OUKA
The University of Osaka
Institutional Knowledge Archive

Title	商品トレーサビリティ管理システムにおける運用性ならびにセキュリティに関する研究
Author(s)	小林, 雄一
Citation	大阪大学, 2008, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/49281
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

氏名	小林雄一（こばやしゆういち）
博士の専攻分野の名称	博　士（情報科学）
学位記番号	第　２２１５６　号
学位授与年月日	平成 20 年３月 25 日
学位授与の要件	学位規則第４条第１項該当 情報科学研究科マルチメディア工学専攻
学位論文名	**商品トレーサビリティ管理システムにおける運用性ならびにセキュリティに関する研究**
論文審査委員	（主査） 教　授　薦田　憲久 （副査） 教　授　西尾章治郎　　教　授　藤原　　融　　教　授　岸野　文郎 教　授　下條　真司　　准教授　秋吉　政徳

論 文 内 容 の 要 旨

近年、食品の安全の問題、リサイクル法の成立、薬事法の改正など、商品の安全性に対する消費者の要求が次第に高まってきている。一方で、企業間競争が激化するなか、企業内業務の効率化をはじめ、企業や業種間の連携に基づく業務効率化が求められている。これらの要求に対して、サプライチェーン全体に亘り、商品の生産・流通経路の透明性を確保し、消費者に迅速に情報提供すると共に、問題発生時の対象商品を迅速かつ正確に把握することを可能とするトレーサビリティの早期実現が期待されている。その実現のため、小型で無線通信が可能な IC タグと呼ばれるデバイスの利用が注目を集めている。しかし、商品をサプライチェーン全体に亘り管理するためには、大手企業だけではなく中小企業の参加も必要となり、商品トレーサビリティ管理システムの実現には敷居の低い運用性が求められる。また、商品を流通させるにあたり、商品に関連付いた情報を正確かつ確実に伝達するためのセキュリティが求められる。

本研究は、サプライチェーン全体に亘り、バックエンドにおける商品に関連する情報の共有と、フロントエンドにおける商品に装着した IC タグの共有について、運用性ならびにセキュリティ向上の観点で実施する。バックエンドでの情報共有においては、⑴食肉業界を例に、複数の企業間で取引情報を共有するために必要な複数のコード変換方式を比較評価する。フロントエンドでの IC タグ共有においては、⑵出版業界を例に、IC タグに書き込むデータの改ざんを抑止する方式についてセキュリティ性能を評価する。また、⑶消費者以降の二次流通での IC タグ運用と、消費者プライバシーの保護を同時に満たす方式を提案し、ショッピングモールを例にシミュレーションを実施し評価する。

本論文では、全体を５章に分けて構成する。

第１章の序論では、サプライチェーン全体に亘る商品トレーサビリティ管理システムの重要性および、それを構築するための課題を述べ、関連する従来研究を概観すると共に、本論文の目的と位置付けを明らかにする。

第２章では、サプライチェーン全体に亘る各企業が独自のコード体系を築いているため、業界標準のコード体系への移行が困難な業界において、企業間での取引情報の共有を早急に実現可能なコード変換方式を提示する。産地偽装問題などから食の安全性確保への要求が急速に高まる食肉業界を例に、企業間における取引情報を共有可能とするシ

ステムを設計する。特に、食肉業界では各々の企業が独自のコード体系で運用いるため、このコード体系相違問題の解決が必要となる。このコード体系相違問題に対して、いくつか考えられる解決策の中から、食肉業界の現状に照らし合わし、最もシステム導入の負担が小さい解決策を提示する。また、解決策を施した取引情報共有システムを、実際に食肉業界に導入し、その効果を確認する。

第３章では、IC タグのメモリ領域をユーザごとに割り当て、それぞれ独自に IC タグに設定するタグパスワードにより割り当てられたメモリ領域を保護することが可能なセキュア電子タグを用いて、IC タグデータの改ざんを防止する方式を提案する。例えば、一種類のタグパスワードを多くの企業間で共有する場合、タグパスワードが漏洩するリスクが高く、さらに漏洩したときに被害がおよぶ範囲が広い。この問題を解決するために、出版業界においてセキュア電子タグを利用した書店での業務に焦点を絞り、タグパスワードを分割して管理するいくつかの方式を提示する。また、セキュリティ向上を評価するために、各タグパスワード管理方式に対して FTA（Fault Tree Analysis）を実施しセキュリティに関して比較評価する。

第４章では、IC タグに格納する識別子をグループ単位で管理することで識別子による IC タグの特定を困難にし、IC タグ所持者のロケーションプライバシーを保護する IC タグパスワード群管理方式を提案する。そして、提案方式を運用する上で重要となる PASS KEY が同じ値となる個数（以下、同値個数と略す）が、プライバシー侵害のリスクとパスワード漏洩のリスクに関係することを示す。また、ショッピングモールでの IC タグ利用を例に、消費者の動線を把握するシミュレーションを実施し、このシミュレーション結果から、同値個数の具体的な設定基準を提示する。

第５章では、本研究で得られた成果を要約した後、今後の課題について述べる。

論文審査の結果の要旨

近年、商品流通分野において、安全性に対する消費者の要求や、企業間の連携に基づく業務効率化に対する企業の要求が高まっており、サプライチェーン全体に亘り商品の追跡を可能とするトレーサビリティの実現が期待されている。その実現のためには、柔軟な運用性やセキュリティの確保が求められる。本論文は、これらの課題とニーズを踏まえ、企業間の情報共有、IC タグデータのセキュリティ確保、IC タグによるプライバシー保護について商品トレーサビリティ管理システムにおける運用性ならびにセキュリティに関する研究成果を纏めたものである。その主要な成果を要約すると次の通りである。

⑴企業間の情報共有において、サプライチェーン全体に亘る情報共有を実現する上で、標準コード体系の普及がまだ途上のため取引情報共有の早急な実現が困難な食肉業界に対して、企業間コード相違問題を重く捉え、各企業がコード体系を取引相手のコード体系に変換するコード直接変換方式の採用が有効であることを確認し、取引情報共有システムを速やかに導入する方法を提示している。

⑵IC タグデータのセキュリティ確保において、運用上 IC タグデータの書き換えが必要であると共に、第三者による改ざんの防止が必要な出版業界を例に挙げ、セキュア電子タグを利用した書店での業務に焦点を絞り、タグパスワードを分割して管理するいくつかの方式を提示している。また、各方式に対してフォールトツリー解析を行い比較評価し、各方式の有用性を確認している。

⑶IC タグによるプライバシー保護において、IC タグに格納する識別子をグループ単位で管理することで識別子による IC タグの特定を困難にし、IC タグ所持者のロケーションプライバシーを保護する IC タグパスワード群管理方式を提案している。また、ショッピングモールでの IC タグ利用を例に、消費者の動線を把握するシミュレーションを実施し、この結果から、提案方式に使用するパラメータの設定基準を具体的に提示している。

以上のように、本論文は商品トレーサビリティ管理システムにおける運用性ならびにセキュリティにおいて成果を挙げた先駆的研究として、情報科学に寄与するところが大きい。よって本論文は博士（情報科学）の学位論文として価値あるものと認める。