M_006

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—

Development of Traceability System for Fishery Products Using Falsification Prevention Method

女川 穂高† Hodaka Onagawa　三上 貞芳† Mikami Sadayoshi　長野 章† Akira Nagano　高木 剛† Tsuyoshi Takagi

鳴海 日出人‡ Hideto Narumi　桑原 伸司§ Shinji Kuwabara　若林 隆司¶ Takashi Wakabayashi

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，万が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．重量に基づく偽装防止策

本研究で行った主な 2 つの実験では，重量に基づいた偽装防止策を実装した．

† 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）

2.1 電子署名を用いた偽装防止策

まず，水産物の流通経路を全て記録し，偽装防止に重量情報を用いたトレーサビリティシステムを構築し，実証実験を行った（2004 年 11 月）．対象は，日本鯨類研究所による南氷洋鯨類捕獲調査によるミンク鯨の赤肉で，中卸，加工業者，小売を流通し，消費者へ渡る．具体的な手順は以下の通りである．

まず，生産者は製品の情報（採取日時，採取地区，種類，部位，重量）をサーバに登録する．次に，サーバに記録された情報から，製品識別コードと偽装防止用電子署名を含んだ QR コードを発行し，製品に貼付する．この電子署名は，重量を，生産者の秘密鍵暗号化したものである．流通に関わる全ての業者は，この QR コードを入出荷時に読み取り，サーバに入出荷情報を記録する．消費者では，携帯電話で QR コードに含まれる URL にアクセスする．サーバでは，電子署名を公開鍵で複合化し，製品情報と共に消費者へ開示する．このとき，公開された重量と実際の製品の重量を比較することで，偽装を検知する．

2.2 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．出荷された製品には，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，製品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．

3 QRコードのコピー・改竄防止策の提案

以上の実験では，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)ディジタルコピー
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コードのディジタルコピーを防ぐ方法

QR コードのディ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，ディ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，検査官が店頭に赴き，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 1）．

図 1

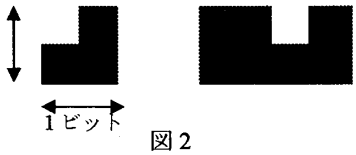

図 2

例えば図 2 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@FIT2006」に「秘密」を埋め込んだ例を図 3 に示す．


図 3

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@FIT2006」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，2.2 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.