1F-4

流通経路に基づくトレース情報のアクセス制御方式

水野 高宏† 國廣 健太郎† 高橋 成文†
株式会社 ＮＴＴデータ†

1. はじめに

近年、複数のプレイヤ間を流通するモノの情報管理を行うトレーサビリティサービスの実現に向けた取り組みが行われている[1]。製品のトレース情報を各プレイヤが分散管理するトレーサビリティシステムでは、システム同士の連携によってトレース情報を収集・統合する仕組みが必要である。このとき、トレース情報に流通経路上のプレイヤのみに公開したい情報が含まれている場合には、流通経路に基づき情報参照を制限する機能が必要となる。しかし、流通経路が既知であることを前提とするアクセス制御方式では、流通経路が事前に決定していない製品のトレース情報を制御することはできない。そこで本稿では、実際に製品が流通したプレイヤを識別することで、流通経路が未定の環境にも適用可能なアクセス制御方式を提案する。

2. 異種 PF 連携モデルのアクセス制御問題

本稿では、連携センタを介して各プレイヤの異なる仕様のプラットフォーム(PF)の間でトレース情報の流通を行う異種 PF 連携モデルを想定環境とする[2][3]。本モデルの構成を図 1 に示す。連携センタには、各製品の流通経路情報を一元管理する流通経路 DB が設置される。連携センタには以下の 3 つの機能がある。

- **経路登録**: 各プレイヤが、製品を手にしたタイミングで、自 PF の ID(PFID)を流通経路 DB に登録する。
- **情報収集**： 経路情報に基づいて、各 PF の情報格納 DB にアクセスし、製品のトレース情報を収集する。
- **情報統合**： 収集されたトレース情報を統合する。

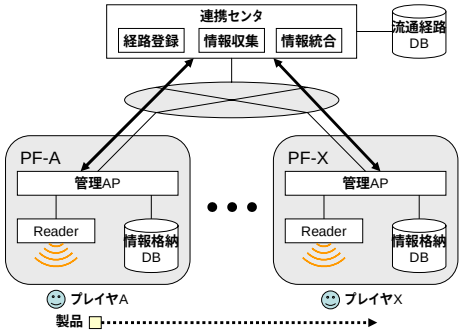

図 1 異種 PF 連携モデル

各 PF の情報格納 DB には、各プレイヤが所有した製品のトレース情報が登録される。トレース情報には、入出荷時間や商品情報等の流通経路上のプレイヤのみに公開したい情報が含まれている場合がある。製品の流通経路が既知であれば、流通経路上の PFID や属性(PF 属性)により指定することで、アクセス権限を付与することができる。しかし、製品の流通経路が未定の場合には、あらかじめ公開先の PF を特定することができないため、PFID や PF 属性に基づいたアクセス制御方式を適用できないという問題がある。

例えば、図 2 のように、製品が複数の PF を経由して流通する場合、製造者は出荷時点では各製品が流通していく PFID を特定できないため、PFID を指定してアクセス権限を設定することができない。また、ルート A を通ることが確定した時点では、既に製品が製造者の手元に無いため、このタイミングでアクセス権限を変更することはできない。

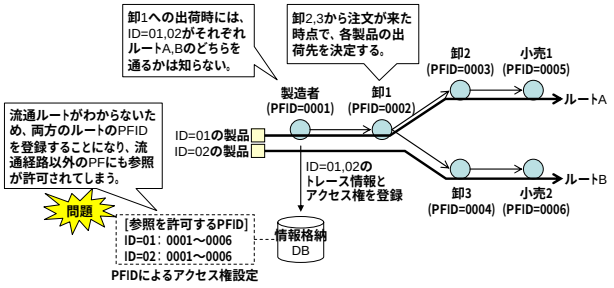

図 2 アクセス制御の問題

3. 提案方式

異種 PF 連携モデルの情報収集機能では、連携センタが流通経路 DB から経路情報を読み出し、経路情報として登録された PF からトレース情報を収集する。提案方式では、連携センタが経路情報を読み出す際に、アクセス元 PF の流通経路 DB への登録状況を確認し、その登録状況に基づいてアクセス制御を行う。このとき、実際の流通経路どおりのアクセス制御を行うためには、流通経路 DB に経路情報が正しく登録されている必要がある。そこで、製品を所有するプレイヤのみが経路情報を登録できるよう制御を行うことで、登録される経路情報の正当性を担保する。

具体的には以下の 2 つの仕組みからなる。

(1) 経路情報の登録制御

流通経路 DB に登録される経路情報の正当性を担保するために、経路情報の登録制御を行う必要がある。そこで、製品がプレイヤ間を移動する際に、移動元のプレイヤが移動先のプレイヤの PFID を連携センタに事前通知し、連携センタでは最後に事前通知された PF からの経路情報の登録要求のみを受け付けるようにす

Access control method based on a distribution channel for traceability information

† Takahiro MIZUNO (mizunotk@nttdata.co.jp)
Kentaro KUNIHIRO (kunihirokn@nttdata.co.jp)
Shigefumi TAKAHASHI (takahashisg@nttdata.co.jp)
NTT DATA CORPORATION

る。これにより、移動元プレイヤが事前通知した PF 以外からは、経路情報を登録することができなくなる。図 3 に、製品がプレイヤ間を移動するときの処理手順を示す。

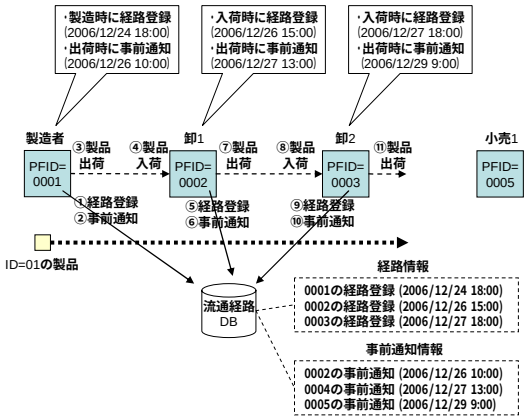

図 3 製品移動時の処理手順

製造者は製造時に経路登録(①)を行い、出荷時に事前通知(②)を行う。以降のプレイヤは、入荷時に経路登録(⑤⑨)を行い、出荷時に事前通知(⑥⑩)を行う。

事前通知を行う権限は、経路情報を最後に登録した PF のみが持つ。すなわち、実際に製品を持っているプレイヤのみが事前通知を行えるようにすることで、悪意のあるプレイヤからの不正な事前通知を防ぐことができる。

また、経路情報が未登録で、かつ一度も事前通知されていない製品については、どの PF からでも経路情報を登録できるようにする。代わりに最上流の PF が登録時に初期登録確認を行うことで、不正な経路情報の登録を防ぐ。初期登録確認では、最上流のプレイヤが当該製品について初めて経路情報を登録する際に、経路情報が未登録であることを確認する。これにより、仮に正当な製造者ではない悪意のあるプレイヤが不正に経路情報を登録した場合でも、登録されている経路情報が不正であることを検知できる。

(2) 経路情報の参照制御

各プレイヤが流通経路 DB に経路情報を登録する際に、参照アクセス権限を設定できるようにする。連携センタは、アクセス元 PF からの参照要求を受けると、流通経路 DB に登録されている経路情報のうち、参照アクセスが許可された PF からのみトレース情報を収集する。流通経路上の PF のみにトレース情報を公開したい PF は、参照アクセス権限を「流通経路上の PF のみに与える」として登録する。このとき、連携センタは、アクセス元 PF の PFID が流通経路 DB に登録されていれば、当該 PF からトレース情報の収集を行う。未登録の場合には、アクセス元 PF が流通経路外の PF であるとみなし、トレース情報の収集は行わない。

以上、2 つの仕組みにより、流通経路が未定の環境下においても、トレース情報の公開範囲を流通経路上のプレイヤに限定できるようになる。

4. 実装例

プロトタイプ実装では、以下の機能を追加することで提案方式を実現した。

(1) 登録制御機能

事前通知テーブルを新設した(図 4:①)。経路情報を登録する際には、連携センタが事前通知テーブルの事前通知日時カラムを参照し、最新レコードの通知対象 PF カラムが登録要求元 PF と同一だった場合のみ、登録を許可する。事前通知を行う際には、連携センタが流通経路テーブルの登録日時カラムを参照し、最新レコードの流通 PF カラムが事前通知要求元 PF と同一だった場合のみ、事前通知を許可する。(図 4:②)

また、初期登録確認の機能として、最上流のプレイヤが流通経路テーブルへ経路情報を登録する際に、同時に登録済み件数を取得するようにし、不正な経路情報が登録されていることを検知できるようにした。

(2) 参照制御機能

流通経路テーブルに、各経路情報の参照権限として次の 3 パターンを設定できるようにした。

all: 全ての PF から参照可能
channel: 流通経路上の PF からのみ参照可能
owner: 他 PF からは参照不可能

参照権限が channel のレコードは、流通経路テーブルの流通 PF カラムに参照要求元 PF が登録されていた場合のみ、参照を許可する。

① 事前通知テーブル

タグID	PFタイプ	通知対象PF	通知者PF	事前通知日時
01	03	0002	0001	2006/12/26 10:00
01	03	0004	0002	2006/12/26 13:00
01	03	0005	0004	2006/12/27 9:00

② 流通経路テーブル

タグID	PFタイプ	流通PF	登録日時	参照権限
01	03	0002	2006/12/26 10:00	all
01	03	0004	2006/12/26 13:00	channel
01	03	0005	2006/12/27 9:00	owner

新しく追加した部分

図 4 流通経路 DB のテーブル設計

5. まとめ

本稿では，経路情報に基づいたトレース情報のアクセス制御方式の提案を行い、実装例を示した。これにより、流通経路が未定の環境でも、トレース情報の公開範囲を流通経路上のプレイヤに限定することが可能となった。

謝辞

本研究は，総務省の平成 18 年度「電子タグの高度利活用技術に関する研究開発」の委託を受け実施している。関係者各位に感謝する。

参考文献

[1] http://www.maff.go.jp/trace/top.htm
[2] 國廣，布田，高橋，桑田，山本，”異種 RFID システムにおけるプラットフォーム連携モデルの提案”，情報処理学会 2005 年 3 月
[3] 布田，高橋，” 電子タグプラットフォーム認証技術に関する提案”，情報処理学会 2006 年 3 月