

Auto-IDにおけるネットワークサービスの課題と可能性

NTT 第三部門 大和 淳司

Auto-IDセンタが標準化を進めているRF-IDタグのシステムでは、タグ自体には、ePCコードと呼ばれるユニークなIDのみが記録され、タグが貼られた物品についての情報はすべてネットワーク側で管理する。ここでは、Auto-IDセンタの構想における、ネットワーク側の機能について概説し、課題と可能性についてまとめ、最後にNTTの目指す活動について紹介する。

ネットワーク機能の概要

MIT Auto-IDセンタが進めている標準化では、電源の要らないパッシブなRF-IDタグを使用し、タグを貼り付けた物品に関する情報はすべてネットワーク側で管理する。これには2つのメリットがある。まず、タグが単純化されるため、コストが低減されることである。これによってタグの単価を5セントを目標に下げて、あらゆる物にRF-IDタグを貼るという構想を実現する。次に、情報がネットワーク上にあるため、柔軟な情報管理が可能となる点である。たとえば、タグの記録容量の制限とは無関係に、情報量の多い商品属性を記述することもできますし、移動・購入の履歴を随時書き換えることもできる。さらに、管理の仕組みを作れば、特定の場所・状況・アクセス元に応じた情報提供も可能になる。

このような機能を実現するには、一方で、膨大な情報の管理が必要になる。ePCコードには、現在のバーコードと異なり、商品のシリアル番号も含まれ

るため、初期データの入力はもちろん、移動や購入履歴を管理するとなると、莫大なトランザクションが発生する。これを管理・運用するため、Auto-IDセンタでは、2段階の仕組みをとっている(図1)。

ONSサーバ

ONSとは、Object Name Serviceの略で、ePCコードから、商品情報を提供するサーバのアドレス解決をするサービスである。タグリーダーが読み取ったRF-IDタグのePCは、次の構造を持っている(図1左)。まず、バージョンを示す8bitのヘッダ、次に製造者を示す28bitのePC Manager、物品種別を示す24bitのObject Class、最後に個体を示す36bitのシリアル番号である(ePC-96 Type-1の場合)。これをONSサーバに送ると、商品情報のありかを示すIPアドレスが返ってくるわけである。

これは内部の仕組みとして、次の2段階に分かれている。まず、プレゾルバが、ePCからePCドメイン名への変換を行なう。これは、ePCコードを下位ドメイン名として含んで、`***.epc.objid.net`で終わる形をしている。次にこのドメイン名をPMLサーバのIPアドレスに変換する。この段階は通常のDNSと同じである。こうして、ePCコードから、商品情報のありかをまず取得する。

PMLサーバ

PML(Physical Markup Language)は、RF-IDタグが貼られたオブジェクト

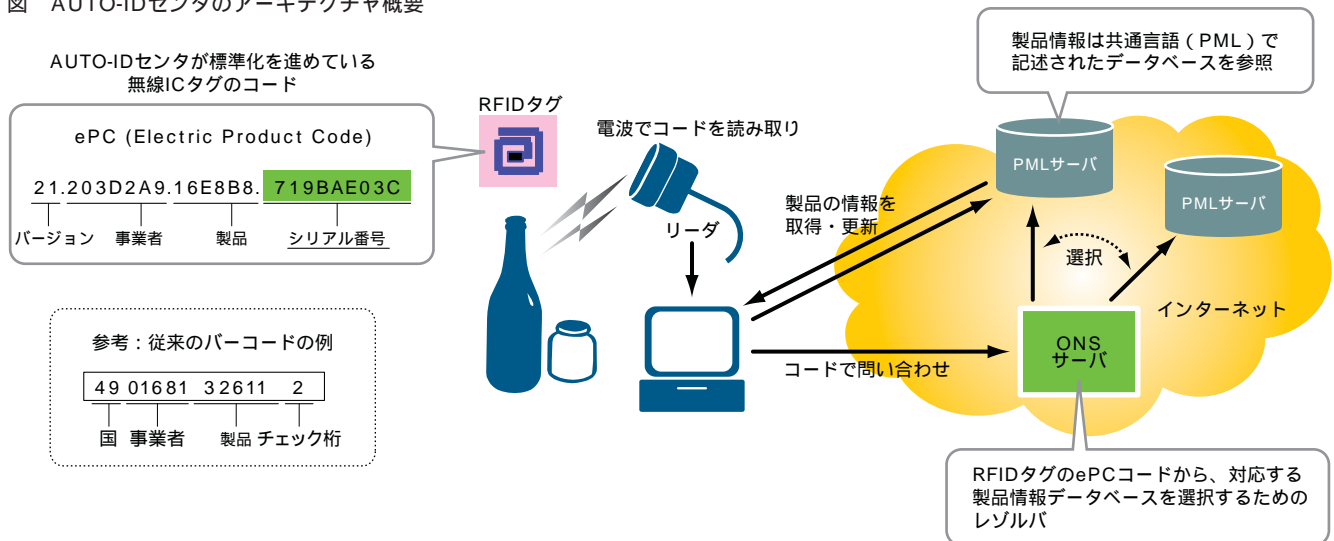
の物理的な属性、過程、環境を表現するためのXMLをベースとした共通言語である。基本的にはサプライチェーンマネジメント(SCM)への応用を念頭において各種エレメントが定義されている。PMLのエレメントとしては、商品の構成、移動履歴、所有者、場所、長さ、質量、温度などの記述が定義されている。SCMで利用するため、たとえば移動履歴は、移動の各段階ごとに日時、場所、所有者、温度などを記述することができる。

このように情報管理を2段階に分けるのは、商品の情報は製造業者がそれぞれ入力・管理するなど、分散して存在すると考えられるのに対して、ONSサーバはDNSと同様、全体として統一された管理が必要なためである。

ネットワークサービスの課題

ここまでご紹介したように、現在のAuto-IDセンタの構想は、インターネットの仕組みを利用したものになっており、RF-IDタグリーダーは、ネットワーク接続されたコンピュータに繋がっている、あるいは直接インターネットに繋がっていることが前提である。このため、実際に膨大な数の物流を管理しようとした際、あるいは購入後の商品のタグを読んでユーザがアプリケーションを利用しようとする際には、さまざまな課題が残されている。ここでは、スケーラビリティとセキュリティ、プライバシーの問題について述べる。

図 AUTO-IDセンタのアーキテクチャ概要



スケーラビリティ

現在バーコードによるPOSを利用しているスーパーマーケット、コンビニエンスストアなどで販売されている商品の個数は、年間900億個と言われている。このほとんどすべてがAuto-IDセンタ仕様のRF-IDタグを利用した場合、物流の各段階、小売店での在庫調査、販売時点、販売後の消費者自宅内での所在管理や廃棄時の分別など、1つの物品について数十回の照会・書き換えなどのアクセスが発生する。これに耐えるためには相当の処理能力を持ったONSサーバ、PMLサーバが必要となる。小規模な実験での動作検証のみならず、大規模な運用に耐えるかどうか、今後の開発と検証が必要な分野である。

セキュリティ確保・プライバシー保護

現在Auto-IDの標準仕様を裸のまま使用すると、ePCコードを読み取れば、

どの会社の何という製品なのかが、分かってしまう。これはある場面では潜在的な危険性をはらんでいる。たとえば、家に侵入した泥棒がタグリーダで辺りをスキャンすれば、何が高価な物か分かってしまうし、買い物帰りにリーダを向ければ何を買ったのかが分かってしまう。このような不安を取り除くことが、広く普及するには必須と言える。そのため、いくつかの対策が考えられる。

1. タグを商品販売時点で動作停止させる

タグの仕様にはkillスイッチが含まれている。外部から特定の信号を与えることで、タグの動作をそれ以降停止させることができる。しかし、これは2重の意味で両刃の剣と言える。なぜなら、たとえばスーパーで、kill信号をばらまく一種のテロ行為が可能になってしまうからである。もちろんパスワードは

つけられているし、killは密着して行なわなければならないなどの制限もあるが、killの仕方が面倒になると、かえって利便性を損なうことにもなる。また、販売時点でkillすることが当然の使い方となると、消費者が購入したあと自宅での物品管理などさまざまなアプリケーションが広がることは困難になる。そのため、タグをkillせずに済む方が求められる。

2. アクセス制御

タグを元に物品の情報を取得する際に、アクセス制御をするという考え方である。特定のリーダからのアクセスでなければ、一切の情報を出さない、あるいは限定された情報のみを出す、などの制御を行えば、購入者が自分で物品を管理するためには利用できる。これを実現するには、ネットワーク側に、認証機能が必要になる。

しかし、この場合でも、正当なユーザがタグをアクセスした際に、悪意をもった第三者がこれを横から傍受するのを防止するために、暗号通信などが必要になってくる。

3. 暗号化

タグのePCコードそのものを暗号化する、という考え方である。この場合、タグのコードのうち、ベンダーのコードの部分で暗号化したものであることが分かるようにする。たとえばメーカーXが、通常のコードのほかに、「X-Secured」という名前で別コードをつける。そしてプロダクトコード、シリアル番号は暗号化し、この暗号化に対応したレゾルバに問い合わせをすることでのみ情報が得られる、という仕組みである。このためには、暗号化の標準（暗号方式そのものではなく、標準ePCコードへの組み込み方法）や暗号化に対応したレゾルバの運用などが必要になる。

プライバシーの課題

一般的なネットワークセキュリティ問題で論じられる課題に加えて、Auto-IDの仕組みが広く利用されると、プライバシーに関わる問題が新たに生じてくる。あるリーダがあるタグを読んだ、この一事象がそれだけならさして問題にならないとしても、膨大な事象から特定のタグのIDを抽出することができれば、ある人の移動や活動内容をモニタすることが可能になってしま

う。広い範囲にわたる膨大な人の膨大な活動の名寄せができてしまうとすると、重大なプライバシー問題を引き起こしかねない。ネットワークの利用を前提とした仕組みでは、このような状況への対策も含めて、適切な暗号化やアクセス制御の仕組みが必要になる。

さまざまなサービスの可能性

これらの課題が解決され、Auto-IDセンタのRF-IDが広く普及した際には、元々適用分野として狙っているSCM（サプライチェーンマネジメント）以外のさまざまなアプリケーションが出現することが予想される。たとえば、薬のビンにRF-IDがついて、同時に飲むと副作用などの問題が生じる場合について警告を出したり、製品のRF-IDを読んでマニュアルを入手するなどの例がよく挙げられる（図2）。また、将来拡張として、センサを一体化したRF-IDタグも考えられている。たとえば、温度センサを持ったRF-IDタグは、冷蔵して運ぶ必要がある生ものの管理に最適だろう。商品情報として、産地や生産日を持ち、温度の管理と合わせれば、食品が自分で食べごろを教えてくれたり、賞味期限が切れる前に警告を出したりするなどのアプリケーションも可能になる。

これらのアプリケーションは、いずれもあるタグのIDを読んでその商品情報を得るという、いわば順引きの利用方法である。しかし、多数のタグリーダがさまざまなところに配置され、物

の移動履歴を残せば、逆引き的なアプリケーションも可能になる。これは図3に示すように、たとえば「あの本はどこに行ったかな?」、「手近に何か切れるものはないかな?」などという問い合わせに対して、「その本は寝室にあるはずです」とか、「カッターナイフでよければリビングの引き出しにありますよ」などという回答が得られるというものである。ただし、逆引きのアプリケーションを安全に実現するには、タグの情報のセキュリティのみならず、タグリーダの過去の履歴情報に対するセキュリティも考慮する必要があるなど、より高度な技術が必要になるだろう。

NTT（持株会社）は2002年8月にMIT Auto-IDセンタにスポンサーとして参画した。これは日本の企業としては4番目の参加だが、これまでの日本企業各社が、タグそのものの供給が中心の企業であったのに対して、Auto-ID構想の特徴であるネットワーク側の機能に重点をおいた参加者と言える。今後、NTTでは、Auto-IDセンタの構想を実現する上で重要なネットワーク側の仕組みを中心に研究開発と実証実験に取り組んでいく予定である。特に、上で述べたセキュリティ関連の仕組みを、Auto-IDの仕様に整合させつつ実現していくことが重要であると考えている。また、さまざまなアプリケーションが容易に構築できるよう、各種プラットフォームの整備・提供に向けて、技術開発と実証実験を進めていく予定である。