IC カードトランザクション処理方式の考察

吉田壱　鈴木勝彦　平田真一　山本修一郎
NTT 情報流通プラットフォーム研究所
E-mail:yoshida.hajime@lab.ntt.co.jp

概要

近年，IC カードが実サービスに本格的に導入されつつある．また，複数のアプリケーションが搭載できる IC カードが出現し，フラッシュメモリを搭載した大容量 IC カードが実用化されている．実用的な IC カードサービスでは，IC カードアプリケーションのトランザクション管理が重要となる．本報告では，IC カードシステムにおける障害について検証し，中でも特に重要な，IC カードへの電源供給断の障害に対する，大容量・マルチアプリケーション IC カード向けの復旧方式を提案する．また，実装を行い，本方式が実用的な時間で処理可能であることを確認する．

Consideration of a transaction processing method for Smartcard systems

Hajime YOSHIDA, Katsuhiko SUZUKI, Shinichi HIRATA, Shuichiro YAMAMOTO
NTT Information Sharing Platform Laboratories
E-mail:yoshida.hajime@lab.ntt.co.jp

Abstract

The business services that use smart cards are beginning to be offered. Along with the trend that the cards are having multiple applications on the cards, some smart cards that install large flash memory will be put to practical use. If the smart cards are used with these business services, the transaction processing becomes important. In this report, we firstly verify the problems in the smart card systems and understood the major of them is an interruption of the power supply to the smart cards. Secondly, we propose the error recovery method for smart cards with large flash memory and multiple applications installed. And finally, we implement and evaluate the proposed method to conclude that this method is effective.

1. はじめに

近年，IC カードは計算能力を持ったセキュアなデバイスであるという特長により，テレホンカードや定期券やポイントサービス，クレジットカードなど，既存のカードサービスの置き換えだけでなく，本人認証サービス，電子マネーや電子チケットなど，IC カードでしか提供できないサービスなども提供され始めており，本格的に普及しようとしている． 一方，一枚のカードに複数のサービス/アプリケーションが格納可能なマルチアプリケーション IC カードが実用化されている．

NTT 情報流通プラットフォーム研究所では，このようなマルチアプリケーション IC カードに対して，ネットワーク経由でサービスを追加，削除を可能とするために，IC カードプラットフォーム NICE(Net-based IC Card Environment)を開発している．

現在，IC カードプラットフォームの運用モデルに関しては報告されているが，IC カードプラットフォームにおいて発生する障害分析，及び障害復旧に関する報告はない．

本稿では，IC カードプラットフォームで発生する障害を分析し，IC カードに求められる障害復旧機能，及び障害復旧に必要なメモリ管理方式に関して報告する．

2. IC カードの特徴

IC カードは，携帯電話や PDA(Personal Digital Assistants)のような装置と比較して以下のような特徴を持つ．

(1)耐タンパデバイスであるため，不正なアクセスによるデータの読み出し，改ざんが困難である．

(2)内蔵電源を持たないため，端末(リーダライタ)から電力が供給されることにより動作可能となる．

(3)IC カードの状態を利用者に伝えるための GUI 機能を持たないため，利用者とのインタラクションは端末経由で行う．

特に(2)に関しては，IC カードのトランザクション処理を検討する上で重要な特徴である．

3. IC カードプラットフォーム運用時に発生する障害

IC カードプラットフォームは，サーバ，端末(リーダライタ)，IC カードから構成される．図 1 に IC カードプラットフォームの構成例を示す．

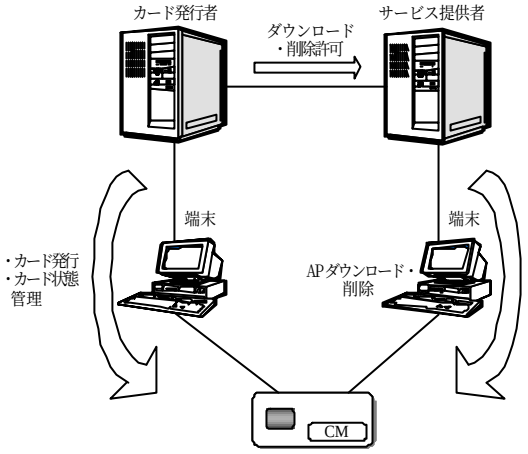


図 1:IC カードプラットフォームの構成例

IC カードプラットフォームの運用中に発生する可能性がある障害を以下に分類する．

(1) サーバ障害
(2) サーバ-端末間の通信障害
(3) 端末障害
(4) 端末-IC カードの通信障害
(5) IC カード障害

(1)～(3)に関しては，オンラインシステムでの

障害対応技術として従来より検討されている．(4),(5)は IC カード自身の破損等の障害以外に，端末からの電源供給断による障害が考えられる．このような障害は，非接触 IC カードを考えた場合，駅の**改札口**におけるタッチ＆ゴーのように IC カードと端末が動的に接続され，かつ利用者による操作が含まれることにより，発生する可能性が高い．このことから，以降の章では，IC カード処理中の電源供給断が発生した際の問題点，障害に対する復旧処理に関して述べる．

4. IC カード処理の中断による問題

IC カードに対しての電源供給断により，予期しない IC カード処理の中断が発生する．このことにより，サーバが管理する IC カードの状態情報と IC カード内で管理する情報の不一致が発生する可能性がある．

一般的に IC カードシステムの 1 トランザクションは，サーバからコマンドを発行し，IC カードからの応答をサーバが取得するまでである．前述の問題点は，トランザクション中に障害が発生した場合の処理が，サーバと IC カードで異なるポリシで運用されている場合に発生する．このことから，トランザクション中に障害が発生した場合，トランザクション開始前の状態にサーバ，IC カードを復旧するポリシで運用することが必要であると考える．

サーバのトランザクション管理方式に関しては，実用化レベルの技術が確立されているため，本稿での説明は省略する．

IC カードのトランザクション管理方式に関しては，単一サービス向けの小容量メモリカードにおいては，データ形式/データサイズが固定であるため，メモリの二重化管理の方式により実現している例はあるが，データ形式/データサイズが固定とならないマルチアプリケーション IC カードに対しての方式は確立されていない．

5. IC カードトランザクション処理に要求される機能

IC カード内で不揮発メモリへの書き込み処理を行っているときに電源供給断が発生した場合，不揮発メモリ上のデータが不定となる．

このため，IC カードはトランザクション開始前（コマンド受信前）の不揮発性メモリの状態をトランザクション完了（レスポンス返却）まで保持し，トランザクション中に障害が発生した場合，保持している情報を復帰するための機能が必要である．前述以外にマルチアプリケーションに適したメモリ管理方式の要件として以下がある．

(1)複数のデータ形式を扱えること．
(2)可変長のデータが管理可能であること．

以上の条件を満たすメモリ管理方式に関して述べる．

6. マルチアプリケーション対応 IC カードメモリ管理方式の提案

現在の IC カードは，メモリデバイスと EEPROM，フラッシュメモリを採用している．

フラッシュメモリを採用している IC カードは，EEPROM を採用している IC カードと比較して 10 倍以上の容量(EEPROM:64KB 程度，フラッシュメモリ:1MB）であるため，今後マルチアプリケーション IC カードとして有用なデバイスと言われている．このことから，フラッシュメモリを対象としたメモリ管理方式の検討結果に関して以降の章で説明をする．

7. フラッシュメモリの特性

ここで, 対象とするフラッシュメモリにおけるメモリ管理方式の設計上考慮すべき特性について述べる.

フラッシュメモリは以下の特徴を持つ.

①不揮発性
②高密度
③低消費電力
④高速読み書き
⑤低コスト

上記の特徴により，面積や消費電力が問題となる組み込み機器である IC カードのメモリデバイスとして優れている.

しかし，フラッシュメモリは, EEPROM や通常の RAM と異なり，完全ビット変更性(Fully Bit-Alterable)がない．つまり，EEPROM や RAM では，データを書き換えるときに，あるビットについて，'1'→ '0'の変更も '0'→ '1'の変更も可能であるが，フラッシュメモリの場合，あるビットについて，'1'→ '0'の変更は可能であるが '0'→ '1'の変更は不可能**である．このため，**ビットを '0 '→ '1 'に変更するようなデータ更新があった場合，まず，データを一旦クリアしてから新しいデータを書き込むという方法をとる.

ここで注意すべきフラッシュメモリの特性はフラッシュメモリの消去はメモリブロックの単位でしか行えないことである. 1 バイトだけ書き換えるために, 1 ブロックのデータを消去し, 1 バイト書き換えたデータを 1 ブロック分書き戻す必要があり, 一般的なフラッシュメモリを使用した場合, 1 バイトの書き換えに少なくとも1 秒掛かる.

このような特性により, EEPROM のような完全ビット変更性のあるデバイスを前提としたメモリ管理方式は適用できない. 従来の IC カードのトランザクション管理方式であるメモリの二重化管理は，完全ビット変更性のあるデバイス を前提とした方式であるため適用ができない.

8. トランザクション処理方式の提案

8.1. メモリ管理方式

本方式では，メモリ領域を図 2 に示すデータ構造で管理し，論理メモリ領域を物理メモリ領域と対応させる．このようにしてアロケーションテーブルから物理メモリをたどっていくことにより，論理

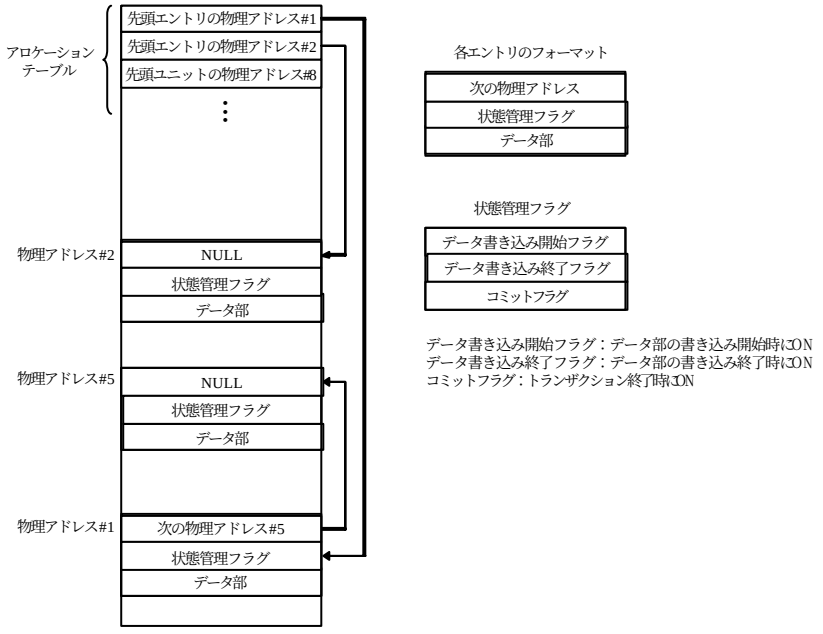


図 2 :メモリ配置イメージ

アドレスに格納されている最新データを検索する．また，データ書き込みでは，新しくメモリユニットをメモリ上に確保し，リストに追加する．

この方法により，更新前の情報を消去せずに，更新後の情報を追記していくことが可能になる．このことから，電源供給断が発生した場合でも，トランザクション開始前の状態に復旧が可能となる．

データ部のトランザクション状態を示すフラグ（状態管理フラグ）より，正常にトランザクションが完了しているか，トランザクション処理中に障害が発生により処理が中断しているか，の判断を可能とする．データ書き込み時には，図 3 に示す処理を行う．

最初に新しく必要なメモリユニットを確保し，新しい領域にデータを書き込む．メモリユニットを確保した時点で状態管理部の「データ書き込み開始フラグ」をON 状態とし，メモリ書き込みが完了した時点で「データ書き込み終了フラグ」をON 状態とする．

最後に IC カードの トランザクション完了の時点で，トランザクション中に生成された全メモリユニットの「コミットフラグ」を ON にする．

このメモリ管理方式を行うことにより，電源供給断が発生した場合は，メモリユニットの 状態管理フラグの状態が 「書き込み開始フラグ」または 「書き込み終了フラグ」が ON，「コミットフラグ」が OFF の状態になるため，これらのフラグ情報を利用することにより，復旧処理の要否を判断することが可能になる．

8.2. 復旧処理

メモリユニットの状態管理フラグの状態が電源供給断を示す状態である場合，IC カード電源供給時（IC カード活性化時）にメモリユニットの状態の復旧処理を行う．メモリユニットの復旧処理は以下の通りである．

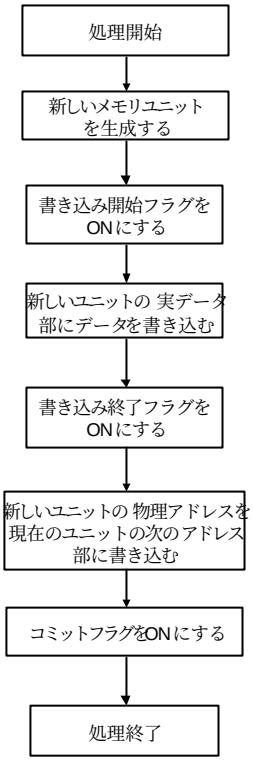


図 3:メモリ書き込みフロー

(1) データ書き込み開始フラグ:ON,
データ書き込み完了フラグ:ON,
コミットフラグ:OFF の場合

[復旧処理] データ部の書き込みが正常に終了しているが，トランザクション完了前に障害が発生している．この場合は，メモリユニットを廃棄し，更新前のメモリユニットと同一データのメモリユニットを新規に作成し，復旧する．

(2) データ書き込み開始フラグ:ON,
データ書き込み完了フラグ:OFF,
コミットフラグ:OFF の場合

[復旧処理] データ部の書き込みが完了する前に障害が発生している．この場合は，更新前のメモリユニットから新規に作成したメモリユニットのリンク情報（次の物理アドレス）の設定が完了

していない可能性があるため，更新前のメモリユニットのリンク情報を復旧した後に新規に作成したメモリユニットを廃棄し，更新前のメモリユニットと同一データのメモリユニットを新規に作成し，復旧する．

9. 実装・評価

今回提案したメモリ管理方式を NTT が開発した ELWISE カード[4]に実装し，性能評価を実施した. ELWISE カードの主要機能と性能を表 1 に示す．

表 1 :ELWISE カードの主要機能と性能

機能	ELWISE カード	標準的な市販品
CPU	16bit, 30MHz	8bit, 3.5～5MHz
暗号・認証処理コプロセッサ	ESIGN, RSA, 楕円曲線対応の演算機能	RSA 対応の演算機能
RAM	8KByte	128～512Byte
不揮発性メモリ	1MByte フラッシュメモリ	8～32KByte・EEPROM
入出力速度	9.6～76Kbit/s	9.6Kbit/s～32Kbit/s

今回開発したメモリ管理モジュールは下記に示す機能をアプリケーションに提供する．

(1)メモリ空間の初期化機能(Init)

(2)データ消去機能(Erase)

(3)データ読み出し機能(Read)

(4)データ書き込み機能(Write)

(5)データ比較機能(Compare)

(6)トランザクション開始機能
(Begin Transaction)

(7)トランザクションコミット機能
(Commit Transaction)

(8)トランザクションアボート機能
(Abort Transaction)

(9)ガーベージコレクション機能
(Garbage Collection)

(6)～(8)の機能により，トランザクション処理の開始処理と終了処理を実行する．IC カード処理中に(6)の実行後に(7) or (8)が実行されていない場合，次回の IC カード活性化時に自動的にデータの復旧処理が実行される．

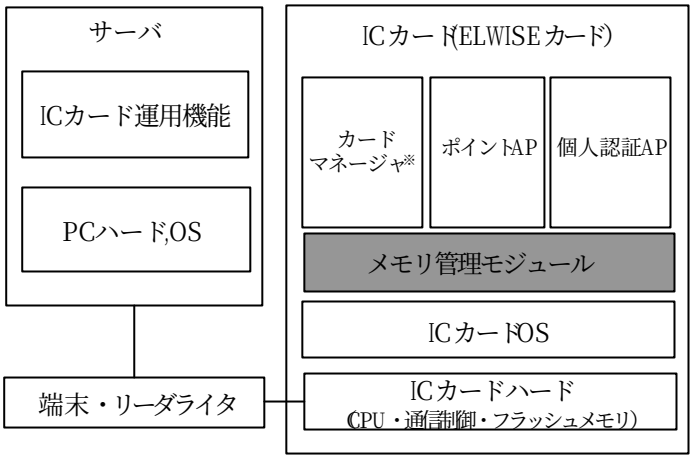
(9)の機能は，本メモリ管理方式の場合，データの更新が発生する毎に更新前のデータがメモリ領域に全て残るため，最後には新しくメモリユニットを新規に作成できなくなり，データの更新処理ができなくなる．そのため，あるタイミングで参照されなくなったメモリユニットを消去するための機能である．

メモリ管理モジュールの性能評価として，基本処理であるデータの読み出し・書き込み処理の処理時間を測定した. 処理時間の測定結果を表 2 に示す．処理時間は IC カード内の処理時間のみである．

表 2 :処理時間

処理	データサイズ	時間
読み出し処理	32byte	10ms
	64byte	20ms
書き込み処理	32byte	20ms
	64byte	30ms

データ書き込みとデータ読み出しに対するフラッシュメモリのハードウェア処理時間が 1ms 以下であるため，表 2 に示した処理時間は，メモリ管理モジュールの処理時間（アルゴリズム処理時間）である．



※）カードマネージャ :APをダウンロード，削除，実行を行うモジュール

図4 ICカードシステムの構成

次に，IC カードを利用したサービスとして一般的なポイントサービス，本人認証サービス(PIN 認証サービス）に，本モジュールを適用することでフィージビリティの検証を行った．評価に利用した IC カードシステムの構成を図 4 に示す．各サービスに対応した IC カードアプリケーション(IC カードAP)の機能は以下の通り．

(1)ポイントサービス AP

a.ポイントの加算：

サーバからのコマンドで送信されるポイントの値と，IC カードの不揮発メモリ上に格納されているポイントの値を加算した値を不揮発メモリ上に書き込む機能

b.ポイントの 減算

IC カードの不揮発メモリ上に格納されているポイントの値から，サーバからのコマンドで送信されるポイントの値を減算した値を不揮発メモリ上に書き込む機能

(2)本人認証サービス AP

a.PIN の設定：

サーバからのコマンドで送信される PIN をIC カードの不揮発メモリ上に書き込む機能

b.PIN の照合：

サーバからのコマンドで送信されるPIN とIC カードの不揮発メモリ上に書き込まれたPIN をIC カード内で比較する機能

各アプリケーションが実行するメモリ管理モジュールの機能と実行回数を表 3 に示す．

表 3 :アプリケーション利用機能

アプリケーション	トランザクション	機能（回数）
ポイントサービス	ポイントの加算	・Init(1) ・Read(1) ・Write(1)
	ポイントの減算	・Init(1) ・Read(1) ・Write(1)
本人認証サービス	PIN の設定	・Init(1) ・Write(1)
	PIN の照合	・Init(1) ・Compare(1)

各アプリケーションの処理時間を表 4 に示す．処理時間はサーバ/端末-IC カード間の通信時間も含む．

表 4 :アプリケーション処理時間

アプリケーション	トランザクション	時間
ポイントサービス	ポイントの加算	120ms
	ポイントの 減算	120ms
本人認証サービス	PIN の設定	110ms
	PIN の照合	100ms

各アプリケーションのトランザクション時間は，1 秒/トランザクションであれば実用上問題ないと考えられる．表 4 の結果から，全トランザクションが約 100ms で完了していることから，実用的なメモリ管理方式であることを確認できた．

10. まとめ

本報告では，IC カードプラットフォームで発生する障害を分析し，IC カードに求められる障害復旧機能を提案した．また，マルチアプリケーション IC カードに適したデバイスであるフラッシュメモリに対して有効なメモリ管理方式を提案し，実装，評価を行った．
性能評価では，一般的な IC カードサービスであるポイントサービス，本人認証サービスを対象として実施し，実用的な処理時間でトランザクションが完了することを確認した．

11. 参考文献

[1]Information technology Identification cards Integrated circuit(s) cards with contacts ISO/IEC 7816-4:1995
[2]JIS X 6304：外部端子つき IC カード－電気信号尾帯伝送プロトコル
[3] “IC カード総覧”,株式会社シーメディア 2000
[4]竹田ほか，接触型超多目的 IC カードシステムの開発，NTT 技術ジャーナル，Vol.49，No.12，PP733-739, 2000
[5] 山本,竹内,細田,“ネットワーク指向 IC カードプラットフォーム”,NTT R&D Vol.49,No.12,2000
[6] 田中康之，”フラッシュファイルシステムのファイル管理技術”,Interface Jan2000,
[7]樋浦・鈴木・吉田：“フラッシュメモリ型 IC カード向け Java カード(Sapphire)の実装と評価,” 電子情報通信学会, KBSE2000-55, 2001.01