非接触カードの復習

冨島 千歳，田中 美里
Chitose TOMISHIMA, Misato TANAKA

1　はじめに

近年，磁気ストライプカードやICカードに続き，読取端末にかざすだけで利用できる非接触カードの普及が進んでいる．非接触カードは鞄や財布に入れたまま利用できるため，操作性に優れている．また，読取端末との接触部を持たないため，接触不良などの問題がなく，メンテナンス性が高い．本報告では，非接触カードの概要と分類について述べた後，非接触カードの原理や，どのように通信を行っているか，また非接触カードが抱える問題点について述べる．

2　非接触カードの概要

非接触カードとは，外部の通信端末であるリーダライタとの電磁波通信により，カード内部の情報を読み書きできるICカードのことである．非接触カードは1980年代半ばから入退室管理などに利用され始め，日本では，2002年にJR東日本がSuicaの利用を開始したことによって普及が進んだ．現在では，以下に示すように多くの分野で利用されている．

- 交通機関
  乗車券としての利用が盛んである．また，これらの非接触カードは電子マネーとしても利用範囲を広げている．
  - PiTaPa（スルット関西）
  - ICOCA （JR西日本）
- サービス・流通
  最近では，顧客管理のために，非接触カードをポイントカードやメンバーズカードとして発行する企業が増えてきている．
  - Edy（ビットワレット）
  - nanaco（セブンイレブン）
- 公共機関
  - 住民基本台帳カード
  - e-パスポート
- 企業セキュリティ
  - 社員証
  - 入退室管理

3　非接触カードの分類

3.1　通信距離による分類

非接触カードは，ISO/IEC（International Organization for Standardization/ International Electrotechnical Commission : 国際標準化機構/国際電気標準会議）[2]によって，カードとリーダライタ間の通信距離の違いにより「密着型」「近接型」「近傍型」の3種類に分類されている．このほか，「マイクロ波型」という通信距離70cm以上のものもあるが，標準化された規格ではない．Table 1にそれぞれの特徴を示す．

Table1　通信距離による非接触カードの分類（参考文献[3]より参照）

形式	密着型	近接型	近傍型	マイクロ波型
通信距離	～2mm	～10cm	～70cm	70cm～
クロック周波数	4.91MHz	13.56MHz	13.56MHz	2.45GHz
初期通信速度	9.6Kbps～	106Kbps～	～26Kbps	1.0Mbps～
通信方式	電磁結合/静電結合	電磁誘導	電磁誘導	電波
用途	電子マネー	入館カード		ETC

近傍型や近接型では誤ってリーダライタと通信してしまう可能性がある．そのため，金銭や個人情報などの重要な情報を扱うカードでは，密接型が使われている．また，近接型や近傍型は，鞄や財布の中にカードを入れた状態でもリーダライタとの通信を行えるため，会社の入館カードなど，認証に利用されている．マイクロ波型は，高速道路の料金支払いに用いられているETC（Electronic Toll Collection）などが該当する．

3.2　近接型における通信方式による分類

近接型については，変調方式や符号化方式などの違いから「TypeA」「TypeB」の2種類が標準化されている．「TypeA」はICテレホンカードなど，「TypeB」は住民基本台帳カードなどに利用されている．また，SuicaやICOCAなどに利用されている「FeliCa」[4]も日本では普及している．Table 2に各種の特徴を示す．

Table2　近接型非接触カードの通信方式による分類（参考文献[3]より参照）

名称	TypeA	TypeB	Felica
CPU	あり/なし	あり	あり
変調方式 ASK[*1]変調度	100 %	8～14 %	10 %
符号化方式	変形ミラー，マンチェスタ	NRZ[*2]	マンチェスタ
通信速度	106Kbps	106Kbps	212Kbps

[*1] Amplitude Shift Keying：振幅偏移変調
[*2] Non-Return to Zero

4　非接触カードの原理

4.1　原理

非接触カードの構造を Fig. 1 に示す．非接触カードには，IC チップとアンテナコイルが搭載されている．IC チップは CPU，メモリ，電源回路，復調回路，変調回路などによって構成されている．アンテナコイルはリーダライタとの情報伝送において用いられる．なお，一部の非接触カードには CPU が含まれていない．

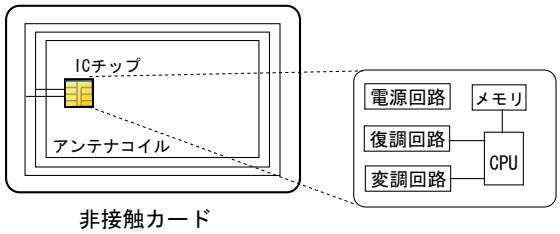

Fig.1　非接触カードの構造（参考文献 [1] より参照）

非接触カードとリーダライタ間の通信方式には，静電結合と電磁結合，電磁誘導，電波の 4 種類存在する．多くの非接触カードでは電磁誘導方式が利用されている．非接触カードとリーダライタ間の電磁誘導による通信手順を，以下に示す．

1. リーダライタ側のアンテナコイルに電流を流すと，交流磁界が発生する．
2. 交流磁界の中に非接触カードをかざすと，電磁誘導によりカード側のアンテナコイルに交流電圧が誘起される．
3. 誘起された交流電圧が，カード内で直流電圧に変換される．これを電力とし，IC チップが動作する．
4. カードとリーダライタ間で情報の伝送が行われる．(3.2 節)
5. 余った電圧を放電する．

非接触カードは電池を保持しない．これは，上記で述べたように情報伝送に必要なカード側の電力が，電磁誘導によって供給されるためである．

4.2　情報の伝送

リーダライタからカードへの情報伝送は，リーダライタの交流磁界によって生じるカード内の電圧を利用する．リーダライタは，交流磁界を調節することにより，カードが得る電圧を変化させる．この電圧変化を，IC チップ内の復調回路で復調することにより情報伝送を行う．この交流磁界により発せられる電磁波を搬送波という．(Fig. 2)

カードからリーダライタへの情報伝送においても，リーダライタの発する交流磁界が用いられる．カードは，リーダライタの交流磁界を変化させることにより情報を伝送する．この変化による電磁波を副搬送波という．リーダライタは，これを復調することで情報を読み込む．非接触カードは自ら搬送波を発しないことで，カード側の使用する電力を省力化している．これは，電池を持たない非接触カードに適した伝送方式となっている．

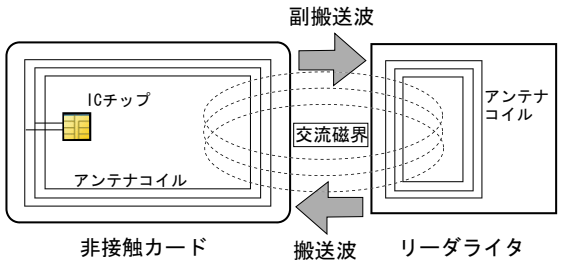

Fig.2　非接触カードとリーダライタの通信（参考文献 [1] より参照）

4.3　メモリ

非接触カードのメモリは，プログラム用のプログラムメモリ，データ格納用のデータメモリ，データ処理用のワーキングメモリからなる．非接触カードは電源を保持しないため，データメモリには不揮発性のメモリが使用されている．

メモリサイズは，その用途によって異なる．一般に，入館カードなど情報量の少ない場合はメモリサイズが小さい．一方，列車運賃の支払いなどに用いられるカードでは，乗車駅や運賃など多くのデータを保持しなければいけないため，メモリサイズは大きくなる．

5　通信プロトコル

5.1　概要

カードとリーダライタの通信には，Fig. 3 に示すように，初期応答と活性状態の 2 状態が存在する．通信は，常にリーダライタがコマンドを送出し，それをカードが受信して応答することによって行う．

[初期応答]

初期応答では，リーダライタと目的のカードとの通信路を確保する．カードは，リーダライタの交流磁界に入ると電源が供給され，その後リーダライタからのリクエストコマンド待機状態になる．リーダライタからリクエストコマンドが送信され，カードが応答することにより，カードがリーダライタに認識される．その後，通信速度などの条件をカードとリーダライタ間で相互に確認する．

[活性状態]

活性状態では，リーダライタとカード間で伝送ブロックを用いた情報伝送を行う．この伝送ブロックは，先頭フィールド，情報フィールド及び最終フィールドの 3 つで構成される．先頭フィールドには全体の伝送をコントロールするための情報が含まれている．リーダライタのコマンドや，カードのレスポンスは情報フィールドに含まれる．また，エラー検出コードが最終フィールドとして付加される．

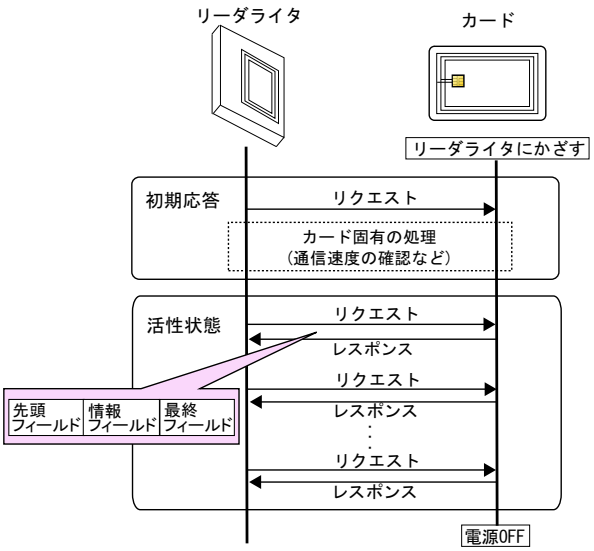

Fig.3　通信シーケンスの概要（参考文献 [1] より参照）

5.2　アンチコリジョン

現在普及している非接触カードは，同じ分類であってもサービス同士の互換性がないものが多い．そのため，複数枚のカードを同時にリーダライタにかざすと，カードを正しく認識できない状態が発生する．この状態をコリジョンという．その対策をアンチコリジョンといい，手法としては以下のものが挙げられる．

- ビットコリジョン方式
  主に TypeA のカードで利用されている．この方式では，リーダライタは，カードの応答ビット列を順番に受信していく．コリジョンが発生すると，発生したビット以降について，それぞれのビットパターンのカードのみに応答を求め，受信を続ける．すべてのカードが識別されるまで，これを繰り返す．
- スロットマーカ方式
  主に TypeB のカードで利用されている．この方式では，まずリーダライタ側からのリクエストに対し，カードがそれぞれ乱数を生成する．その後，リーダライタがその乱数 1 つ 1 つを順に問い合わせていく．
- タイムスロット方式
  主に Felica で利用されている．この方式は，スロットマーカ方式と同様に，リーダライタ側からのリクエストに対し，カードがそれぞれ乱数を生成する．その後，カードがその乱数に応じたレスポンス時間帯にレスポンスを返すことでカードの特定を行う．

5.3　暗号化

非接触カードでは，データをより安全に読み書きする方法として，暗号化が用いられている．暗号化の方式として，公開鍵暗号方式の RSA 方式や共通鍵暗号方式の DES 方式などが用いられている．非接触カードのメモリは，メモリの一部を外部から参照できないようにすることが可能である．これにより，暗号化に使用する鍵の安全を確保することができる．

6　非接触カードの問題点

非接触カードには，電磁波で通信を行うことによる問題も存在する．以下にその問題点について述べる．

- スキニング
  非接触カードでは通信に電磁波を用いるため，カードの所有者が気づかない間に盗聴される可能性がある．これに対しては通信開始時の認証や，暗号化による対策が行われてる．
- 誤って通信を行う
  非接触カードでは，通信を行うつもりがなくても，カードとリーダライタが接近しただけで通信が行われる．そのため，カードの通信距離に応じた用途を選択する必要がある．
- 電源断
  カードとリーダライタ間の通信中にカードの電力が切れることにより，カードの内部状態の異常や破損が起こることがある．そのため，トランザクション処理機能を備えておく必要がある．

7　今後の展望

非接触カードは，交通機関に利用されたことで注目を集め，企業や公共などの多様な分野で普及してきた．最近では，接触型が主であった金融機関や公共機関においても非接触カードが導入され始め，今後も生活に浸透していくと考えられる．

現在では，ほとんどの非接触カードがサービスごとに異なるリーダライタを使用している．しかし，6 種類のカードに対応する NEC のマルチサービスリーダライタ・システムなどが開発され，今後も更に多くのカードに対応したリーダライタが開発されていくだろう．また，これに伴い，異なる分野でのカードが 1 つに統合され，1 枚の非接触カードで様々なサービスが受けられるようになることが期待される．

参考文献

1) NTT 技術ジャーナル (2008 vol.20 No.1)
http://www.ntt.co.jp/journal/0801/index.html
2) IEC - International Electrotechnical Commission ¿ INTERNATIONAL STANDARDS AND CONFORMITY ASSESSMENT
http://www.iec.ch/
3) 重里雅男 : 次世代メモリ FeRAM を搭載した IC カードシステムによるビジネス創出の研究, 第 3 章, pp.8-9, 高知工科大学院 (2004)
4) Sony Japan ｜ FeliCa
http://www.sony.co.jp/Products/felica/