

水産トレーサビリティシステムの信頼性確保 —2次元コードへのすかしコード導入—

女川 穂高†

三上 貞芳†

長野 章†

高木 剛†

鳴海 日出人‡

桑原 伸司§

若林 隆司¶

1. はじめに

近年、BSE 問題に始まる、食に関する事件・事故により、消費者の「食」に対する信頼性低下の問題が顕著になっている。このような状況から、食に対する安全管理体制の強化が望まれており、生産情報の提供、流通過程の記録、開示、万一事故が起こった際の、迅速な回収のための、トレーサビリティシステムの開発が、様々な機関で行われている。

しかし、現状においては、稼動しているトレーサビリティシステムのほとんどは、生産者や販売者側の情報の提供に留まり、流通過程の情報の点において、消費者の信頼を得るには不十分である。

これらの原因として考えられるのは、トレーサビリティシステムの導入には、様々なコストが掛かることである。必要機器の導入、作業工程見直し等のコストを、生産者から販売者まで流通に関わる全ての者に対して課せることも、システムの導入を困難にしている一因である。特に水産物の流通においては、システムのコスト・信頼性・安定性・耐久性・一貫性等、要求が非常に厳しいため、IT技術の導入、トレーサビリティシステムの適用はほぼなされていない状況である。

本研究では、これら水産物におけるトレーサビリティシステムを、導入コストを低減し、信頼性・安全性・業務効率の向上を目的として研究開発してきた。そこで明らかになったことは、偽装防止策の重要性である。本論文では、情報の信頼性を確保し、よりセキュアなトレーサビリティシステムを構築するための、いくつかのメソッドを提案する。

2. シジミトレーサビリティシステムの実用化

本研究では、重量に基づいた偽装防止策を実装したシステムを、開発、実用化した。

2.1 重量管理による偽装防止策

このトレーサビリティシステムでは、重量管理による偽装防止策を実装した。対象は、青森十三湖産大和シジミである（2005年7月）。詳細は以下の通りである。

まず、生産物を識別するためのIDが含まれたQRコードを、予め用意しておく。このQRコードは、一定の重量単位に相当するチケットと考える。つまり、1枚のQRコードが200gに相当すると設定した場合、10kgの生産物を出荷する際に50枚のQRコードを添付することになる。生

産者は、生産物を出荷する際、これらのQRコードを読み取り、どの中卸業者に出荷したかをサーバに記録する。出荷された生産物には、その重量に相当するだけのQRコードが添付されており、流通業者は分割の際、その重量に見合うQRコードを添付すればよい。販売段階では、添付されていたQRコードを商品に貼付し、消費者はこのQRコードを携帯電話で読み取り、生産物情報を閲覧することができる。

この方式では、「チケット（QRコード）が貼付されていない商品＝偽装されたもの」とすることで、偽装を検知する。

このシステムは、2005年10月から実用化され、約1年4ヶ月の運用実績がある（2007年1月9日現在）

2.2 シジミトレーサビリティシステムの稼動状況

現在までの、シジミトレーサビリティシステムの稼動状況を以下にまとめる。

(1) 総生産量

現在データベースに登録されている総生産量は、684540kgである。これは、1業務日平均1380kgになる。生産量のグラフを以下に示す（図1）。

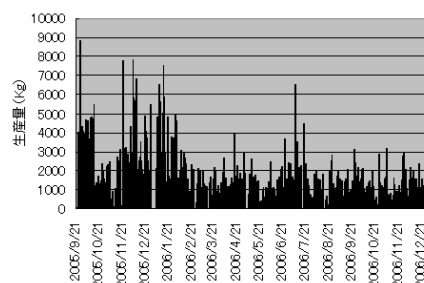


図1. 生産量の遷移

(2) 業務フローへの影響

導入前の業務フローは、仲買人が生産物を順次指定する方式であった。本システムでは、この仲買人が指定した生産物のQRコードを順次読み取る方式とした。この生産物QRコードの読み取りは、多い日では920回に上る。1業務日平均では約143回である。しかし、必要とする業務時間は、導入前と変化はない。本システムは、生産物のQRコードを読み取る者が1人必要とすることを除き、以前の業務に影響を及ぼすことなく導入が可能と言える。

2.3 シジミトレーサビリティのアクセス状況

消費者からのアクセスは、1日平均1.7件程度ある（2006.11.12～2007.1.10）。今後は、協力仲卸業者、小売業者を増やし、より多くの消費者からのアクセスを目標とする。

† 公立はこだて未来大学大学院

‡ 日本データサービス（株）

§（株）北日本港湾コンサルタント

¶ アルファ水工コンサルタンツ（株）

3 QRコードのコピー・改竄防止策の提案

以上のシステムでは、重量に基づいた製品の偽装防止を主眼としていた。しかし、QRコードはコピーが容易で、大量に複製されて使いまわされる恐れがある。以下において、QRコードのコピーを防ぎ、情報の信頼性を確保する方法を提案する。

まず、考える脅威として以下が考えられる。

(1) シリアルナンバーの類推

現在、IDに連番を用いているため、類推される恐れがある

(2) デジタルコピー

QRコードを生成するツールは数多くあり、同一内容のQRコードを大量に生成される恐れがある

(3) フォトコピー

複写機を用いて大量に複製される恐れがある

(4) フィッシング

(3)については、複写が困難な素材を用いる等、(4)については認証局を用いる等が考えられる。本研究では、(1)、(2)を対象とした偽装防止策を提案する。

3.1 IDの類推を防ぐ方法

シリアルナンバーの類推を防ぐ方法を以下に示す。まず、現在用いているQRコードの内容が以下の通りである。

<http://www.traceability.jp/SJMTS/Trace?sid=SJM-1234-S-10-0123456789-500>

この、「1234」が生産者IDであり、「0123456789」がシリアルナンバーである。つまり、「1234という生産者が、0123456789番目に作った製品」ということを示している。この数値を書き換えることにより、他の製品の情報を取得できてしまう恐れがある。これを防ぐには、数値を改竄したことを検知すればよい。

最初に、生産者は秘密鍵を用意する。そしてその鍵で、「SJM-1234-S-10-0123456789-500」を鍵で暗号化し、URLの末尾に追加する。出来上がった内容は

<http://www.traceability.jp/SJMTS/Trace?sid=SJM-1234-S-10-0123456789-500-343000fd009df2f2418f27c0c691d13c53ceadcc>

となる。サーバでは、343000fd009d2418f0～を公開鍵で複合化し、SJM-1234-S-～と比較する。もし、SJM-1234-S-～を改竄した場合、複合化したメッセージと一致せず、343000fd009d2418f0～を改竄した場合は複合化が不可能なため、改竄を検知できる。

3.2 QRコードのデジタルコピーを防ぐ方法

QRコードのデジタルコピーを防ぐ方法を以下に示す。これらの方法は、QRコードを生成する者しか知り得ない情報を埋め込むことによって、デジタルコピーを防ぐ。

(1) 意図的に誤りを含ませる方法

QRコードには、最大で30%までの誤り訂正機能がある。この特徴に着目したのが以下の方法である。

最初に、QRコードを生成者が鍵を用意する。その鍵と、QRコードに含ませるデータから、QRコード上の座標を複数個算出する。その座標のビットを反転したQRコードを生成し、通常通り利用する。そして、検査官が店頭へ赴き、

専用端末でそのQRコードを読み取り、同様の手順でQRコードを生成する。この生成したQRコードと、商品に貼付されているQRコードを比較することにより、偽装を検知することができる。

(2) QRコードにQRコードを埋め込む方法

QRコードのビットを分割し、その一部を用いて新たな情報を付加する方法を以下に示す。

まず、1つのビットを何分割するか、分割したビットのどの部分を使用するかを定める。例として、ビットを4分割、使用する部分は左上を用いるものとする(図2)。



図2. 1ビットの左上を用いる例

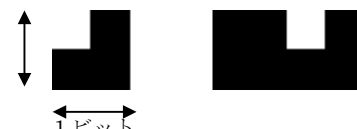


図3. 1011に0010を埋め込む例

例えば図3の場合、通常のデータとしては「1011」であるが、4分割されたの左上部分を見ると「0010」である。この方法で、QRコードにQRコードを埋め込むことができる。「これはテストデータです@FUN」に「秘密」を埋め込んだ例を図4に示す。



図4. 実際に情報を埋め込んだQRコード

この埋め込みQRコードは、通常のQRコード読み取り機(携帯電話等)では「これはテストデータです@FUN」と認識される。これは、ビット単位で白黒の値が3/4になるだけで、読み取りに支障がないためと考えられる。埋め込むQRコードは専用端末のみで読み取りが可能である。通常のURLに、鍵を用いて暗号化したデータを埋め込むことで、(1)と同様に偽装を検知できる。

4. 今後の予定

以上の提案した案を、2.1の青森十三湖産大和シジミのシステムに実装する予定である。また、以上の案は特許出願中である。

なお、この研究は平成18年度文部科学省都市エリア産学連携促進事業(発展型函館エリア)の援助を受けて進められた。

5. 参考文献

- [1] 日経 NETWORK 編集「暗号と認証」,日経 BP 社, 2004.
- [2] 女川 穂高, 三上貞芳, 長野章, 高木剛, 鳴海日出人, 桑原伸司, 若林隆司. 「水産トレーサビリティシステムにおける偽装防止技術の実用化—2次元コードへのすかしコード導入による信頼性の確保—」, FIT2006 講演論文集. 2006.