以下の 5 つの事例を簡単な紹介文と共に掲載した。

・事例 1：欲しい商品がすぐ探せます
　ショッピングで在庫確認が簡単に出来る事例を紹介
・事例 2：医療の信頼性が高まります
　調剤や投薬などのミスが現象する事例を紹介
・事例 3：図書館が便利になります
　図書館の貸出・返却が便利になる事例を紹介
・事例 4：食品の詳しい情報を表示できます
　産地や生産者情報が簡単に確認出来る事例を紹介
・事例 5：製品の修理やリサイクルが便利になります
　製品情報や購入・修理履歴などが簡単に確認できる事例を紹介

3.3 パンフレット「やさしい IC タグ入門」の本体

ICタグとは

「ICタグ」は、ミリ単位のICチップと小型アンテナで作られている無線機能部分と、それを支える包装部分からなる小さな通信機です。ICチップ内に書き込まれている情報を、専用の読取機によって直接触れずに自動的に読み取ることが可能です。ICタグの動作原理は「ICカード」と同じですが、ICカードが主として人の認証に使われるのに対し、ICタグは主に商品などのモノに添付して使われます。そこでICタグを「電子荷札」「電子値札」と呼ぶこともあります。現在商品に貼付されているバーコードは、商品の情報を読み取るだけですが、ICタグでは情報の書き換えも可能です。そのほか、複数のICタグの同時読取ができる、小型化できる、耐久性がある、情報量が多い――などの特長があり、さまざまな分野で幅広く利用できます。

ICタグの種類

ICタグは無線周波数によって分類されます。種類によって最大読取距離や電波の広がりが異なりますが、店頭や倉庫など、利用シーンによって使い分けます。主なものは次の3種類です。

最大読取距離	数10cm	約1m	数m
無線周波数	13.56MHz	2.45GHz	UHF (952~954MHz)
電波の広がり	大きい	小さい	ふつう

読取機の種類

ICタグの情報を読み取るには、専用の読取機を用います。店の入口や棚など決まった場所に設置される据置型、手で持って操作するハンディ型などがあります。

プライバシーへの配慮について

ICタグは、書き込まれている情報を、接触することなく読取機で読み取ることが可能という便利な特徴があります。しかし、この特徴を悪用する人が現れて、他人のICタグの情報を無断で読み取るといった恐れもあります。そのような問題は、電波を反射したり吸収したりする素材でICタグを覆ってしまうとか、情報を暗号化するなど、適切な防止策を講じることで、安全に解決することができます。また政府や業界団体でも法制度・ガイドラインを策定しています。

医療機器への影響について

総務省の指導でわが国の民間団体が、ICタグの読取機が発する電波が、心臓ペースメーカー、除細動機などの一部の医療機器の動作に影響を及ぼすことを確認しています。ただし、読取機と適切な距離を保てば心配いらないことも確認されています。適切な距離を保つためのマークも制定されています。

環境への配慮について

将来、大量にICタグが使用されるようになると、その廃棄時に環境への配慮が必要になります。

「ICタグ」の呼称について

正式な技術規格ではJIS X 0500 で、「RFタグ」の用語が決められていますが、このパンフレットでは、「ICタグ」と呼ぶことにしています。

ICタグのより詳しい情報は
ECOM「やさしいICタグ入門」ホームページ
をご覧ください。

http://www.ecom.jp/ictag

次世代電子商取引推進協議会
〒105-0011 東京都港区芝公園3-5-8 機械振興会館3階
Tel:03-3436-7500 E-mail:TAGguide@ecom.jp

やさしい ICタグ入門

―ICタグってなんだろう?

ECOM 次世代電子商取引推進協議会

ICタグの利用シーン

ICタグは、その特長によって、様々な業務・分野で利用されています。今後ますます幅広く利用できるとされています。

1 欲しい商品がすぐ探せます

商品にICタグがつけられると、商品の特徴や色・サイズの違う在庫を画面上で簡単に確認できます。

2 医療の信頼性が高まります

医薬品や医療機器にICタグがつけられると、調剤や投薬などの間違いが無くなり、医療の安全を確保することができます。

3 図書館が便利になります

図書館の書籍やCD・DVDなどにICタグがつけられると、貸出カードで確認しながら貸出・返却が簡単にできます。

4 食品の詳しい情報を表示できます

食料品のパッケージなどにICタグがつけられると、産地や生産者情報、レシピなどの情報を簡単に確認できます。

5 製品の修理やリサイクルが便利になります

電気製品などにICタグがつけられると、修理やリサイクルする時などに製品情報や購入・修理履歴などが簡単に確認できます。

他にもこんなところで

ICタグは、これらの他にも、レストランでの料金精算など、身近な生活での利用だけでなく、工場、オフィスなどでも製造管理、在庫管理、運送管理、資産管理などで、業務効率の向上のために利用されはじめています。

4. 消費者啓発用 HP のリニューアル

4.1 消費者啓発用 HP リニューアルの趣旨

普及促進・社会受容性検討推進 WG では電子タグに関して一般向けに広報を行うことを目的に、経済産業省からの平成 17 年度受託事業として、ホームページ（以下「HP」）の作成を行った（タイトルは「やさしい IC タグ入門」）。

この HP 利用者の想定ターゲットとしては広く一般におき、電子タグに関しての初心者が広範な知識を持ってもらうことを基本とした。しかし同時に、ビジネスマンの業務上の書類作成などのためのレファレンスに際しても使えるものとできるよう留意した。せっかくの制作機会であるので、IC タグに関して総合的に記述し、各方面に広範に参照・引用されるようなサイトを作成することを目指す内容とした。現在のところ、世界で最も主要な検索エンジンである Google において、「IC タグ」と検索すると比較的上位の 18 位（2 画面目）で登場しており（平成 19 年 2 月 28 日現在）、当初の意向はある程度達せられているものと考える。

平成 17 年度に制作した HP のコンテンツは完成後 ECOM サイト内に移管され、「やさしい IC タグ入門」のコーナーとして、平成 18 年 7 月から公開されている。平成 18 年度においては、ECOM の自主事業として、この「やさしい IC タグ入門」のコンテンツの見直しを行った。時間の経過に伴って情報を更新する必要がある部分を加筆修正したほか、昨年度のバージョンをよりわかりやすく、見やすくデザイン等をリニューアルする作業を行うこととし、普及促進・社会受容性検討推進 WG の TF（タスクフォース）2 にて、その検討を実施した。

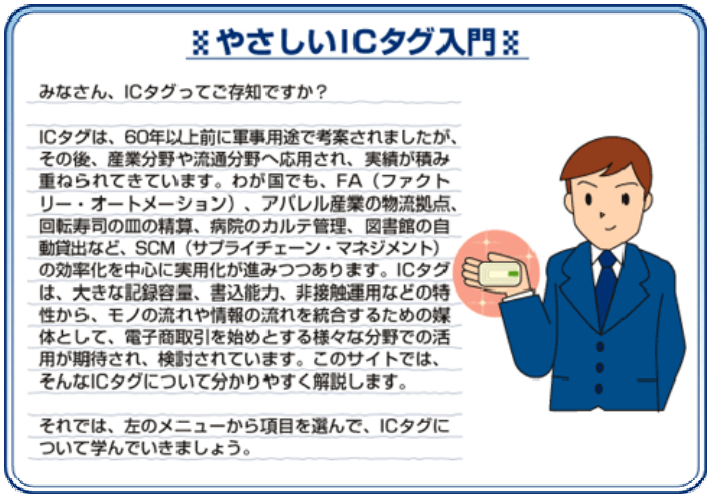

図 4-1 「やさしい IC タグ入門」HP エントランス説明部（平成 17 年度制作版）

4.2 消費者啓発用 HP リニューアルの方針

平成 17 年度当初の作成の方針として「初心者に対して、電子タグに関する一般知識をわかりやすく」という趣旨から、本 HP においても、

- 電子タグの基本的な技術知識

・　導入の実例
・　国の政策
・　プライバシー啓発

などまでを含むものとした。また、ECOM の HP 中にある「やさしい EC」のコーナーを先例とし、記述項目・内容、説明のトーンなどを参照した。その結果、図表・イラストや写真を多用し、長い文章での説明を避けることとした。また制作する HP の分量についても、見る側の負担感と、制作参加者のキャパシティ、制作期限などを考慮し、その範囲内に納めることを前提とした。

HP のタイトルとしては、「やさしい EC」を先例とし、「やさしい IC タグ入門」とした。タイトルの用語に「IC タグ」を用いることに関しては WG/TF 内でも議論をしたところであるが、新聞記事検索結果などでも類語の中では「IC タグ」の表記が多いこと、また「IC カード」の用例が一般化していること、一般の初心者も含めてまず見ていただくことを目指すというスタンス、などから（電子タグ、RFID などの類語ではなく）あえて最も広く使われている、「IC タグ」という用語をタイトルに利用することとした。

平成 18 年度版のリニューアル作成に際しては、基本的には前年度に作成した時点の方針を踏襲したが、以下においては変更した。

・　（17 年度版）イラストがサラリーマン風の男性一人で硬い印象がある
　→（18 年度版）男性に加え、女性や子供なども加筆しやわらかい印象にした

図 4-2　「やさしい IC タグ入門」HP エントランス説明部（平成 18 年度制作版）

・（平成 17 年度版）説明をシンプルにしてある
　→（平成 18 年度版）説明テキストを加筆修正して、より詳しい情報を提供するなど、表現をやわらかくする。トップページ、導入事例の説明、Q&A の加筆修正など

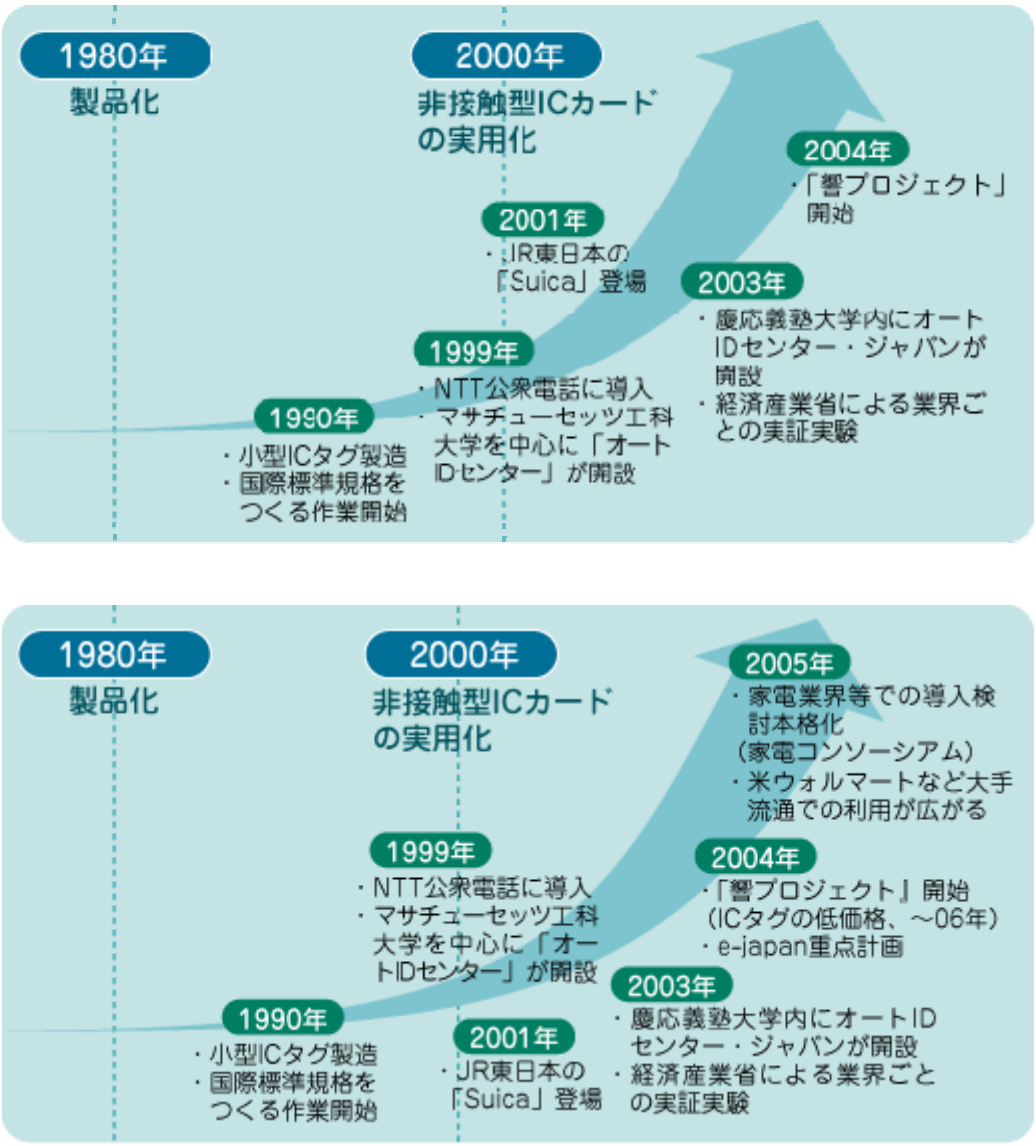

図 4-3　説明の追加事例「IC タグの歴史」
（上：平成 17 年度制作版、下：平成 18 年度リニューアル制作版）

4.3　HP リニューアルのプロセス

「やさしい IC タグ入門」HP の制作は、平成 17 年度普及促進・社会受容性検討推進 WG のタスクフォース（TF）3 において検討、推進され、HP 制作会社であるカデナ株式会社に引継ぎ、HP 画面化の作業を行った。

「やさしい IC タグ入門」HP のリニューアル制作は、平成 18 年度普及促進・社会受容性検討推進 WG のタスクフォース（TF）2 において検討、推進された。平成 18 年 7 月 27 日の WG において今年度の方針を審議、決定し、9 月 22 日、10 月 25 日の TF2 会議で、今年度変更の骨格と分担を決定し、以後、各担当部分の修正原稿作成作業に移った。変更内容は 12 月 15 日、平成 19 年 1 月 29 日の WG 会議にて適宜報告され、制作会社であるカデナ株式会社が順次これを受け

取ってホームページ画面に制作した。最終的には 3 月 1 日の WG においてリニューアル版の完成を見た。

表 4-1　リニューアル検討した項目

大項目	中項目	趣旨	対応
改訂の大前提	著作権はMETIに	METIの意向確認	METIに確認する
	予算の制約	予算内でできる作業に限定	予算内でできる内容を明示化
全体に関わる事項	全体トーン	TF1と足並み揃える	予算等で可能な範囲で
	注目度確認	ページビューのカウント	同左機能を検討
	双方向化	意見記入・問い合わせ欄の設置	同左機能を検討、ただし対応何処まで？
	ビジュアル	写真、動画の導入	動画は困難、写真は検討
	ビジュアル	絵の多用を	現行でも既にイラストは多い。見せ方は要検討
	構成・内容の精緻化	外部資源によるチェック	予算の制約あり困難
デザイン	METIロゴ？	違和感がある	ECOMとのダブルロゴ化検討(経産省へ確認)
	キャラクターデザイン	背広の男性では硬い	キャラクタは無理としても、家族の絵など検討余地あり
タイトル・著作権	名称	変更してはどうか	決定の経緯や制約から、現実的にはこのままか？
	COPYRIGHT	©METIのままか	表記方法は内容に応じて検討(経産省にも確認)
なぜ注目されるのか	意識調査結果	データが陳腐化する	指摘どおりだが、対案には予算必要
こんな使われ方	構成・表現	企業→消費者の並びは逆？	指摘どおり。要検討
	構成・表現	「消費者」言葉が硬い	「家で」「会社で」などの言い換え
	ビジュアル	動画（アニメ）の利用	メリットが協調できれば検討
	構成・表現	アニメ前の説明文タイトル	抽象的。わかりやすく改善検討
	削除内容の復活	人につけるタグ	復活を検討
	ビジュアル	絵やアニメではなく、実写の現実感	三越導入写真なども検討
	ビジュアル	動画（NHKニュースなど）	利用料金の問題、画面作成上の技術的問題で不可
	構成・表現	実証実験事例紹介を追加しては？	検討可能（現在のパネルレベルであれば）
普及のための課題	（特になし）		
プライバシーの確保	ビジュアル	侵害、保護の絵が削除になっている	印象悪いので、削除のままとする（文章は検討余地あり）
	内容	米国消費団体のガイドライン追加	確認して追加の方向で検討
国の政策	構成・表現	検討したが現状のままとする	経産省の政策（変更点）は追記
Q&A	FAQ	TF1消費者関連団体での質疑を反映	そのようにする
リンク集	構成	事業者や実験団体の追加検討	現状どおり。
補足	TF1作成パンフ	掲載し、ダウンロードできるようにする	そのようにする

(1) 使われ方事例紹介の変更例

（平成 17 年度版）・企業内での使われ方（医療の安全性と生産性向上など 6 例）

・企業間での使われ方（資材のリユースなど 6 例）

・消費者との係わりでの使われ方（顧客満足度の向上など 6 例）

（平成 18 年度リニューアル版）

・みなさんの身近で活躍する IC タグ（医療の安全性と生産性向上など 10 例）

・みなさんの知らないところで働く IC タグ（書類管理の自動化など 10 例）

昨年度と比較して、事例の括り方を工夫、変更し、2 例の事例を追加した（航空手荷物の管理、道路での位置情報の提供)。昨年度は「人につける IC タグ」事例は除外した経緯がある。

(2) パンフレットダウンロードの追加

TF1 にて作成した、A4 版（３つ折）の「やさしい IC タグ入門」パンフレットを PDF としてダウンロードできる機能を追加した。

図 4-4　「やさしい IC タグ入門」パンフレット

4.4 リニューアル HP のサイトマップ

平成 18 年度に制作した消費者啓発用 HP、「やさしい IC タグ入門」（リニューアル版）の内容は下記のとおりである。平成 17 年度版と大項目での変更はなく、小項目で若干の変更がある程度である。サイトマップの大項目、小項目、および主な内容について記す。

表 4-2　やさしい IC タグ入門　（リニューアル版）サイトマップ

大項目	小項目	主な内容
ICタグってなに？		
	ICタグとは	ICタグの特長についてわかりやすく解説
	ICタグとRFID	無線タグ、無線ICタグ、電子タグなど多くの名称があることを紹介
	ICタグの種類	周波数帯域で種類があること。代表的な3例をわかりやすく解説
なぜ注目されるのか		
	タグの歴史	ICタグが注目されるまでの歴史的な経緯
	ICタグの特長	ICタグとバーコード技術の簡単な比較より特長を示す
	ICタグの活用例	ICタグには幅広い用途があることを概説
	企業が注目するICタグ	企業のICタグ導入意向についてアンケート結果を紹介
	消費者が注目するICタグ	消費者のICタグ利用意向についてのアンケート結果を紹介
こんな使われ方		
	ICタグの導入事例	身近な事例10例と、知らないところで利用される10例を、イラストで紹介
	経済産業省電子タグ実証実験	経産省の実証実験事例の紹介と、リンク
普及のための課題		
	コストの低減	響タグの開発やリユースによりコストが低減される可能性があることを紹介
	ベストプラクティス創出	キラーアプリケーションの登場が待たれることを紹介
	消費者の正しい理解の促進	消費者に正しく理解してもらう必要について紹介
	標準化の促進	国際標準化の必要性について紹介
プライバシー		
	プライバシーについて	ICタグの利用とプライバシー確保の必要性について紹介
	法制度･ガイドライン	総務省・経済産業省のガイドラインなど、4例を紹介
	使用告知マーク	国際標準化機構などで検討されている告知マークを紹介
国の政策		
	ICタグに関する国の政策	政府各省庁のICタグ関連施策を紹介し、HPアドレスも掲載
Q&A		
	よくある質問	特長やプライバシーについて一問一答形式で記載
リンク集		
	ICタグ関連団体	ECOMなど関連5団体を紹介、HPアドレスも記載
お問い合わせ		
プライバシーポリシー		
サイトマップ		

5. 電子タグのセキュリティ技術とプライバシー保護技術

電子タグは、物流の効率化や製品ライフサイクル管理を実施するうえで有効な技術として注目されている。現時点での電子タグの利用範囲は企業内や業界内が多く、一般消費者の認知度はそれほど高くない。そのため、電子タグの普及促進以前に、誤った理解や知らないことから生じる不安から、消費者が電子タグに対して警戒心を抱きかねない。

そこで、前章までは電子タグの啓蒙のために製作したパンフレットやホームページなどについて説明したが、本章では、技術的な視点に立って電子タグのセキュリティ技術とプライバシー保護技術について、最近の事例を解説する形で説明する。

5.1 電子タグのセキュリティ技術

電子タグの利用範囲が限定可能で第三者が介在する可能性が低い場合は問題ないが、電子タグが様々な目的で利用され不特定多数の手に渡ることになると、悪意を持った第三者の攻撃に備える必要がある。

本節では、最初に電子タグを含むシステム（以下、電子タグシステム）に対する脅威と、それに対する一般的な対策方法を説明する。次に、脅威の事例として、電子タグ電力解析攻撃と、電子タグウィルス問題について説明する。同じく脅威として考えられる電子タグプライバシー問題については次節で説明する。

5.1.1 電子タグのセキュリティに関連する脅威と対策方法

現時点における電子タグの基本的な用途は、バーコードの代わりに製品に貼付して識別することで、その製品の生産や流通、販売などの効率化に役立てることである。バーコードと比較して電子タグには次の利点がある。

①離れていても、目に見えない位置に貼られていても、読み取りが可能。

②書き込めるデータ容量が多い。

③データを書き換えることが可能。

④複数同時読み取りが可能。

これらの利点は生産、流通、販売などの業務負荷を軽減するが、一方で悪意を持った第三者の攻撃対象になる可能性が指摘されている。電子タグの脅威は、一般的な情報システムと同様に、盗聴、改竄、なりすましが考えられる。以下にそれぞれについて説明する。

(1) 盗聴

電子タグとリーダー／ライター（R/W）間の通信路から情報を盗み出す攻撃が考えられる。例えば、電子タグ自身にパスワードを設定し、利用者のアクセスを制限する機能を搭載するタグがあるが、アクセス時などに通信路を盗聴されパスワードが盗み出される可能性がある。

また、電子タグの所持者に気付かれることなく、第三者が電子タグを読み取る攻撃が考えられる。この攻撃により、所持品の内容や所持者の居場所や行動を監視されプライバシーを侵害される可能性がある。

(2) 改竄

改竄とは、悪意を持ってデータの一部または全部を書き換えることを言う。例えば、電子タグに製品を説明する生産者、製造年月日、保証期限、識別番号などのデータが格納されている場合、これらのデータが改竄されることにより、被害をこうむる可能性がある。

(3) なりすまし

なりすましには、電子タグのなりすましと R/W のなりすましが考えられる。

電子タグのなりすましは、電子タグの応答を模倣して電子タグになりすます方法と、データが何も書き込まれてない電子タグに適切なデータを書き込むことにより特定の電子タグになりすます方法が考えられる。

一方、R/W のなりすましは、R/W が発信する適切なデータを模倣して正規の R/W になりすます方法が考えられる。

(4) サイドチャネル攻撃

サイドチャネル攻撃とは、電子タグの処理時間や消費電力などの動作状況を様々な物理的手段で精密に測定することにより、電子タグ内部の情報を不正に取得しようとする攻撃である。

これらの脅威に対して以下のような対策が考えられる。

「(1)」(盗聴) については、電子タグの取り外しやアルミ箔で覆うなどの対策が考えられ、「(3)」(なりすまし)については、利用者による電子タグの目視の確認を行うことで攻撃を回避できる。「(4)」(サイドチャネル攻撃) については、電子タグに重要な情報を格納しなければ問題にならない。

また、(1)通信路の盗聴や(2)格納データの改竄、(3)R/W のなりすましについては、通信路を簡易的に暗号化したり、データ格納領域を書き換え禁止状態にロックしたり、電子タグが R/W を認証したりする機能を搭載した電子タグが製品化されているので、それを活用することによりこれらの攻撃を回避できる。

これらの対策は一例であり、電子タグの用途に応じて別の対策の方が効果的な場合も十分ありえる。以降では、電子タグに対する脅威について具体的な事例を紹介し、その対応策について説明する。

【事例】 EPC Tags Subject to Phone Attacks

2006 年 2 月に“ RFID JOURNAL ”が「EPC Tags Subject to Phone Attacks (携帯電話で EPC タグを攻撃)」というタイトルの記事を報じた。この記事は、同月に開催された「RSA Conference 2006」での Adi Shamir 氏の発表を基に書かれている (参考文献[1])。この記事によると、イスラエルのワイツマン研究所の Adi Shamir 氏は、Yossi Oren 氏と共に、EPC Class 1 Generation 1 の電子タグの Kill パスワードをハッキングして、Kill (無効化) したとのこと。

ハッキングの方法は、サイドチャネル攻撃のひとつである電力解析攻撃が用いられている。電子タグは、R/W のコマンドを処理するときに消費電力が増える。電力解析攻撃は、この現象を傍受することで、処理内容を類推する攻撃手法である。この手法は電子タグだけに限らず、IC カードなどでも有効であり、実験室レベルで IC カードに記録された DES の鍵を特定したという発表もされている。

EPC Class 1 Gen 1 の電子タグは、電子タグを無効化する Kill 機能を搭載している。この Kill 機能は、R/W が正しい Kill パスワードを電子タグに送信すると、電子タグは無効化状態になり、以降 R/W のコマンドに対して反応しなくなる。EPC Class 1 Generation 1 の電子タグの Kill パスワードは 8 ビットである。

Adi Shamir 氏は、すべて異なる Kill パスワードを電子タグに送った場合と、1 ビットだけ異なる Kill パスワードを送った場合における電子タグの消費電力を比較した結果、後者の方が電子タグの消費電力が大きくなるという現象を検出した。その理由として、この電子タグは Kill パスワードを 1 ビットずつ検証しているため、前者は最初の 1 ビット目で検証処理を終えているのに対して、後者は最後の 7 ビット目まで検証処理を実施するため消費電力が大きくなると説明している。この考え方で、1 ビットずつ 8 回比較を繰り返せば Kill パスワードを導き出すことができることになる。

この電力解析攻撃に対して、Adi Shamir 氏自身が「電力解析攻撃に関しては、かなりの量の対抗策がある。現に IC カードは、電力解析攻撃に耐えられるように設計されており、この技術は電子タグにも応用可能である。」と述べている。

例えば、IC カードなどでは，主に次のような対策が実施されている。

(1) 内部処理の相関を小さくする

(2) 消費電力測定に対して雑音を付加する。

(3) 応答信号の振幅を小さくする。

実際には、電力解析攻撃をするために膨大なサンプルデータと非常に精密な計測が必要であり、あまり現実的な攻撃手法とはいえないと考えられている。

“ RFID JOURNAL ”が、携帯電話で攻撃できるとタイトルで述べている。これは今回調査した EPC Class 1 Generation 1 の電子タグの周波数帯が携帯電話の周波数帯に近いというだけであり、携帯電話で攻撃できる根拠は示されていない。

5.1.2 電子タグのウィルス問題

2006 年 3 月に開催された「IEEE PerCom 2006」にて、オランダ、アムステルダム自由大学の Melanie R. Rieback 氏、Bruno Crispo 氏、Andrew S. Tanenbaum 氏が、世界初の電子タグウィルスを発表した（参考文献[2]）。この電子タグウィルスについて、「Is Your Cat Infected with a Computer Virus?（あなたの猫はコンピュータウイルスに感染していませんか？）」と題した論文に詳細が述べられている。この論文には、特殊なコードが書き込まれた電子タグを、試験的に用意した電子タグシステムに紛れ込ますことで、このシステムがウィルスに感染するという実例を示している。

このウィルスの種類は、電子タグ特有の新しいものではなく、従来からウェブサーバーやデータベースシステムなどで利用されてきたバッファオーバーフロー、コードインサーション、SQL インジェクションというような攻撃手法である。

以下にこれらの攻撃方法について簡単に説明する。

(1) バッファオーバーフロー（Buffer Overflow）

バッファオーバーフローとは、大きなサイズの入力データを送り込むことで、アプリケーショ

ンが確保したメモリーを溢れさせ､想定外の動作を引き起こさせる最も一般的な攻撃手法である。バッファオーバーフローにより、企業は年間数億ドルもの被害を被っていると言われている。

(2) コードインサーション（Code Insertion）

コードインサーション攻撃の中で最も一般的な手法にクロスサイトスクリプティング（XSS）という攻撃がある。クロスサイトスクリプティングは、攻撃者があるホームページに送り込んだコードを、他のユーザーがそのホームページを閲覧したときに実行させてしまう攻撃である。ユーザーがそのコードを実行した結果、対象のユーザーのクッキーやセッション情報が盗まれてしまう。

(3) SQL インジェクション（SQL Injection）

SQL インジェクションは、Web アプリケーションに SQL コマンドを挿入することによって、システムで使用しているデータベースを呼び出す攻撃手法である。たびたびニュースで報道される Web サイトからの個人情報漏えいは、SQL インジェクションによるものが多いと言われている。この攻撃は比較的簡単に発見しやすいものだが、SQL コマンドが実行されたときの被害は、そうとう大きいという特徴がある。

これらの攻撃方法は、電子タグに限ったものではなく、従来から知られているものである。今回の論文は、従来の攻撃方法を電子タグシステムに応用したものである。以下に、SQL インジェクションとコードインサーションを電子タグシステムに応用した実例を紹介する。

想定する電子タグシステムは、いくつかの R/W と 1 つのデータベースで構成する。パレットに貼付された電子タグには、タグの ID とパレットの内容物の情報が書き込まれている。電子タグシステムは、この電子タグのメモリーを読み込み、タグ ID と内容物の関係をデータベースに書き込み更新する。データベースの内容は WEB ブラウザに表示する。

正常な動作例を以下に記す。

(1) 電子タグのメモリーにタグ ID として"123"、内容物として"Apples"が書き込まれている。

(2) R/W で上記電子タグを読み取り、下記の SQL コマンドを実行しデータベース中のタグ ID（TagId）が"123"に該当する内容物の項目（OldContents）に"Apples"という値を上書きする。

```
UPDATE ContainerContents SET OldContents='Apples' WHERE TagId='123';
```

(3) このデータベースの内容は、WEB 上でパレット ID と内容物の関係の一覧を提供する。

以上のような処理をする電子タグシステムを想定する。

次に電子タグシステムが電子タグウィルスに感染する動作例を説明する。

(1) 電子タグのメモリーにタグ ID として"123"、内容物のデータを格納する領域には以下に示す特殊なコードを格納する。以下のコードは、自己複製を実行する SQL コマンドと、サーバーのバックドアを開けるコードが含まれている。

```
Apples', NewContents=(select SUBSTR(SQL TEXT,43, 127)FROM v$sql WHERE
INSTR(SQL_TEXT,'<!--#exec cmd=''netcat -lp1234|sh''-->')>0)--
```

(2) R/W は通常通り上記電子タグを読み取り、従来通り SQL コードを生成すると、次のようになり、データベース中の内容物（OldContents）の値が全て"Apples"になり、パレット積み替え後の内容物（NewContents）の値が全て上記特殊なコードに書き換わる。

```
UPDATE ContainerContents SET OldContents='Apples', NewContents=(select
SUBSTR(SQL_TEXT,43, 127)FROM v$sql WHERE INSTR(SQL_TEXT,'<!--#exec
cmd=''netcat -lp1234|sh''-->')>0)--' WHERE TagId='123';
```

(3) さらに Web ブラウザでこのデータを表示すると、上記のウィルスが発動し、サーバーのバックドアが開いてしまう。

以上のように、この論文では、特殊なコードが書かれた電子タグが市場にばらまかれると、各ユーザーの電子タグシステムがウィルスに感染していくことを示唆している。しかし、前述したようにこれらの攻撃手法は従来から知られており、様々な対策方法が考案されている。

例えば、コードインサーションの場合、サニタイジングが有効である。サニタイジングとは、入力データから HTML タグや JavaScript、SQL などの制御文字を検出し、無害な文字に置き換える処理のことである。上記の場合であれば、電子タグから読み取ったデータをデータベースに書き込む前に、"<"を"<"、">"を">"に変換すればスクリプトは実行されない。また、記号など使える文字の種類を制限するのも有効な対策方法である。

また、SQL インジェクションについても特殊文字を悪用することによって行われるため、文字種制限やサニタイジングが有効である。

まとめると、今回の電子タグウィルス問題は電子タグ技術の問題ではなく、システム側の問題である。電子タグシステムを構築するときは、このような攻撃を想定してセキュリティ対策をするべきである。

ちなみに、この「Is Your Cat Infected with a Computer Virus?」という題目は、電子タグをペットの体内に埋め込み管理する世界が近い将来やってくる可能性があることからつけられたようである。

5.1.3 まとめ

電子タグのセキュリティに関する脅威のほとんどは、従来から知られているものであり、状況に応じて様々な対応策が考案されている。電子タグを利用するシステムで、これらの脅威を防止するには、従来の対応策を参考にすればよい。ただし、対応策を実施することで、電子タグやシステムの性能が劣化したり、コストが高くなったりして利便性が落ちてしまう場合がある。電子タグに限らず一般的に言われることだが、タグの用途に応じて、利便性とセキュリティとのバランスを考慮し、最適な対応策を選択する必要がある。

5.2 電子タグのプライバシー保護に関する技術

前節では、電子タグシステムに対するいくつかの脅威について説明したが、そのほとんどが電子タグ特有のものではなく、従来からある攻撃方法を電子タグに応用したものであった。これらの攻撃方法の対応策もすでにあり、タグシステムに対しても有効であることを説明した。

しかし、電子タグのプライバシーに関しては、前節で述べてきたセキュリティとは区別して考える必要がある。セキュリティの場合は、パスワードの盗聴やウィルス感染などセキュリティが破られたときの損害規模が見積もれるため、利便性を考慮した対抗策が立てやすい。それに対してプライバシーの場合、個人それぞれの価値観が異なるため、プライバシー侵害の対抗策が立て難いという課題がある。

この背景の中、電子タグに関わる研究者や事業者は、電子タグ技術の開発や、電子タグの運用指針の制定など、あらゆる観点からこのプライバシー問題に取り組んでいる。電子タグのプライバシー保護技術に関する研究開発の歴史は 10 年に満たないが、様々な保護技術が提案されている。本節では、執筆時点で最新のプライバシー保護を中心に紹介する。

5.2.1 電子タグのプライバシー問題と保護技術の分類

電子タグのプライバシー問題として指摘されているポイントは、企業側が電子タグに書き込んだ商品コードやユニーク ID が消費者のプライバシーと結びつく可能性があることである。

電子タグの貼付対象物を識別するために、電子タグには商品コードを格納するケースが多い。この商品コードが格納された電子タグを消費者が所持しているとき､消費者が知らないところで、悪意のある第三者によってその商品コードが読まれ、所持しているものが何か知られてしまう可能性がある。そして、その所持品からその人の趣味、嗜好などセンシティブなプライバシー情報まで知られてしまう可能性がある。この問題をコンテンツプライバシー問題と呼ぶ。

電子タグ本体や電子タグの貼付対象物を個品単位で識別するために、電子タグにはユニークな ID を格納するケースが多い。この電子タグを消費者が所持しているとき、各地点に設置したリーダライタを用いてそのユニーク ID を読むことで、消費者の行動範囲や現在位置が知られる可能性がある。この問題をロケーションプライバシー問題と呼ぶ。

ただし、これらの情報をプライバシーと感じるかどうかは個人それぞれによって異なる。最も安全側に倒して、商品を消費者に渡す段階で例外なく電子タグを取り外すことにすると、プライバシーと感じない人に対して、電子タグを用いたサービスの提供ができなくなってしまうなどの課題がある。この課題に対して、電子タグを取り外したり無効化したりしないでプライバシーを保護する方式が多数提案されている。表 6-1 に、電子タグの実現時期、電子タグシステムにかかるコスト、消費者にかかるコストという 3 つの指標から特徴的なプライバシー保護技術を分類した。電子タグの実現時期については、電子タグとして既に実現可能なもの、現時点で可能になりつつあるもの、実現には数年かかりそうなものに分類している。電子タグシステムにかかるコストは、電子タグ自体のコストと電子タグを利用するシステムのコストの両者を含んでいる。消費者コストとは、プライバシー保護方式を実施するために消費者自身が行使する度合いを表している。プライバシー保護技術は、最近日本から発表されたものを中心に抽出した。

表 5-1　プライバシー保護方式の分類

電子タグ実現時期	既に可能	現時点	数年後
電子タグシステムコスト	なし	多少あり	高い
消費者コスト	あり	多少あり	なし
プライバシー保護方式	・ブロッカタグ ・クリップドタグ	・可変秘匿 ID 方式 ・ALOHA 方式 ・通信距離制限方式	・ハッシュロック ・ハッシュチェーン ・K 段 ID 照合方式 ・セキュア RFID

各プライバシー保護方式について、以下に説明する。2006 年 3 月に ECOM が発行した「企業間情報共有基盤整備報告書」（参考文献[3]）にて報告した保護方式の中で、大きな進展が無いものは概略にとどめる。

(1) ブロッカタグ(参考文献[4])：ブロッカタグと呼ばれる装置が R/W に対して妨害電波を発信し、目的の電子タグと通信しづらくすることでプライバシーを保護する方式。2003 年に RSA 社の Ari Juels 氏等によって提案された。

(2) 可変秘匿 ID 方式（参考文献[5]）：電子タグのメモリー上には秘匿化したユニーク ID のみを格納し、その ID を逐次更新することでプライバシーを保護する方式。2004 年に NTT 社の木下真吾氏等によって提案された。

(3) ハッシュロック（参考文献[6]）：電子タグがハッシュ演算を用いて R/W を認証することでプライバシーを保護する方式。2002 年に MIT の Stephen August Weis 氏等によって提案された。

(4) ハッシュチェーン（参考文献[7]）：電子タグがハッシュ演算を用いて毎回異なる値に秘匿化した ID を応答することでプライバシーを保護する方式。2003 年に NTT の大久保美也子氏等によって提案された。

5.2.2　クリップドタグ

電子タグのアンテナを切断し通信距離を短くすることでプライバシーを保護する方式である。2005 年に IBM 社の Gunter Karjoth 氏と Paul Moskowitz 氏によって提案された。この技術は、2006 年 11 月にカナダのマーレン RFiD 社にライセンスしたことが発表され、クリップドタグが本格的に製造を開始されている。（参考文献[8]）

クリップドタグは図 5-1 に示すように、ミシン目が付いた電子タグである。消費者が、第三者に電子タグを読み取られたくないとき、ミシン目に沿ってタグを切り取ることで、電子タグのアンテナを短くして、電子タグの通信距離を数 cm にすることができる。また、発明者の Paul Moskowitz 氏は、消費者がタグの一部を切り離したことを目視で確認することで、自らプライバシーを守ることができると述べている。（参考文献[9]）

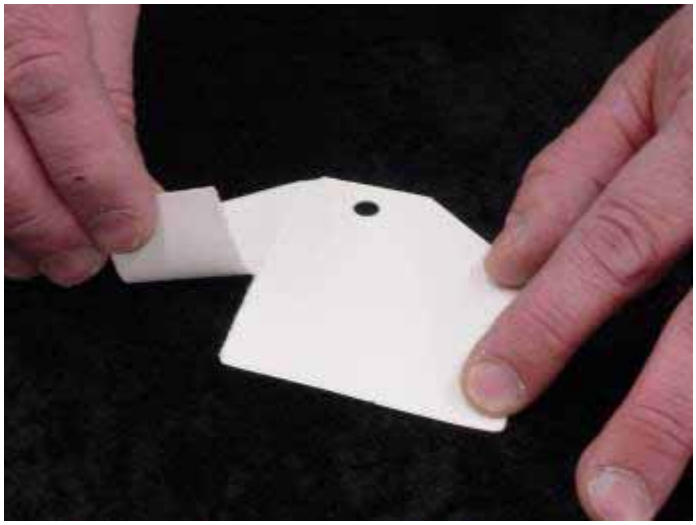

図 5-1　クリップドタグ

5.2.3　ALOHA 方式

電子タグに格納するユニーク ID は、しばしば電子タグを識別するために利用する。しかしこのユニーク ID はロケーションプライバシー侵害を誘発する可能性が高い。これに対して、電子タグの擬似乱数発生器が生成したハンドル値で R/W が電子タグを識別し、ユニーク ID は使わないようにすることで、プライバシーを保護することができる。ハンドル値を使って R/W が電子タグを識別する方式の一つに ALOHA 方式がある。この方式自体は、従来からあったが、最近規格化された EPC Class 1 Generation 2(参考文献[10])や ISO/IEC 18000-6 Type C（参考文献[11]）、響プロジェクト仕様（参考文献[12]）の電子タグに採用・実装されている。

ALOHA 方式はプライバシー保護方式というよりは、複数の電子タグを一括して読み取る輻輳制御方式である。したがって、電子タグを識別して輻輳制御するためには、必ずタグにユニーク ID が必要だから、ロケーションプライバシー問題が生じるという解釈は、必ずしも全ての電子タグが該当するわけではない。ユニーク ID が無くても輻輳制御が可能な電子タグも存在するため、消費者に渡す段階でユニーク ID が格納されていなければロケーションプライバシーは保護可能である。

ALOHA 方式について説明する。複数の電子タグを一括して読み取る際、同時に複数の電子タグが応答すると通信に失敗するため、ALOHA 方式は電子タグの応答する順番を決める。応答する順番は、R/W が指定するのではなく、電子タグ自身に決めさせる。順番を決める方法は、電子タグの擬似乱数発生器を用いて生成した乱数を順番とする。図 5-2 に ALOHA 方式を使って 3 つの電子タグを輻輳制御する例を示す。

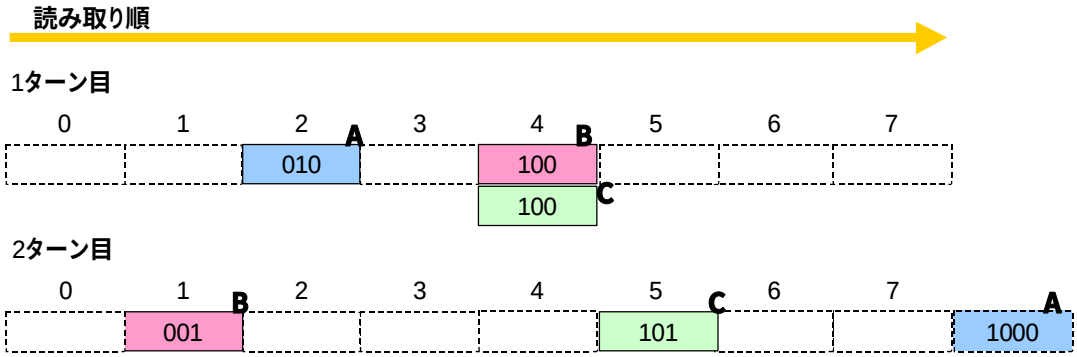

図 5-2　ALOHA 方式

(1) 1 ターン目の開始時に、R/W の要求に従い 3 つの電子タグ（A、B、C）が 0 から 7 の範囲で乱数を生成する。ここでは、A が 2 番、B と C が 4 番を生成した。
(2) R/W は乱数が小さい順に電子タグを読み取っていく。最初に A を読み取る。
(3) 次に B と C とを同時に通信を試みるが、信号が衝突するため通信に失敗する。
(4) 1 ターン目が終了する。
(5) 2 ターン目でまた電子タグは（B、C）が 0 から 7 の範囲で乱数を生成する。ここでは、B が 1 番、C が 5 番を生成した。A は 1 度読み取ったので番外となる。
(6) R/W は乱数が小さい順に電子タグを読み取っていく。最初に B を読み取り、最後に C を読み取る。

この方式により輻輳制御を可能にすると共に、電子タグにユニーク ID を格納しなくても良いことからロケーションプライバシー問題に対しても有効である。

5.2.4　電子タグ通信距離制限方式

通信距離を調節する機能を電子タグ側に持たせることでプライバシーを保護する方式である。2006 年度の経済産業省委託事業であるセキュア電子タグプロジェクトにて日立製作所等が研究開発した技術である。開発対象の電子タグは、UHF 帯のパッシブタイプで、ISO/IEC 18000-6 Type C 規格の仕様をベースに開発された。（参考文献[13]）

このセキュア電子タグプロジェクトは、製品ライフサイクル全体へのタグの適用を考え、消費者のプライバシー保護と、保守・リサイクル段階でのタグの再利用を両立させる方式の開発を目的として進められた。その方式の一つが通信距離制限方式である。この方式は、電子タグが外から見えない形で実装される場合でも、電子タグを破壊することなく通信距離制限を行うことが可能である。また、必要に応じて保守・リサイクル段階での通信距離制限の解除も可能にする。図 6-3 に通信距離制限方式の概念図を示す。この電子タグは、通常の通信距離状態では R/W との距離が数十 cm でも数 m でも読取可能である。通信距離制限方式を実施し、通信距離を制限した状態では、R/W との距離が数十 cm では読み取れるが、数m離れると電子タグは応答しなくなり読み取れなくなる。

この通信距離制限機能は、永久に距離制限するモードと、あらかじめ設定したパスワードで認

証することで距離制限したり解除したりすることが可能なモードの 2 つのモードを持っている。

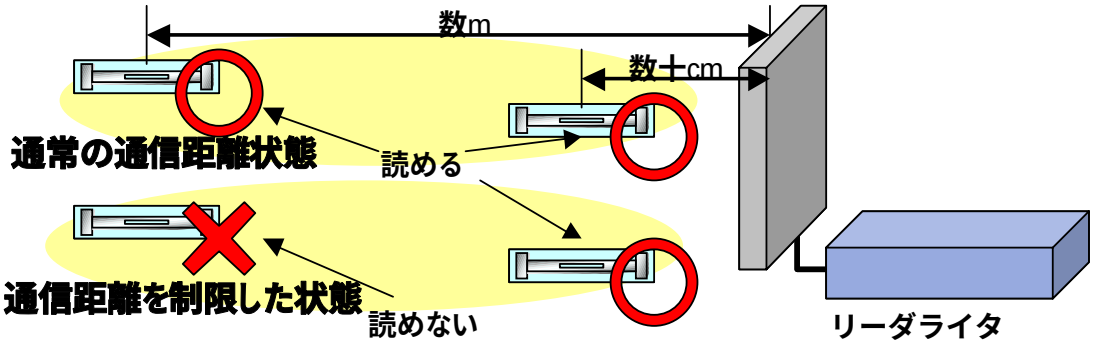

図 5-3　通信距離制限方式

セキュア電子タグプロジェクトは、2006 年 8 月に開始され、2007 年 2 月に通信距離制限機能を搭載した電子タグの試作機が完成した。この電子タグはいくつかの業界で評価されている。

5.2.5　暗号回路搭載方式

その他、数年先に実現可能とされるプライバシー保護方式として、K 段 ID 照合方式とセキュア RFID がある。両者ともにハッシュロック方式やハッシュチェーン方式と同様に、電子タグに暗号回路を搭載する方式である。

K 段 ID 照合方式は、電子タグの ID を K 個に分割しアプリケーションごとに割り振り、分割した ID は、乱数と共に電子タグ側でハッシュ演算してリーダライタと通信することでプライバシーを保護する方式である。2005 年に九州大学の野原康伸氏等によって提案された（参考文献[14]）。ハッシュチェーン方式をベースにしているため第三者によるリンク不能性を実現しており、さらにハッシュチェーン方式の課題であるサーバー側での認証処理負荷の削減も実現しており大規模システムでの適用可能であることが特徴である。

セキュア RFID は、IC カードでの利用実績のある暗号アルゴリズム MISTY（参考文献[15]）を、EPC Class 1 Generation 2 の電子タグに搭載することでプライバシー保護やセキュリティ向上を実現した電子タグである。2006 年 9 月に三菱電機の亀丸敏久氏等によって提案された（参考文献[16]）。搭載する暗号アルゴリズムとしては、高いセキュリティ強度を持ちかつ比較的低消費電力である MISTY を選択した。試作機では、EPC Class 1 Generation 2 の電子タグに暗号化機能と相互認証機能を追加し、盗聴やなりすましの対策を実現した。

現時点では、電子タグに IC カード並みの暗号回路をそのまま搭載することは、タグの IC チップのサイズ拡大や消費電力量の増大、処理速度の劣化を引き起こし、読取距離性能や複数一括読取の性能が落ちると考えられている。しかし、これらの技術的課題は今後の半導体技術の進歩により解決されると考えられている。

5.2.6　プライバシー保護法式のロードマップ

プライバシー保護方式に関するロードマップを図 6-4 に示す。それぞれのプライバシー保護方式について、提案された時期と適用可能になると予想する時期を示している。

ブロッカタグ、クリップドタグ、可変秘匿 ID 方式は、電子タグ自体の制約が無いため既に実現可能としている。ただし本格稼動は、運用面での課題を解決してからになると考えられる。

ALOHA 方式自体の提案時期は古いが、ここでは UHF 帯電子タグに ALOHA 方式を搭載した EPC Class 1 Generation 2 が規格化された時期を提案時期としている。この方式は、EPC Class 1 Generation 2 の電子タグはもちろん、ISO/IEC 18000-6 Type C や響プロジェクトの電子タグにも搭載され実現している。

通信距離制限方式は、試作レベルでは実現しており、実現可能時期は遅くないと思われる。

ハッシュロック、ハッシュチェーン、K 段 ID 照合方式、セキュア RFID は、電子タグに暗号回路を搭載する必要があるため、実現可能時期は他の方式より遅くなると考えられる。

参考までに、MIT や EPCglobal、総務省・経済産業省共管のプライバシー保護に関するガイドラインの発表時期や、EPCglobal、ISO、響プロジェクトの UHF 帯電子タグの仕様公開時期を併記した。また、米国消費者団体「CASPIAN」による不買運動など電子タグ運用に対して警告された時期も併記した。

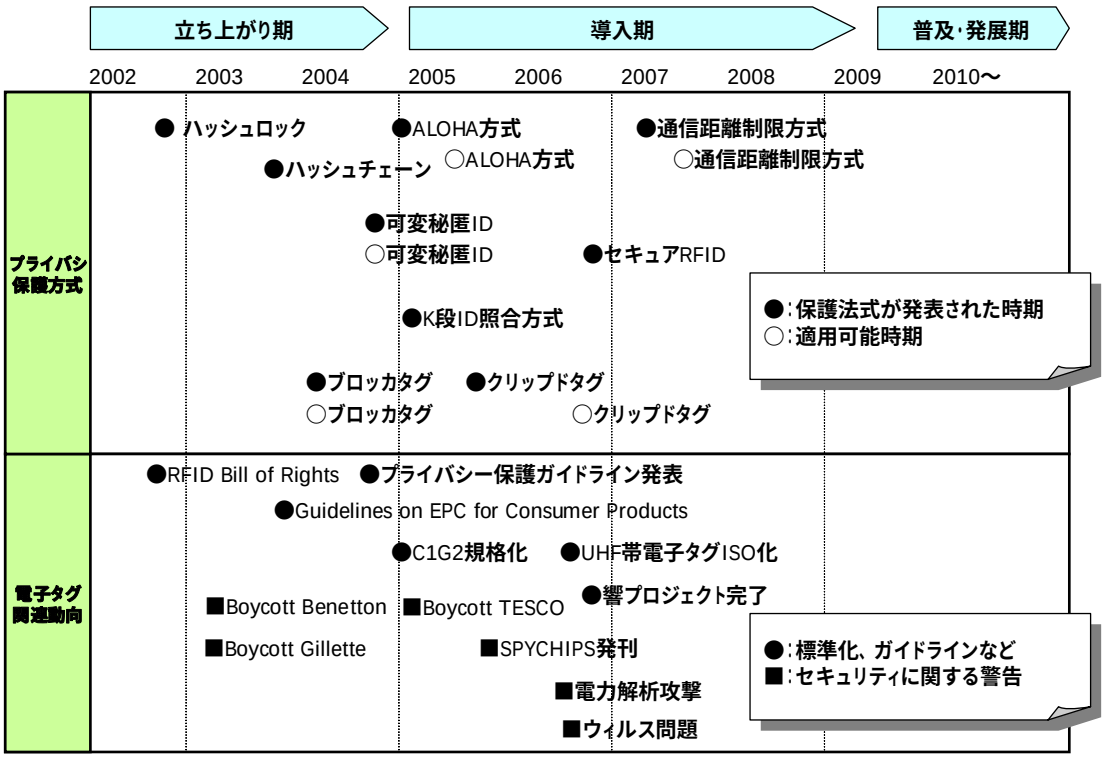

図 5-4　プライバシー保護方式のロードマップ

<参 考 文 献>

[1] Yossi Oren and Adi Shamir, "Power Analysis of RFID Tags", http://www.wisdom.weizmann.ac.il/~yossio/rfid/, 2006.

[2] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?", IEEE. PerCom '06, 2006.

[3] 次世代電子商取引推進協議会,「平成17年度エネルギー使用合理化電子タグシステム開発調査(企業間情報共有基盤整備)企業間情報共有基盤整備報告書」, 平成17年度経済産業省委託調査, 2006.

[4] Ari Juels, Ronald L. Rivest, and Michael Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy", ACM CCS '03, 2003.

[5] 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プライバシー保護方法」, 情報処理学会論文誌, vol. 45, No. 8, pp. 2007-2021, 2004.

[6] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels, "RFID Systems and Security and Privacy Implications", CHES '02, LNCS, vol. 2523, pp. 454-469, 2002.

[7] Miyako Ohkubo, Koutarou Suzuki, and Shingo Kinoshita, "Cryptographic Approach to a Privacy Friendly Tag", RFID Privacy Workshop, 2003.

[8] Guenter Karjoth and Paul Moskowitz, "Disabling RFID Tags with Visible Confirmation", WPES '05, 2005.

[9] Paul A. Moskowitz, Andris Lauris, and Stephen S. Morris, "Privacy-Enhancing Radio Frequency Identification Tag: Implementation of the Clipped Tag", White Paper, RFID Journal Live, 2006.

[10] EPCglobal Inc., "Class 1 Generation 2 UHF Air Interface Protocol Standard Version 1.0.9", EPCglobal Inc., 2004.

[11] ISO/IEC 2006, "Information technology - Radio frequency identification for item management - Part 6: Parameters for air interface communications at 860 MHz to 960 MHz AMENDMENT 1: Extension with Type C and update of Types A and B", ISO/IEC 18000-6:2004/Amd.1:2006(E), 2006.

[12] 株式会社日立製作所,「平成17年度エネルギー使用合理化電子タグシステム開発調査事業(UHF帯電子タグの製造技術及び実装技術の開発)」, 平成17年度経済産業省委託事業, 2006.

[13] 株式会社日立製作所,「平成 18 年度エネルギー使用合理化電子タグシステム開発調査事業（UHF 帯電子タグの技術開発事業）」, 平成 18 年度経済産業省委託事業, 2007.

[14] 野原康伸, 井上創造, 馬場謙介, 安浦寛人,「リンク不能性を実現し大規模 RFID システムに適用可能な ID 照合プロトコル」, SCIS '05, 2005

[15] 松井 充,「ブロック暗号アルゴリズム MITSY」, 1996 信学技報, ISPC96-11, 1996.

[16] 荒川智史, 服部孝, 舩倉英俊, 西川浩司, 亀丸敏久,「UHF 帯 RFID におけるセキュリティ対策」, 2006 年電子情報通信学会基礎・境界ソサイエティ大会, 2006.

6. 電子タグの廃棄問題について

6.1 環境問題と電子タグ

今まさに世界が直面している「地球温暖化」に顕現される地球環境問題は、今世紀人類最大の課題とされているが、我国の産業界においても省エネルギー・省資源や廃棄物削減などの環境マネジメントに取り組み、人と地球環境が調和する持続可能（サスティナブル）社会の実現にどう対応していけるかがますます重要なテーマとなっている。

電子タグは、貼付する対象の個体それぞれを識別できると同時に、個体ごとの様々な履歴を逐次記録できるという優れた機能により、サプライチェーンの上流から下流までの様々な場面で活用されることで、生産・物流・販売にわたるトータルな効率化を促進し、結果として省エネルギーや炭酸ガス排出削減に貢献できるだろうと考えられている。

またその機能を活用することによって、廃棄が必要とされるモノや部品と廃棄すべき時期を自動認識することが可能となり、廃棄する際の分別を容易にすると同時にリユースやリサイクルをスムーズに進める極めて有効な媒体とも考えられ、サスティナブル社会に欠かすことの出来ない役割が期待されている。

しかし一方で、段ボール箱など輸送梱包への電子タグ貼付利用が始まろうとしているが、電子タグが貼付されたままの段ボールを従来と同じようにリサイクルできるかは、使用される各種の電子タグについて充分に検討されねばならない。現状すべての電子タグには微量とはいえ金属成分が含まれているため、段ボール箱のリサイクルを阻害する要因となってしまう可能性が存在するからである。

さらに近い将来、電子タグが広く普及した段階では、貼付対象である膨大な数の商品などと一緒に電子タグ自体も取り外されずに廃棄される場合が多いと予想されるが、個々の電子タグは小さく微量であっても総量としては問題となる可能性が出てくる。

圧倒的なボリュームの産業廃棄物や建築廃材、日々排出される家庭ゴミなどと比較した場合、電子タグの廃棄などは将来的にも極めて微小な量に過ぎず問題にならないとの意見もあるが、一般的に「問題が発生してから対処するコストより、事前に予防策を講じておくコストの方がはるかに安い」との視点からも、導入期である今のうちに将来の様々な普及シーンを想定して「電子タグ自体の廃棄問題」を考えておくことは極めて重要なテーマと言えよう。

現在、社団法人日本自動認識システム協会(JAISA)では電子タグ廃棄問題を考える WG を設立し、廃棄されるタグの問題点と対応策につき検討を重ねているが、本稿はそこで検討された内容も紹介しつつ電子タグ自体の廃棄に関する課題を概観するものである。

6.2 電子タグの組成

電子タグ（現在普及している 13.56MHz ラベル状タグで例示）の構造と組成は下の図と表の通りである。重量比から明らかなように IC チップのシリコンはきわめて微量であるが、アンテナ素材である銅、銀（ペースト）、ベース素材である PET などは大量廃棄されたときに問題となる可能性がゼロではない。

一般的な電子タグで使われている IC チップのシリコンについて試算した結果では、1,000 万枚

でも茶碗一杯分の量にしかなりません。ただしアンテナ素材のアルミや銅、さらにベースの PET は電子タグの種類と大きさによっては相当量となり、環境への影響を検証する必要があると考えられます。

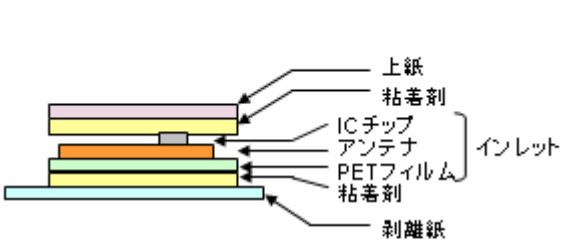

図 6-1 IC タグの構造

・通信周波数:13.56MHz
・規格:ISO／IEC15693
・製品形状:ラベル

部材	主要構成材料	重量／ICタグ1枚
IC	シリコン	0.35[mg]
ACP	エポキシ	0.19[mg]
	ニッケル	0.1[mg]
バンプ	金	0.0024[mg]
アンテナ	アルミニウム	122[mg]
	銅	401[mg]
	銀(銀ペースト)	236[mg]
	樹脂(銀ペースト)	32[mg]
ベース	PET	302[mg]
ラベル材料	PET	756[mg]
	アクリル酸エステル共重合体	270[mg]

図 6-2 IC タグ組成材料

6.3 電子タグ廃棄の現状

すでに電子タグが実導入されている国内の現場では、電子タグがどのように廃棄されているのであろうか。

電子タグが導入されている全国の図書館数ヶ所にて現況をヒアリングした JAISA 調査結果によると、収蔵されている書籍が破損した際には電子タグがまだ高価なためもあって、簡単に剥されないように貼り付けられている電子タグを鋏で切り取りできるだけリユースしているとのことであった。

また数少ない事例ながら電子タグが不良化した際は、タグのアンテナを鋏やカッターで断線（キル）して不燃ゴミとして廃棄したり、あるいは廃棄方法が不明であるため捨てずにそのまま保管したりしているケースもあった。

電子タグの活用が導入されようとしている段ボールでは、タグが貼付されたままの段ボールを溶解する場合、アンテナを形成する金属や IC チップの大きさと厚みによっては、リサイクル工場での金属探知器が感知して溶融がストップしたり、感知されずにそのままリサイクル製品に混入されてしたりしてしまう心配もあるため、現在様々な電子タグを使ってリサイクル性の実験検証が進められているところである。

一方、海外での電子タグ廃棄状況はどうなっているのであろうか。

米国ではウォルマートなど量販店による納品メーカーに対する電子タグ使用の義務付けを受けて、メーカー製品の段ボール箱、リサイクル金属、リユース容器に貼付された電子タグが、回収された段ボール箱や金属のリサイクル、容器の再利用に際して、環境面、安全性、効率性の各側面でどのような影響を与えるかにつき、連邦環境庁（EPA)、段ボールメーカー、リサイクル業者などの関連業界を中心に議論がすでに始まっている。

正式結論はまだ出ていないようであるが次のような報告がされている。

①製品の段ボール箱に貼付されたフィルムベースの電子タグは、リサイクル工程でフィルターによって除去できる。

（なお日本で進められている実験では、除去しきれないケースも出ている）

②段ボール箱に貼付された電子タグで銀ペーストなどのアンテナにチップを実装したものは、段ボールのリサイクル工程で銀ペーストが排水に混入したり、リサイクル製品に残留したりすることでの影響が懸念される。

ただし、いずれも人体や環境への影響は小さく無視できる可能性が高い。

（なお同報告におけるリサイクル製品への残留に関する懸念では、段ボールの品質について言及されていないが、日本の品質基準では懸念される課題である）

③アルミ、鉄などの金属に電子タグを付けたままで金属リサイクル工程に投入した場合、タグのアンテナの銅成分が金属に混入してリサイクル金属製品の品質を劣化させる可能性がある。

以上が指摘されている。

6.4 電子タグ廃棄の法規制

日本における環境と廃棄問題に関する各種法制度の考え方は、「持続可能な発展」を理念として 1993 年に制定された「環境基本法」がすべての基準となっている。2000 年には廃棄物の適正処理および再資源化、リサイクルに対応するため「循環型社会形成推進基本法」が制定され、廃棄物の抑制や循環的な利用が事業者の責務とされた。2001 年に改正された「資源有効利用促進法（リサイクル法）」では 3R（Reduce、Reuse、Recycle）の概念が導入されている。

電子タグについて直接言及する法規はまだないが、電子タグの廃棄やリサイクルも基本的には上記の法理念に準じ考えられねばならない。

さらに電子タグの廃棄に際しては、前記の段ボールの例に止まらず、電子タグが単独で利用され廃棄されるケースは少なく、何らかの媒体、商品やパッケージ・出版物などに封入されたり貼付されたりして使われ、それらと一緒に廃棄されることが大半と考えられる問題がある。

貼付対象の媒体（モノ）にはそれぞれ関連法規があり、現状では「容器包装リサイクル法」、「家電リサイクル法」、「建設資材リサイクル法」、「食品リサイクル法」、「自動車リサイクル法」にてリサイクル基準が設けられていて、一緒に廃棄される電子タグも原則、各リサイクル法に準じた対応が必要とされる。

例えば容器包装リサイクル法では、容器の再資源化のために消費者は使用済み容器を分別して排出することが義務付けられているが、分別されたガラス瓶、ペットボトル、プラスチック容器、紙パックのそれぞれに電子タグが貼付されたまま回収された場合、容器ごとの再商品化に対して電子タグがどんな影響を及ぼすかにつき各関連業界との検討が必要になってくる。

国際的にも EU では、電気電子機器に含まれる有害 6 化学物質（水銀、カドミウム、鉛、六価クロム、ポリ臭化ビフェニール、ポリ臭化ジフェニエール）の使用制限規制「RoHS」指令が 2006 年 7 月から施行されましたし、2007 年 6 月からは、家電、自動車、化学品など多くの業種に対して約 3 万の化学物質の安全評価を義務づける「REACH」も実施される予定である。

今後、電子タグを環境対応の視点で徹底管理するためには、環境管理の主たる手法とされ、設計や原材料調達から消費、廃棄までの製品生涯全体にわたる環境負荷を評価する LCA（ライフサ

イクルアセスメント）を電子タグに適用することも必要と考えられている。しかし電子タグの場合、貼付対象物のサプライチェーンの様々な段階で活用されうるだけに、それぞれのケースによって電子タグのライフサイクル始点と終点は必ずしも一様でなく、責任や費用負担に関しても、貼付対象物を取り扱う各流通主体のどこが担うかなど今までにない困難な要素が多く存在している。

6.5　今後の方向性（本格普及の前にすべきこと）

かつて塩化ビニールが製品素材のネガティブ基準となってしまったが、その教訓を生かし、電子タグが最終的にグリーン購入（環境負荷の小さい製品を優先的に買う）基準のネガティブな対象とならないよう、ユーザーや社会に対してアピールしていかねばならないし、その根拠となるデータを揃えておかねばならない。

具体的には次のようなフェーズを踏み、環境への対応策を取っていくべきであろう。

フェーズ 1：RoHS 指令の 6 物質を含まない
フェーズ 2：廃棄物（一般・産業）として、他のゴミと一緒に処理しても問題ない
フェーズ 3：他の循環資源をリサイクルする際に禁忌品とならない
　　グリーン購入のネガティブ基準とならない
フェーズ 4：大量の電子タグを集めればタグ自体がリサイクルできる
フェーズ 5：電子タグそのもののグリーン購入基準ができる（グリーン製品となる）

現状での電子タグ組成材料はフェーズ 1 をクリアーしている。廃棄量はまだ微々たるもので環境問題となるレベルにないが、フェーズ 2〜3 についての実験や検討を重ね、将来の大量普及した段階に備えねばならないし、貼付対象物リサイクルや電子タグ自体のリサイクル過程で問題物質が濃縮される可能性など、考えられる様々なワーストシナリオをも想定しておく必要がある。

そのワーストシナリオに準じた廃棄実験検証（焼却、溶解、土中投棄ほか）を重ねてデータを揃えておくと同時に、これから電子タグを導入していくユーザーに対して、電子タグの LCA 実態をヒアリング調査しておくことも必要であろう。

最終的には各方面での実験や研究の成果をベースにして、フェーズ 4〜5 に適合する電子タグの供給が望まれる。

将来の普及を見据えてできる限りの廃棄対策を考え、環境保全上の障害を未然に防止する体制を整えておく――「未来のために今すべきことをしておく」ことが、21 世紀のキーテクノロジーたる電子タグに課せられた 21 世紀的スタイルだと言えよう。

電子タグ利活用における事業者向け消費者保護の指針
－H18 年度改訂版－

序文

この指針は、消費者を相手方とする電子タグ利活用を行う事業者などが、電子タグの有用性を利活用しつつ、消費者の利益を確保し、電子タグが円滑に社会に受け入れられるようにするため、電子タグ利活用取引における消費者保護と公正な執行を図るための不可欠な要件を、指針として定めたものである。この指針が、事業者と消費者双方にとって有意義に利用されることを期待する。

1. 適用範囲

この指針は、消費者を相手に国内で電子タグ利活用を行う事業者に適用する。

2. 引用法規等

次に掲げる法律・ガイドライン等は、この指針に引用されることによって、この指針の規定の一部を構成する。これらは、その最新版を適用する。

・個人情報保護法
・電子タグプライバシー保護ガイドライン
・JIS Q 10002「品質マネジメント-顧客満足-組織における苦情対応のための指針」

3. 定義

この指針で用いられる主な用語の定義は、次による。

a) 電子タグ

IC チップとアンテナにより構成され、物品等に装着されるものであって、その中に当該物品等の識別情報その他の情報を記録し、電波を利用することによりこれらの情報の読み取り又は書き込みができるものをいう 。

b) 事業者

事業として、商品、サービスなど（以下、「商品等」）の売買を、電子タグの利活用によって行う者。

c) 消費者

個人。ただし、個人が事業として又は事業のために電子タグ利活用場面提供の当事者となる場合は、当該個人を事業者として取り扱う。

4. 消費者に対する情報提供

4.1 消費者への明瞭、正確な情報提供

事業者が消費者に対して行う情報提供のうち、下記の内容については経済省･総務省共管の「電子タグプライバシー保護ガイドライン」（2004.6）に準拠する。

1. 商品に電子タグが装着されていることの表示、及び店舗内の読取装置設置表示など

2. 電子タグの読み取りに関する消費者の最終的な選択権の留保
3. 電子タグの社会的利益などに関する情報提供
4. 電子計算機に保存した個人情報データベースと電子タグの情報を連携する際の取り扱い
5. 電子タグ内に個人情報を記録する場合における情報収集および利用の制限
6. 電子タグ内に個人情報を記録する場合における情報の正確性の確保
7. 情報管理者の設置
8. 消費者に対する説明および情報提供

4.2 上記以外の消費者に提供必要な情報の具体的内容

4.2.1 電子タグ読取装置設置の通知と表示

事業者は、消費者がその事業者の電子タグ利用を明確に認識できるように、電子タグを読み取るリーダー（読み取り機）の存在とその位置・場所を表示する。

4.2.2 記録される情報項目の公開

電子タグが貼付・装着された商品を販売する事業者は、電子タグ貼付・装着商品についてこれに記憶される情報項目、電子タグ内のキー情報から検索されるデータベースに記憶される情報の項目を全て公開する。

4.2.3 電子タグ情報利用に関する問合せ方法と窓口

事業者は、電子タグに関連する消費者からの問い合わせ方法と窓口を表示する。

4.3 情報提供･告知等の方法

消費者に対する情報提供・告知等の方法は、次による。

①提供手段

（1）事業者ホームページ・配布パンフレット・契約書類（会員申込み用）等

（2）店内ディスプレイ・店頭看板・店頭掲示板等

（3）電子タグ装着商品自身もしくはそのパッケージ

（4）消費者のPC・PDA・携帯電話等への電子的メッセージ

②提供記述内容

（1）文章もしくは画像及びそれらの組合せ

（2）電子タグマーク（認知可能なレベルが前提）もしくはシール等の張り付け

4.4 責任の明確化

事業者は、電子タグ利活用で予想されるトラブルについて、第三者の苦情処理団体等がみても、一方的に消費者が不利にならないような合理的なリスク分配を行い、店舗における苦情処理窓口の責任者名・連絡先等を消費者にわかりやすく、理解できるように明示する。また、消費者が非合理的なリスクを負うことのないような方策を講じる。

5. 安全管理等

5.1 電子タグ関連システムの安全管理

5.1.1 安全管理

事業者は、電子タグ利活用に関わるシステム運営を行う場合、システム情報への不当なアクセス又は情報の消失、破壊、改ざん、漏えいなどの危険に対して、情報セキュリティの各規格や各種ガイドライン等からみて十分な安全対策を行う。また、事業者が安全対策をとっているにも関わらず、予期せぬ障害が発生した場合には速やかな復旧に努めると同時に、障害の状況に応じて消費者に対して告知その他の適切な対応をする。

5.2 委託

事業者は、電子タグ利活用に関わる技術面、組織面及び設備面において外部委託を行う場合、十分な安全性が確保できる委託先を選択する。また、事業者は、障害が委託先で発生した場合であっても、消費者に対し障害の状況に応じて適切な告知や対応を行う。
特に個人情報を含むデータを委託する際には、個人情報保護法に沿った委託管理をすること。
また、再委託については、委託先に事前確認のうえ、委託契約上にその安全管理責任の範囲を明記する。

5.3 取引データのバックアップ等

電子タグ利活用データの保管に当たっては、定期的なバックアップ、フェールセーフなど、適切な措置を講じる。

5.4 装置等の管理･保守

事業者は、電子タグ利活用時に使用する電子計算機、端末機器、周辺機器及び回線並びに当該機器に使用されるソフトウェアについて、安定性・安全性を十分に確認する。また、定期的な保守点検、改善などを実施し、安定性・安全性の維持に努める。

6. 個人情報

個人情報の保護に関しては、個人情報保護法、電子タグに関するプライバシー保護ガイドラインなどを参考に徹底を図ること。また、個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを作成・維持・改善を行うことが望ましく、その体制の整備に当たっては、日本工業規格JIS Q 15001「個人情報保護マネジメントシステム－要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格JIS X 5070「セキュリティ技術－情報技術セキュリティの評価基準」、日本工業規格JIS Q 27001「情報技術－セキュリティ技術－情報セキュリティマネジメントシステム－要求事項」、日本工業規格JIS Q 27002「情報技術－セキュリティ技術－情報セキュリティマネジメントの実践のための規範 」、個人データの安全管理措置の実施状況の確認に当たっては、経済産業省の「情報セキュリティ監査制度」を、それぞれ参考にする。

7. 万人（子ども、高齢者を含む）に対する配慮

7.1 子どもの理解力への配慮

子ども（通常13歳未満）を主たる対象とする電子タグ付商品等を販売する事業者は、対象とする年齢層の子ども知識、理解力、判断力などに配慮し、平易で、正確、かつ、誠実な表現を用いて、子どもがその提供情報を正確に理解できるよう配慮する。
特に13歳未満の子どもから個人情報を収集する際は、明確な親の同意を得る。

7.2 高齢者等、万人への特別な配慮

事業者は、高齢者・ハンディキャップのある方等も含めた消費者、万人の利用を念頭に置きつつ、情報提供方法、内容等について子ども同様に、理解力、判断力などに配慮し、平易で、正確、かつ、誠実な表現を用いて特別な配慮をする。

8. 医療機器・人体影響への配慮

総務省で実施されている**「電波の医療機器等への影響に関する調査」**（電商品監視機器、無線LAN 機器等が植込み型医用機器へ与える影響について）を参照する。

9. 苦情処理体制の整備

苦情対応に関しては、JISQ10002「品質マネジメント－顧客満足－組織における苦情対応のための指針」を参考する。

10. 個人の所有物に貼付された電子タグの所有者同意無しでの読取の禁止

読取機・読書機を所有する事業者は、いかなる目的・理由があっても、個人の所有にかかる物品（当該事業者外の販売品）及び個人の「所有」となる前で個人を特定できる物品に貼付・装着された電子タグから情報を所有者の許諾なしに読取りまたは書込みを行ってはならない。
電子タグ情報を読取る場合、もしくはその可能性のある場合は事前に消費者に通知し、その同意を得た場合のみとし、了解が得られない場合は読み取った情報は削除する。

11. 防犯カメラ等他のネットワーク接続機器との連動利用の告知

店舗等において、消費者が、所有権が事業者にある商品を手に取った際などに、商品に添付された電子タグを読取り、防犯カメラで撮影した個人の画像と商品の ID を連携できるシステムなどを設置する場合には、その旨を店舗の入口等に明瞭に掲示する。

12. 裁判外紛争処理

当事者間での解決が図れない場合、事業者は信頼できる第三者機関などの関与を通じた迅速、公正かつ消費者の使いやすい裁判外紛争処理（ADR：Alternative Dispute Resolution）メカニズムが利用可能であれば率先してそれを利用する。
（EC関連の民間苦情処理団体や認定個人情報保護団体等を含む）

13. 法律の遵守

事業者は、前述の個人情報保護法を含めて、電子タグ利活用に関連して適用される関係法令の定めを遵守する。

付属資料

Ⅰ. 米 CDT ガイドライン：RFID テクノロジーの配備のためのプライバシーのベスト・プラクティス（2006 年 5 月）

Ⅱ. カナダ・オンタリオ州 IPC の RFID プライバシー・ガイドライン（2006 年 6 月）

米 CDT ガイドライン：RFID テクノロジーの配備のための プライバシーのベスト・プラクティス

暫定ドラフト
2006 年 5 月 1 日

概要

無線を利用した認識（RFID: Radio Frequency Identification）テクノロジーの独創的な応用に、消費者、企業、および政府機関は期待をかけている。それにより示唆される可能性として、さまざまな応用があるが、たとえば在庫管理の改善によるコストの削減、薬剤供給の安全性の向上、高齢者と障害者の介護の支援、病院での医療過誤率の低減、空港での手荷物と貨物の追跡の改善によるセキュリティと旅客サービスの改善などがある。

RFID は、大きなプライバシー問題を引き起こさずに多くの応用が可能である。しかし、RFID デバイスが個人識別情報（PII）にリンクできる範囲で（そのようなデバイスにより可能になる個人の位置の追跡も含め）、RFID はプライバシーに関する重要な疑問を提起する。この資料は特に PII の制御に関して、このようなプライバシーが意味するものに取り組むことを主に意図しているが、消費者に関わる RFID テクノロジーの使用についての透明性を向上させることもその目標である。

RFID とは何か?

RFID とは、対象を識別するために電波を使用するテクノロジーのことである。RFID システムは一般に、タグ、リーダー、およびデータベースの 3 つの要素で構成される。

RFID タグ（トランスポンダー）は、対象を識別する固有番号（および場合によっては他の情報）が含まれるチップで構成され、アンテナに接続されている。それぞれのアンテナによりチップは電波を用いてリーダーと通信することができ、リーダーはタグ上の固有番号または他のデータを取り込む。次いでそのデータは、タグが添付されている対象に関する情報を保管しているコンピュータに伝送できる。たいていの場合、リーダーとタグとの間の通信プロトコルにより、一定のコマンド・セットが実行できる。一般にタグには付加的なソフトウェア・プログラムをアップロードして実行する機能はない。

RFID タグ

最も単純な RFID タグは「パッシブ」であり、受動であるためデータ伝送を可能にする固有の電源機構は備えていない。パッシブ・タグは、リーダーが放出する電磁波から電力を受信してタグ内に電流を発生させ、これによってタグに保管されている情報の伝送が可能になる。他のタグは「アクティブ」であり、何らかの形の電源機構を備えているので情報をリーダーにブロードキャストすることができる。アクティブ・タグはパッシブ・タグよりもはるかに広範囲の伝送が可能であり、一般にその距離は 100 フィート以上である。これと比較してパッシブ・タグの範囲は最小限のものであり、数ヤード以内である。通信範囲が数インチ以内となるように設計されている RFID タグもある。

アクティブ・タグもパッシブ・タグも、ボード上のデータを処理する機能がない「ダム」の場合もあれば、暗号化などの可能なデータ・セキュリティ手段をサポートするかなりの記憶容量を持つ「スマート」なものや、圧力や熱などの条件を測定するセンサーを組み込んだものもある。

リーダーと読取範囲

RFID リーダーは、RFID チップに問い合わせて ID 番号や他のデータを受け取る。リーダーはさまざまな無線周波数を使用してチップとやり取りする。低周波数のリーダーとタグは、超高周波数のリーダーとタグよりも安価で消費電力も少なく、非金属物体の貫通性も高い。一方、超高周波数のタグはリーダーから読み取れる範囲がより広く、低周波数の同等のタグよりもデータを高速に転送できる。高周波および低周波のどちらの RFID システムも、見通し範囲アクセスが不可能でも範囲内であれば対象を読み取り可能であることや、バーコード・システムで必要とされる個々の対象のスキャンとは異なり、同時に複数の対象を読み取り可能であるという点で、従来のバーコード・システムよりも優れている。

読取範囲とは、リーダーによりアクセス可能な RFID チップの最大距離のことを指す。読取範囲にはかなりの幅があり、システムによっては 100 フィートの読取範囲を持つものもあれば、1〜2 インチしか読取範囲がないものもある。特定の RFID システムに計画的に組み込まれる読取範囲は、個別のアプリケーション要件に適したものとなるように選択される。たとえば在庫管理や在庫追跡などでは、望ましい読取範囲は広範囲になる。他の状況ではごく狭い読取範囲しか必要でなく、実際にそれがセキュリティ上の理由から望ましい場合もある。

データと RFID システム・ネットワーク

最終的にデータはリーダーから業務処理アプリケーションに、次いで識別された対象に関する情報が保管されるデータベースにネットワーク経由で伝送される。これらのネットワークのセキュリティは、RFID システム全体のセキュリティにとって重要である。RFID システム内のデータの重要度に応じて、データを暗号化して、他のセキュリティ手段を組み込むことができる。**[1]**

RFID テクノロジーのファミリーには、固有の属性を持つ多くのサブグループと、このテクノロジーの構成要素のさまざまな能力に依存する機能が含まれている。これにはタグ内の回路の高度化、関係する電力のレベルとソース、タグとリーダーを結ぶ通信プロトコル、効率的な通信のためのタグとリーダーとの間に必要な距離などが含まれる。タグのさまざまな用途に応じて開発された種々の標準があるため、すべてのリーダーがどのタグでも読み取れるわけではない。

大まかに言えば、RFID テクノロジーは次の 4 つの一般的な目的に使用できる。1) 対象の追跡、2)人物の追跡、3) サービスの提供、または 4) 製品または装置の内部構成要素。[2] テクノロジーの技術的な相違点は、それぞれの応用に反映される。[3]

RFID とプライバシー

RFID テクノロジーは、他者がそれを使用して、位置情報など他の方法では入手できないか入手が許可されない特定の個人に関する個人識別情報を入手できる場合に、プライバシー問題を引き起こす。この情報にはたとえば、その人物の位置、その人物が特定の製品を所有していること、または特定のサービスを使用したことなどがある。セキュリティ問題は、無許可の他者がタグとリーダーとの間の無線通信の傍受、タグの無許可読み取り、またはネットワークやデータベースへの無許可アクセスのいずれかによりそのような情報を入手できる場合に引き起こされる。

これらの新たなテクノロジーを背景として、プライバシーとセキュリティの問題の詳細な分析が明確に求められている。3 つの一般的な原則がこの分析から浮かび上がり、それらは RFID の既存および新たな応用におけるプライバシー問題への取り組みに適用できる。その 3 つの原則とは、テクノロジーの中立性の原則、基本的設計要件としてのプライバシーとセキュリティの原則、および透明性の原則である。

テクノロジーの中立性: RFID テクノロジーはそれ自体、プライバシーへの脅威とならない。RFID は、他のテクノロジーと同様、適切なプライバシー保護を促進する信頼できる情報管理の慣行と矛盾した方法で配備されると、プライバシー漏洩を引き起こすことになる。

基本的設計要件としてのプライバシーとセキュリティ：RFID テクノロジーのユーザーは、初期設計の一環としてプライバシーとセキュリティの問題に取り組まなければならない。プライバシーとセキュリティの問題に対応するように RFID システムを後から改良するより、プライバシーとセキュリティを最初から考慮して設計するほうがはるかに望ましい。

消費者への透明性: 秘密の RFID タグまたはリーダーがあってはならない。RFID テクノロジーの使用は可能な限り透明性のあるものでなければならず、消費者は、RFID システムを利用した取引に関わるときに、RFID テクノロジーの実装と使用について（タグ、リーダー、および PII の保管を含め）通知されなければならない。同時に、通知だけでプライバシーに関するすべての問題が軽減するわけではないことを認識するのも重要である。たとえば、通知だけで、不適切なデータ収集や共有、適切なセキュリティ手段が配備されていないことなどが正当化できるわけではない。通知は、信頼できる情報管理の慣行をよく考えてしっかり実施することで補完されなければならない。

このガイドラインの目的

さまざまな消費者グループと営利企業からの代表が、現在のプライバシー問題に取り組み、RFID テクノロジーの配備に関係した将来的な問題に歯止めをかけるために、民主主義と技術のためのセンター（CDT）の主導の下にこのガイドラインを作成した。この資料は、RFID の現在および近い将来の応用、それらの応用がプライバシーにどのように関与するか（またはしないか）、および企業がそれらに取り組める方法についての詳細分析の結果である。このガイドラインは、現在の RFID システムの多様性と汎用性、応用の幅、およびテクノ

ロジーの発展速度を考慮に入れて、原則のレベルで設計されてきた。この資料は、RFID テクノロジーを背景としたプライバシーに関して、政策立案者、開発者、およびユーザーにガイドを提供することを意図している。

作成に加わった参加者は、論議を絞り込むために、OECD が「プライバシー保護と個人データの国際流通についての勧告」で示したガイドライン（「OECD ガイドライン」）で明確に表現された、公正な情報管理の慣行という枠組みを用いた。この枠組みは、RFID テクノロジーを電子データ・フローに関する特定の問題と関連付けるために有用であることが実証されてきたが、RFID に関係するプライバシー問題の多くは情報収集と保管のどのシステムにも共通であり、場合によっては RFID が独自の新たな課題を発生させることが参加者に明らかになってきた。したがって、この資料は OECD ガイドラインのポイントごとの応用を考慮するものではなく、通知、選択と同意、二次転送、アクセス、およびセキュリティという領域における公正な情報管理の慣行という特定の面に適用する場合に、RFID テクノロジーにより引き起こされる特定の課題に焦点を当てている。

このガイドラインは、幅広い業種に適用するのに十分な柔軟性を持って設計されている。これが成功するかどうかは、どのように実施・保守するのが最適かをうまく決定する企業にかかっている。特定の RFID アプリケーションの性質、企業のビジネスモデル、およびそれら両方が配備される環境に基づいて、一部の企業ではたとえば他の企業とは著しく異なる仕方で通知を出すことも予想される。したがって、小売業者が家庭医療システム提供企業とは異なる方法で通知を出すこともある。さらにこの資料は、RFID を配備する企業が、情報収集と共有に関する既存の法律や規制を順守することを前提としている。

この資料は、商業および民間企業の消費者への RFID の応用を対象としており、行政への応用、または雇用者と従業員間の利用のため企業が内部的に配備した RFID の応用、企業間取引への応用、または個人識別システム用の RFID の使用への対応は意図していない。

このイニシアチブへの参加者は、RFID テクノロジーが継続的に発展を遂げ、それがプライバシーに与える影響についてさらに学ぶにつれて、このガイドを再読することが必要になることを明確に意識している。たとえば、かなりの注目を集める 1 つの問題は、個人の位置を追跡するために RFID を使用できるか、またはどの程度実用的に使用できるかというものである。位置の追跡などの問題は、他の問題もそうであるが、テクノロジーが進化して新たな応用が出現するごとに再考することが妥当であることを示している。RFID テクノロジーとその応用が急速に発展しているので、民間企業がその実施により経験を積むにつれて、ドラフト作成者はガイドラインをレビューして改良する意向である。

結局のところこの活動の目的は、ベスト・プラクティスを定義しようとすることであった。このプロセスには、広範囲で多様な観点を代表する関係者間の健全な持ちつ持たれつの関係を伴う、原則と参加者の両方についての広範囲な討議が関係している。したがって、すべての参加者が必ずしもすべての勧告を支持しているわけではないが、最終成果は、これ

らのガイドラインが消費者のプライバシーを損なうことなく、RFID の潜在的な利点を具現できる、有効な実践内容を提示しているという集団としての判断を表している。

このガイドラインは、立法のための青写真として編集されたものではない。ドラフト作成プロセスの参加者は、このガイドラインを広く自発的に採用し、消費者教育に大きな労力をかければ、RFID の使用のための環境は大幅に向上すると確信している。

ベスト･プラクティス

注： 情報（位置情報を含む）が、RFID システムにより収集されてリンクされたり、商業団体により RFID タグ自体でまたはデータベース利用のいずれかで個人情報にリンクされたりすることが予定されている場合、明確、明瞭、かつ簡潔な通知を消費者に提供しなければならない。（この資料の目的を考慮して、この情報を「リンクされた情報」と呼ぶことにする。）

●このどちらの状況においても、通知では以下が示されることになる。

○リンクされた情報に関係する RFID の存在。

○リンクされた情報が収集される目的。

○リンクされた情報が使用される方法。

○リンクされた情報が単に消費者が購入した装置を作動させたり、消費者が契約したサービスが提供されるようにしたり、または営利企業が消費者との取引を遂行するためだけに使用されるのかどうか。

○リンクされた情報が、さらにその後マーケティングなどに使用される可能性があるかどうか。

○リンクされた情報がそのように使用される場合、消費者の選択に沿った方法でのみ使用されるのかどうか。

○RFID タグは取り外しまたは非活性化できるのかどうか。

●可能な限り、リンクされた情報の収集に RFID システムを使用するという通知を、商品またはサービスを入手するための取引完了前に提供しなければならない。入手する商品またはサービスがない場合には、通知は PII と RFID システムにより収集される情報とを関連付ける前に提供しなければならない。

通知を提供する責任は、消費者と直接的な関係を持つ企業にある。[4]

タグ番号などの RFID タグ上の情報が、特定の個人と直接関連付けられていない場合、RFID タグ上の情報と特定の個人との間にリンクを作成するために、通常は一連のデータベースまたは他の情報リポジトリにアクセスすることが必要である。[5] 収集した情報をリンクさ

れた情報と見なせるほどリンクが深いかを慎重に判断するのは、RFID システムの配備に関与した商業団体の責任である。

●一般に、商業団体は、通知が必要かどうかを判断する際に、PII および／または位置情報と RFID 識別番号との間のリンクの可能性を考慮しなければならない。この判断を下す際に、企業は以下について誠実に考慮しなければならない。

○リンクを有効にするために必要な情報のすべての要素およびデータベースに単一の個人または団体がアクセスする可能性。

○リンクを有効にするために必要な情報の要素数。

○情報に巡らすセキュリティ手段。

○情報のアクセスまたは使用に適用される法的保護または保護手段。

○RFID データにリンクされる情報の機密度。

●PII と RFID 識別番号との間の関連が希薄になるにつれ、プライバシーのリスクは間違いなく低減し、通知の必要性は一層判断にまかされることになる。

RFID テクノロジーを使用している商業環境または公的環境に入る際に、消費者は通知を受けなければならない。可能な限り、個々の RFID リーダーは RFID リーダーであることが識別できなければならない。

企業は毎年内部査定を実施して、送られた通知が正確に RFID システムに関係した情報管理の慣行を反映しているかどうかを確認しなければならない。

RFID テクノロジーを配備している企業には、RFID により可能になる PII 収集に関して消費者に背景と状況を示すための消費者教育の取り組みに参加し、このテクノロジーとその利点についての社会の意識を高めることが強く勧められている。

選択と同意

RFID テクノロジーの使用と、RFID タグで収集されるか RFID 番号と関連付けられるリンクされた情報の使用には選択が伴う。

通知についてのガイドラインに従って、RFID テクノロジーの使用に関して、または RFID タグで収集されるか RFID 番号と関連付けられるリンクされた情報の使用に関する選択を行う機会がある場合、消費者に明確に通知しなければならない。

可能であれば、消費者が商品またはサービスを入手する取引を終える前に、そのような選択を提示しなければならない。それにより、しっかりした通知と相まって、消費者には RFID テクノロジーの使用に関して効率的に選択する手だてが与えられることになる。

●RFID テクノロジーの使用に関する消費者の選択

○消費者は、タグの取り外し、非活性化、または破壊が選択できる場合、および選択できる場合にはどのようにするかについて、明確、明瞭、かつ簡潔な方法で通知されなければならない。

○そのような場合、RFID タグの取り外し、非活性化、または破壊という選択を消費者がすぐに利用でき、すぐに実行できるものでなければならない。

○タグの取り外し、非活性化、または破壊を選択することで、消費者がアイテムを返品したり、保証を受けたり、地域法による保護を受けることができなくなるようなことがあってはならない。この選択を行ったことにより製品が損傷したり不良品になったりしてはならない。

●タグで収集される、または RFID 番号と関連付けられる PII の使用に関する選択と同意

○場合によっては、リンクされた情報は、消費者が購入した装置を作動させたり [6]、消費者が契約したサービスが提供されるようにしたり、または営利企業が消費者との取引を遂行するためだけに使用される。そのような場合、消費者に RFID タグの存在について（通知に関する規定に従って）通知しなければならないが、PII の使用に関する消費者の同意または選択を求める必要はない。

○収集され RFID 番号と関連付けられたリンクされた情報が、消費者が購入した装置を作動させたり、消費者が契約したサービスが提供されるようにしたり、または営利企業が消費者との取引を遂行したりする以外の目的で使用される場合（マーケティングや、他の何らかの目的で第三者とリンクされた情報を共有するなど）、消費者にその旨を通知して、そのような使用に同意する機会を与えなければならない。

選択を提供する責任は、消費者と直接的な関係を持つ企業にある。[7]

二次転送

可能な限り、RFID システムを配備して PII を収集する企業は、PII を共有する企業に対して（その関連会社、子会社、および第三者企業を含め）、情報を収集している企業がその共有データに与えている保護レベルに見合うまたはそれより高度な保護レベルを求める条件を契約に組み込まなければならない。

アクセス

PII がタグそのものの上で維持される場合、個人からその情報に妥当なアクセスができるようにしなければならない。

個人が自身に関するリンクされた情報に基づいて不利な決定を受ける場合 [8]、その個人はその情報に妥当なアクセスができなければならない。一般原則として、コスト効果および効率が良ければ、RFID テクノロジーを使用して収集された位置情報を含む個人識別情報への妥当なアクセス手段が消費者に提供されることが望ましい。

上記の状況では、適切なアクセス手段は個人と接触がある団体が提供しなければならない。

アクセス手段が提供される場合、それは消費者が簡単かつすぐに利用できるものでなければならない。

リンクされた情報への行政機関のアクセスは、適用法の下で令状を送達することによってのみ許可されるものでなければならない。

セキュリティ

企業は、RFID タグ、リーダー、および該当する場合はそれらにより収集されたリンクされた情報を、無許可の読み取り、ロギング、および追跡から保護するために妥当で適切な労力を払わなければならない。保護の対象には情報を伝送または収容するネットワークまたはデータベース、およびリーダーとタグとの間の無線伝送も含まれる。さらに、企業はリンクされた情報が無許可アクセス、紛失、または改ざんなどの問題に遭わないように保護するために妥当で適切な労力を払わなければならない。

その場合、企業は業界標準に沿う、システムに保管される情報の量と重要度に適した情報セキュリティー・プログラムを確立して保持しなければならない。そのようなセキュリティー・プログラムには、リンクされた情報のセキュリティ、機密性、および保全性に対する合理的に予想可能な内外のリスクを識別するプロセスと、それらのリスクに取り組むプロセスを含めなければならない。

タグとリーダーとの間で伝送される情報のセキュリティを強化するために、企業は実行可能な範囲で、RFID タグそのものに保管される情報を最小化しなければならない。

米国図書館協会（American Library Association）

Quantive, Inc.

民主主義と技術のためのセンター(Center for Democracy & Technology)

Cisco Systems Inc.

Eli Lilly and Company

IBM

Intel Corporation

エリオット E.マックスウェル(Elliot E. Maxwell)、RFID コンサルタントならびにジョーンズ・ホプキンス大学コミュニケーション・プログラム・フェロー

Microsoft Corporation

全米消費者連盟(National Consumers League)

The Procter & Gamble Company

Verisign

Visa U.S.A.

注:

[1] たとえば、多くの非接触型決済カードは 128 ビットの Triple-DES 暗号化を採用している。決済取引では、非接触チップは固有の数字コードを生成する。このコードが検出されないと、取引は拒否される。

[2] これを考慮できる例は数多くある。RFID システムは、製造在庫倉庫で品目を追跡するために使用されているが、そこではたとえば（タグが埋め込まれた）入庫パレットがリーダーを通過するだけで納入物が自動的に記録される。次いでこの情報は在庫システムに記録される。病院や刑務所内では RFID システムによって人物が追跡されており、将来的には在宅医療に応用されて介護職員が在宅の高齢者や寝たきりの人の日常動作をモニターするために使用することができる。RFID テクノロジーを早くから応用したよく知られているサービスは、有料道路での料金徴収タグに組み込まれたものであり、これによって RFID 対応カードを持つドライバーは徴収ゲートを通過するだけで料金を支払えるようになった。さらに別のサービス応用例として非接触型決済カードがある。加えて、固有の ID を持つ RFID タグは自動車のキーの内部構成要素となっている。このキーをロックに挿入すると、車の電気系統に組み込まれたリーダーと通信する。

[3] たとえば、電子バーコードに使用されるチップには、パスワードによりセキュリティを管理する機能や他の保護手段があり、数フィート先の距離から読み取ることができる。他方、非接触型スマート・カードに使用される RFID タグは、一般的には堅固な暗号方式（タグの保護と、伝送プロトコルの機密保護に使用できるもの）をサポートし、数インチの距離で読み取られるように設計されている。

[4] 消費者との直接的な関係は持たないが、RFID システムの配備または使用に関わっている商業団体は、消費者への通知を促進するための誠実な努力を払わなければならない。その製品に RFID システムを組み込んでいる商業団体は、その事実を直接購入者に通知し、実行可能な範囲でその直接購入者に対して、さらにその先の購入者に同様の通知を与えるように促さなければならない。これには、消費者と直接関係を持つ企業が、RFID テクノロジーの使用についての適切な通知を与えることができるようにするという目的がある。

こうした備えをすることの論拠としては、RFID の使用に関わっていないまたはその利点を享受していないが、タグが組み込まれた製品を受け取る企業は、受け取る製品に RFID タグが組み込まれていることを知らない場合があるため、通知するために適切な情報を得ることが必要になるからである。EPCglobal の関連メンバーが従っているような、対応する

ガイドラインに合う認知度の高いロゴを使用することは、この通知をサポートする 1 つの方法である。

小売環境で、現在配備されている RFID タグが単にバーコードの置き換えとしてしか機能しておらず、拡張機能や追加機能を提供していない場合には、通知は現在実施されていることに応じた内容で提供することができる。

[5] たとえば、車のタイヤに組み込まれた RFID タグを車の所有者に関する PII に相関させるには、いくつかのリンクが間違いなく必要である。

[6] たとえば、RFID により電子装置の機能を使用可能な状態にすることができる。

[7] 消費者と直接的な関係を持たないが、RFID システムの配備または使用に関わっている商業団体は、消費者の選択を促進するための誠実な努力を払わなければならない。

その製品に RFID システムを組み込んでいる商業団体は、その直接購入者に、購入者が消費者に選択と同意の機会を提供すべきかどうかを判断するのを支援するための RFID がシステムに組み込まれている場合はそのことを通知し、実行可能な範囲でその直接購入者に対して、さらにその先の購入者が選択できるように促さなければならない。これには、消費者と直接関係を持つ企業が、適切な選択を消費者に提供できるようにするという目的がある。EPCglobal の関連メンバーが従っているような、対応するガイドラインに適合した認知度の高いロゴを使用することは、この通知をサポートする 1 つの方法である。

[8] たとえば、商品やサービスの入手可能性やクレジットの利用能力について不利な判断が下される場合などがある。

カナダ･オンタリオ州 IPC の RFID プライバシー･ガイドライン

(RFID 情報システムの IPC プライバシー･ガイドライン)

2006 年 6 月

カナダ・オンタリオ州 IPC の RFID プライバシー・ガイドライン

概要

この資料は、無線を利用した認識（RFID）の情報技術とシステムを設計および運用する組織のためのプライバシーの「ベスト・プラクティス」ガイドとして活用されることを意図している。

カナダ・オンタリオ州情報プライバシー監督官室（IPC）には、有効な解決策を推奨することを目的として、公衆を教育し、新たな情報技術により提起されるプライバシーの問題に対処する任務がある。このため、IPC は業界や他の利害関係者と共同でこのガイドラインを作成してきた(1)。このガイドラインは、適用されるプライバシー法や規制に代わるものとなることは意図されていない。

RFID タグは私たちの日常生活の中でますます広く見られるようになっており、セキュリティー・アクセス・カードからイグニッション・イモビライザー、道路通行料金システム、その他の電子通過システムなどの多くの利便性が提供されている。

サプライチェーンのプロセス内で配備されている RFID タグは、プライバシーにとってはほとんど脅威とならない。それらは個人とリンクされることはなく、製品を追跡するために箱、パレット、ケースに付けられる。それらはサプライチェーン内での製品の自動識別のために、無線を利用した認識を使用する固有 ID として機能する。それらのタグには製品と関係がある標準情報が入っており、個人情報は組み込まれていない。

RFID テクノロジーの消費者、小売業者、および提供業者向けの潜在能力を具現化するために、テクノロジーの進化と実装を扱うための原則を確立しながら、そのテクノロジーの現状により対応が求められるプライバシー問題に取り組むことは不可欠である。これに応じて、組織が消費者に影響を与える可能性がある RFID テクノロジーを配備する場合はいつでも、この資料に記載されているガイドラインを順守し採用することを推奨する。

監査官室提供の付属 DVD で示されているとおり、サプライ・チェーン・マネジメント・プロセス内での RFID タグの使用は問題ではない。問題は、消費者のアイテム・レベルでの使用により生じる。RFID タグは、個人識別可能情報とリンクされると、人の活動の追跡や監視と関係したプライバシー侵害行為の可能性が生まれる。このガイドラインの目標は、そのようなデータ・リンクと関連するプライバシー関連問題を軽減し、RFID システムに関連したオープンネスと透明性を向上させることにある。このガイドラインを使用することは、最終的には既存の顧客との信頼できるビジネス関係を維持し、さらに新規顧客を獲得する助けになるはずである。

(1) EPCglobal Canada は IPC と共同してこれらのガイドラインを作成しており、このガイドラインに対する EPCglobal Canada の支持を表明するために、メンバー企業による理事会承認を求めている。

対象範囲

この RFID プライバシー・ガイドラインは、個人識別可能情報と関係またはそれにリンクする可能性がある消費者商品に対する、RFID テクノロジーの使用に関わる情報システムを運用する組織に適用される。

「組織」という語は、団体、企業、慈善団体、クラブ、政府機関省庁、研究機関、および専門機関などを幅広く指している。たいていの場合、このガイドラインは特に小売業者と関係がある。

「情報システム」は、RFID および RFID 関連情報の収集、伝送、処理、および保管を扱う RFID タグ、リーダー、データベース、およびネットワークの組み合わせを指す。

「個人情報」は、識別可能な個人に関して記録された情報を指す。人物の名前、連絡先、および経歴情報に加えて、これには個人の嗜好、取引履歴、活動や旅行の記録、またはこれらから派生した情報（プロフィールや成績表など）、および個人のファイルに追記できる他者に関する情報（家族、友人、同僚など）も含められる場合がある。アイテム・レベルの RFID タグでは、個人識別情報と RFID タグがリンクされるため、リンク先のデータは個人情報となる。

このガイドラインは、1996 年のカナダ規格協会（CSA）プライバシー・コードの 10 の原則に基づいている。これは企業、業界、および消費者グループを含む幅広い利害関係者により公式化されたものである。CSA プライバシー・コードの原則は、現在ではカナダのプライバシー法および規制の基礎として役立っている。これらはカナダ国内の組織の日常方針および慣行で順守され、プライバシーの「公正な情報慣行」の最も強力かつ最も明確な表現の 1 つとして広く認められている。

このガイドラインとその応用は、次の 3 つの包括的な原則に従って提供される。

1) テクノロジーではなく、RFID 情報システムに焦点を当てる：問題は RFID テクノロジーそのものにあるのではない。プライバシー問題が生じるのはその配備方法にある。この理由から、RFID 情報システムについては大まかに述べることとする。このガイドラインは、特定のテクノロジー・コンポーネントや機能ではなく、総合的な意味での RFID 情報システムに適用し、幅広いコンテキストで理解される必要がある。

2) プライバシーとセキュリティは最初、すなわち設計時から組み込まなければならない：プライバシー問題を幅広い体系的な方法で識別しなければならないのと同様に、技術的な解決策にも体系的に取り組まなければならない。徹底的なプライバシー影響査定が重要であり、RFID テクノロジーおよび情報システムのユーザーは、データを最小化することに特に重きを置きながら、設計段階の初期からプライバシーとセキュリティの問題に取り組まなければならない。これは、可能であれば、識別性、可観測性、および RFID タグと個人

情報および他の関連データとの連結性を最小化するように努力しなければならないことを意味する。

3) 最大限の個人参加と同意：RFID 情報システムの使用はオープンで透明性がなければならず、可能な限り参加して情報を得た上で決定が下せる機会が個人に提供されるものでなければならない。

この資料では、RFID テクノロジーと情報システムの多様な使用と応用を認める、自発的で多数の意見に基づくガイドを提供している。この異種混交性により、解釈と応用におけるある程度の柔軟性が必要になる。

組織には、その独自の環境とニーズに応じて、固有の方針、手順、および応用にこのガイドラインを採用して適応させることを推奨する。

RFID プライバシー・ガイドライン

1. 責任

組織には個人情報を制御する責任があり、以下に説明する原則を組織が順守していることと、全従業員の必要な訓練について責任を負う人物を指定しなければならない。情報を第三者に開示する場合には、組織は見合ったレベルの保護を提供するために契約その他の手段を用いなければならない。

一般的に個人と最も直接的な接触と 1 次的関係を持つ組織は、RFID タグが付けられたアイテムが製品のライフサイクル内で生成されるところなのか終わるところなのかに関係なく、プライバシーとセキュリティを確保するために、最も重い責任を担わなければならない。

2. 目的の識別

組織は個人情報の収集、リンク、および個人情報へのリンク許可の個別目的について明確に識別して、時宜を得た有効な方法で個人に通知しなければならない。これらの目的は具体的かつ限定的であるべきで、個人情報を収集する組織および人物はその目的を個人に説明できなければならない。

3. 同意

組織は RFID タグにリンクされる個人情報の収集、使用、または開示の前に個別の同意を求めなければならない。同意が有効であるには、組織が使用する RFID テクノロジーと情報の存在、タイプ、場所、目的、および働きについて情報が与えられた上での理解に基づいたものでなければならない。個人のプライバシーに関する選択は、時宜を得た簡単かつ

効率的な方法で実施される必要があり、いかなる強制もあってはならない。消費者は、罰則なしにアイテム・レベルの RFID タグの取り外し、無効化、または非活性化ができなければならない。

販売時に RFID タグを自動的に非活性化し、再活性化できる機能を備えることを最終的な目標としなければならない。消費者が後でそれを再活性化して再度目的を付与できるようにするか、またはタグを機能させて RFID リーダーとやり取りするような制御を実施できるようにしなければならない。

4. 収集の制限

組織は差別的またはひそかに、あるいは欺いたり惑わせたりする目的で、個人識別情報を収集したり RFID タグとリンクさせてはならない。収集する情報は規定の目的を達成する必要最小限のものに制限しなければならず、タグにリンクされる個人データの識別性を最小にすること、許可されていないリーダーまたは人物による RFID タグの可観測性を最小にすること、および収集したデータと個人識別情報との連結性を最小にすることに重きを置く。

5. 使用、開示、および保存の制限

組織が新たな目的のために個人情報を使用、開示、またはリンクする場合には、さらに個人の同意を得なければならない。個人情報は規定の目的を実現するためにのみ保持し、安全に破棄しなければならない。小売業者は先に概要を示したデータ最小化の原則を、その RFID 情報システム全体に組み込まなければならない。

6. 正確性

組織は、個人情報および関連 RFID リンク情報を、規定の目的に必要な正確性と完全性を備えた最新のものとして保持しなければならない。とりわけ個人に影響を与える決定を下すために使用する場合にそのようにしなければならない。

7. 保護手段

組織は RFID タグにリンクされた個人情報を、その重要度に適した方法で紛失や盗難、および無許可の傍受、アクセス、開示、コピー、使用、変更、またはリンクを張ることから保護しなければならない。さらに、適切な研修により、従業員に個人情報の機密性を維持することの重要性を認識させなければならない。物理的、組織的、および技術的な手段がすべて必要であるが、技術的な保護手段を特に重視しなければならない。

8. オープンネス

組織は、RFID テクノロジーと情報システムの運用、および個人情報の管理に関するその方針と実践についての具体的情報を、個人が簡単に入手できるようにしなければならない。この情報は、個人が理解できる形式で入手できるようにしなければならない。

9. 個人のアクセス

組織は、要請に応じて、当人の個人情報の存在、使用、リンク、および開示に関する情報を知らせ、その情報への妥当なアクセス方法を提供し、その正確性と完全性に異議を申し立て、必要であれば修正を受け付けられるようにしなければならない。

10. 順守に対する異議申し立て

組織は上記の原則のいずれかの順守に関する苦情を個人が申し立てできるようにする所定の手続きを持ち、組織の順守について責任を負う人物を指名しなければならない。

以上

普及促進・社会受容性検討推進に関する成果報告書

平成 19 年　3 月　発行

発　行　　次世代電子商取引推進協議会

販　売　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園三丁目 5 番 8 号
機械振興会館 3 階
TEL：０３（３４３６）７５００