

## セキュア RFID プロトコル概要

### セキュア RFID プロトコル開発背景

近年、日本の各産業界において、UHF 帯 IC タグ利活用の実証実験、導入が行われています。しかしながら、実証実験、導入が進むに従い、複数の企業間をまたがるサプライチェーンにおける新たな業界共通のニーズとして、プライバシー情報保護・企業情報保護への対応が IC タグに求められるようになりました。

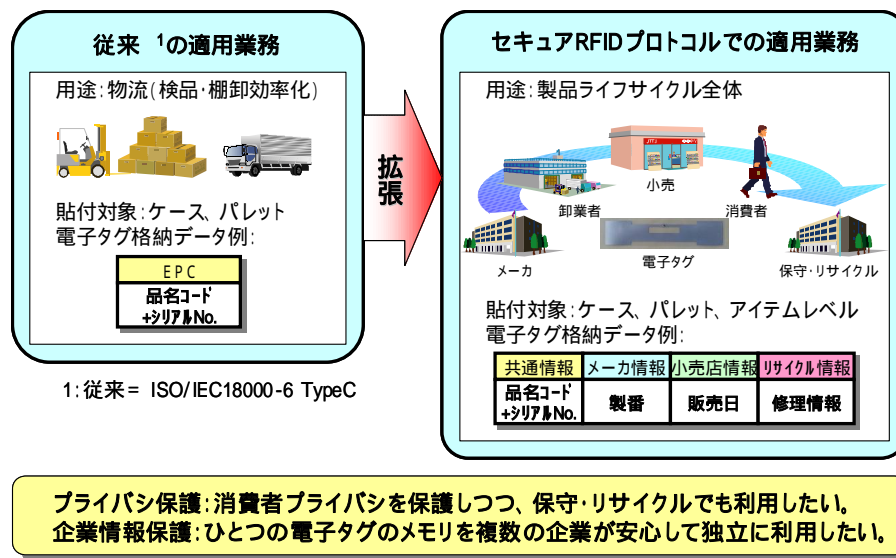


図 1 IC タグへの市場ニーズの変化

これらを解決する取り組みとして、経済産業省は研究開発委託事業「UHF 帯電子タグの技術開発事業 (通称:セキュア電子タグプロジェクト)」(平成 18 年 8 月～平成 19 年 3 月)を実施、日立製作所が受託しました。その成果として「セキュア RFID プロトコル」が開発されました。

### セキュア RFID プロトコル概要

セキュア RFID プロトコルは、UHF 帯 RFID の国際標準規格である ISO/IEC18000-6 Type C 規格を基に新たな機能を追加したもので、ISO/IEC18000-6 Type C 規格と互換性があります。

新たに追加された機能は、大きく分けて以下となります。

- プライバシー情報保護技術 : 通信距離制限機能、読み出し禁止機能
- 企業情報保護技術 : ユーザ領域分割機能

これら新しい機能はセキュア RFID プロトコルに対応した IC タグとリーダライタ装置を使用することによって実現できます。

以下にそれぞれの機能について、説明します。

## プライバシー情報保護技術

UHF 帯の IC タグは、一般に数 m の長通信距離を特徴としており適用業務の拡大に寄与してきましたが反面、悪意のある第三者が、IC タグ所有者に無断で離れたところから IC タグの情報を盗み取る可能性が懸念されていました。つまり IC タグが貼付された商品を販売した場合、その商品を購入した消費者は、その商品情報を意図しない第三者に盗み取られるプライバシー上の懸念があったのです。

ISO/IEC18000-6 Type C 規格では、消費者のプライバシー情報を保護する方法として、IC タグを無効化(Kill)するか、IC タグのデータを削除する方法があります。しかし、これらの方法では保護手段を実施したのち IC タグのデータを読み出しできなくなるため、二次流通(保守・リサイクル)の段階で IC タグの再利用をすることが困難でした。

セキュア RFID プロトコルでは、消費者のプライバシー情報保護と、保守・リサイクル段階での IC タグの再利用を両立させる方法として、以下のプライバシー情報保護技術が採用されています。

### 1. 通信距離制限機能

IC タグの通信距離を制限したり、制限を解除する機能です。本機能を使用することにより数 m の通信距離を数十 cm まで短くすることが可能となります。

商品販売時には IC タグの通信距離を制限することにより、離れたところからの IC タグ情報の不正な読み取りを制限します。二次流通、リサイクル段階においては、IC タグの通信距離の制限を解除することによって、再利用が可能になります。

### 2. 読み出し禁止機能

IC タグの情報を読み出し禁止、解除する機能です。本機能の実行は、パスワード認証によるアクセス制限をすることが可能です。

プライバシー上問題となるような IC タグの一部の情報を読み出し禁止とし、残りのデータを保守・リサイクルの段階で読み出し可能にできます。

プライバシー情報保護技術の利用イメージを図 2 に示します。

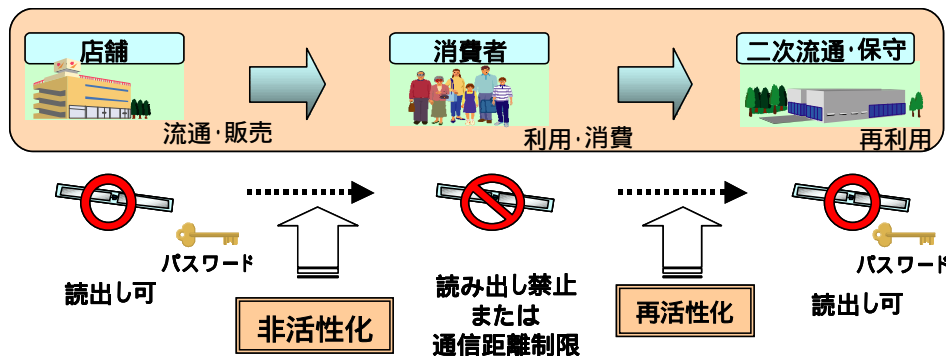


図 2 プライバシー情報保護技術利用イメージ

## 企業情報保護技術

ISO/IEC18000-6 TypeC 規格では、IC タグの格納データの改ざん防止のために、書き込み禁止機能があります。しかし、本機能は IC タグメモリのユーザ領域全体を書き込み禁止する機能しかないので、企業間をまたがる SCM<sup>\*1</sup>において、各企業毎の情報を一つの IC タグに格納する場合、各企業毎に情報の秘匿・改ざん防止することができませんでした。

セキュア RFID プロトコルでは、複数企業間での企業情報保護を実現する方法として、IC タグメモリのユーザ領域分割機能を採用しました。

<sup>\*1</sup> SCM(Supply Chain Management) : 調達から製造、物流、販売、サービスといった、モノづくりから販売までのプロセスにおける情報の流れを整理・統合し、全体で共有する取り組み

### 1. ユーザ領域分割機能

ユーザ領域を複数ブロックに分割し、各ブロックごとのパスワード認証により、ブロック毎に読み出し、書き込みの可否を設定する機能です。本機能により、異業種間にわたるオープン SCM などでも、各企業の情報の秘匿、改ざん防止が可能となります。

企業情報保護技術の利用イメージを図 3 に示します。

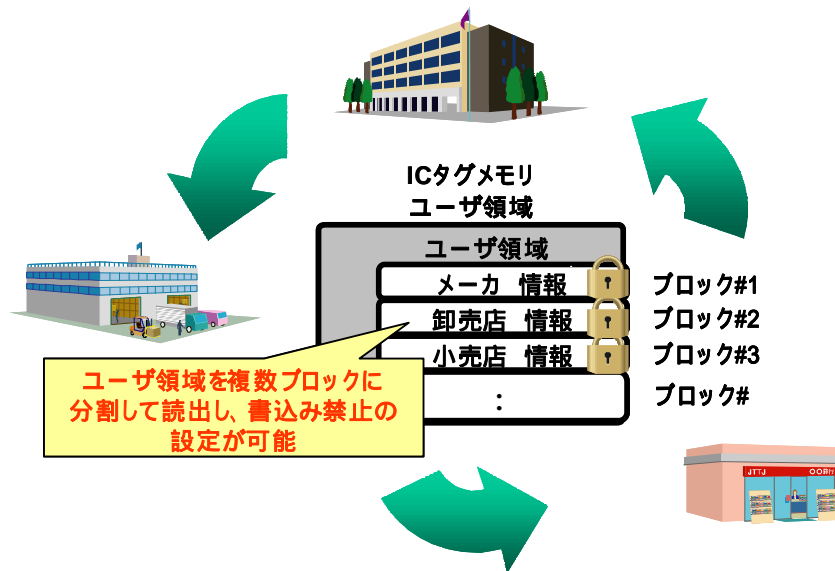


図 3 企業情報保護技術利用イメージ

### セキュア RFID プロトコルの互換性

セキュア RFID プロトコルは、UHF 帯 RFID の国際標準規格である ISO/IEC18000-6 Type C 規格を基に新たな機能を追加したもので、ISO/IEC18000-6 Type C 規格と互換性があります。ISO/IEC 18000-6 Type C 対応(セキュア RFID プロトコル非対応)のリーダライタ装置でセキュア RFID プロトコルに対応した IC タグのご使用の際には、セキュア RFID プロトコル特有の機能はご使用できませんが、ISO/IEC18000-6TypeC 規格の IC タグ、リーダライタとしてご使用できます。

ISO/IEC18000-6TypeC 規格との互換性の相関図を図 4 に示します。

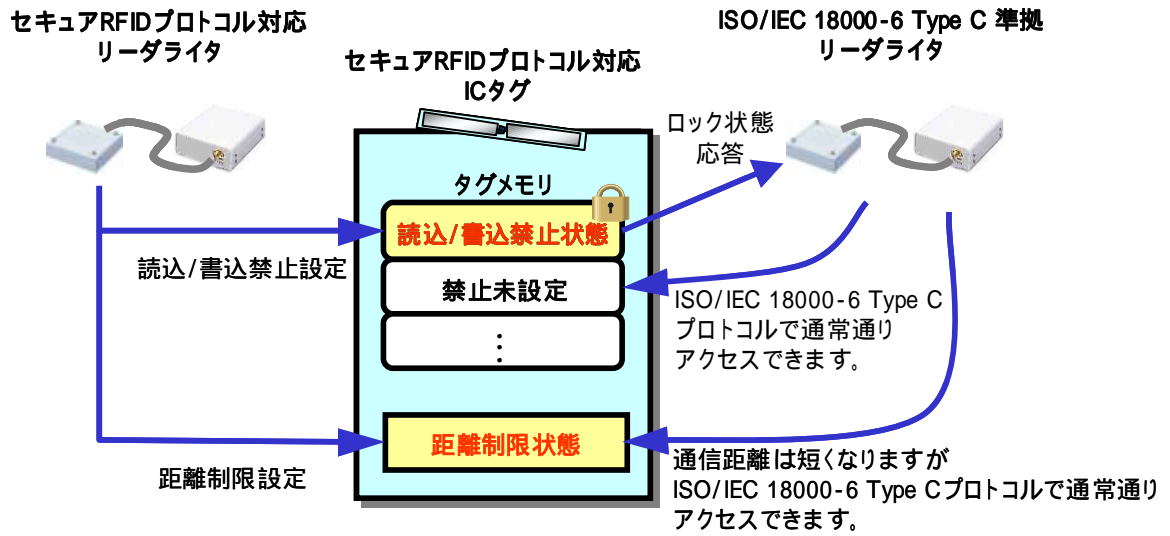


図 4 セキュア RFID プロトコル互換性相関図

以上