

非接触ICカード 技術とその応用

ソニー(株)ブロードバンドネットワークセンター
i-カードシステムソリューション事業部カード企画部
伊藤 政彦 Masahiko.Itoh@jp.sony.com



開発の背景 —

ソニーでは、1988年から非接触ICカード開発を手がけている。非接触ICカードはこれまでの磁気カードや接触式のICカードとは異なり、読み取り機(以下リーダ)にかざすだけで情報をやりとりできるカードで、ソニーが開発した技術方式を“FeliCa”と名づけている。“FeliCa”はエスペラント語で「楽しい」を意味し、後述するように電子乗車券や今後の電子マネーへの展開などさまざまな分野での応用が期待できる。

当初、非接触ICカードとしてではなく、宅配便の自動仕分けを目的とした非接触ICタグとして開発に着手した。宅配便の自動仕分けは秒速20mで動くベルトコンベア上の荷物の仕分けを行うことが必要だったので、通信距離として3~5m程度、100kbps以上の高速なデータ通信と確実な荷物の識別ができる狭い指向性といった要求があった。そこで、それらの条件を満たすために、2.45GHzのマイクロ波帯を用いたバッテリー付き非接触ICタグに開発の的を絞った。技術的な要求を満たす試作品はできたが、もう1つの重要な課題である経済性の面では現実的ではなく、商品化には至らなかった。

一方、社内では技術レベルの高い研究開発の成果をビジネスに結びつけられる可能性が大きいと考え、参

入できる市場を模索した結果、開発の方向を非接触ICタグから非接触ICカードに変え、1989年には2.45GHz帯を用いたバッテリー付き非接触ICカードでのアクセスコントロール(入退出管理)市場に参入した。当時の製品は、1.5~2m程度の読み取り専用で、幕張に新しく建ったビルのいくつかで採用された。しかし、2.45GHz帯の電波の特長から、近隣で多くのリーダを設置する弊害として相互干渉が起り、読み取り性能が劣化する問題が発生した。その結果、この分野での事業化も望めなくなった。

開発当初から大きな需要が見込まれるのは、電子乗車券の分野と確信していた。しかし、その分野はアクセスコントロールの分野と異なり、要求される技術的仕様がはるかに高いことと、大きな設備投資を必要とすることから電子乗車券の実現には時間がかかると考えていた。しかし、テーマとしてはすでに電子乗車券の研究開発を進めていたJRグループの(財)鉄道総合技術研究所と1988年から1992年まで電子乗車券のための2.45GHzを用いたバッテリーカードの共同開発を行った。

1993年、香港では1997年の中国への返還と同時に非接触ICカードを用いた交通用自動料金徴収システムを導入する計画が発表された。その後、要求仕様が提示され入札が開始された。当時は要求仕様にあったバッテリーなしの非接触ICカードが製品としては世界中どこにも存在していないこともあり、ソニーが開発中の仕様コンセプトが最も高い評価を受け、1994年に香港から300万枚のバッテリーなし非接触ICカードを大量受注した。それに伴いその後は開発スピードをさらに加速し、非接触ICカードだけでなくコンパクトで高性能なリーダの開発、非接触ICカードの製造プロセスの開発、製造装置およびラインの立ち上げと一気に事業を立ち上げた。受注から1年後の1995年には、パイロットテスト用の13.56MHzの短波帯を用いたバッテリーなし非接触ICカードの納入を開始した。1997年9月には、予定されていたサービスが一斉に本格稼働し始め、業界の大きな注目を浴びるようになった。

“FeliCa”の技術的特長 —

“FeliCa”技術方式は表-1に示すように、非接触ICカードとして特に交通用途で要求される高速処理と高

項目	仕様
電力伝送	13.56MHz無変調
データ通信の変調方式 (リーダ⇨カード)	13.56MHz電力波に対して 10%ASK
データ通信の変調方式 (カード⇨リーダ)	カード内LSIのロードスイッチング
データ通信の符号化方式 (リーダ⇨カード)	マンチェスター符号
データ通信速度 (リーダ⇨カード)	212kbps, 423kbps, 848kbps
CPU	8ビット RISC CPU
暗号エンジン	ハードウェア DES or 3DES
データ通信のエラー検出	16ビット CRC
カードICの消費電力	約2~5mW
データ通信の暗号化	相互認証時に発生した乱数をトランザクションごとに変わるトランザクション鍵として用いた64ビットのブロック暗号
データ通信のシーケンスコントロール	相互認証時に発生した乱数をトランザクションごとに変わるトランザクションIDとして用いたシーケンスコントロール
カード内の実メモリ容量	2kバイト, 4kバイト, 8kバイト, 32kバイト
カード内のユーザメモリ容量	1.25kバイト, 2.5kバイト, 5kバイト, ≧25kバイト
処理中断からのメモリ保護	書き込み専用Block (Write Buffer) による保護 8~16block (16byte/1block) までの同時書き込み保証

表-1 “FeliCa” の技術方式

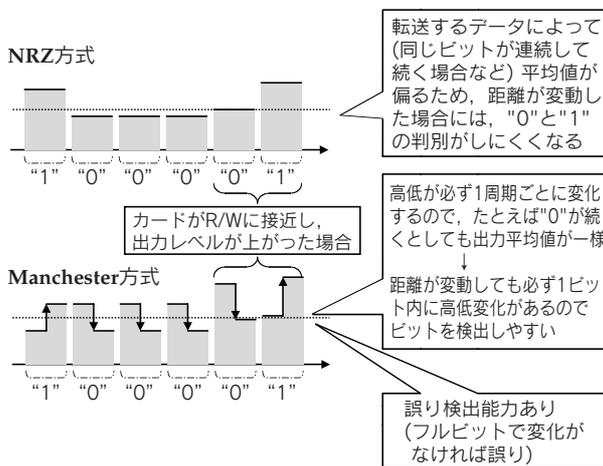


図-1 データ通信の符号化方式比較

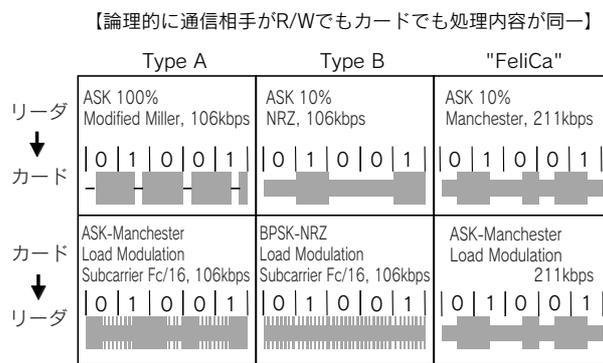


図-2 カード、リーダ間の通信波形

通信信頼性を有し、また 高度なファイルマネージメントを実現している。したがって、金融用途での使用にも耐え得るセキュリティの高い技術であるといえる。

■通信方式

“FeliCa”では図-1に示すように、データ通信の符号化方式としてマンチェスター符号を採用している。比較のため図-1にはNRZ (Non Return Zero) 方式も示す。図-1に示すように転送するデータが同じ“0”のビットが続く場合に、カードがリーダに接近し出力レベルが上がった時には、NRZ方式だと“0”と“1”の判別がしにくくなるのに対して、マンチェスター方式では1周期ごとに必ずデータの高低変化があるために、たとえば同じように“0”データが連続している間にカードがリーダに接近し、出力レベルが上がったとしても、データの誤認識は発生しない。言い換えると1周期の間にデータの高低変化がない場合には誤ったデータであるという検出能力があることになる。“FeliCa”では以上のように高い通信信頼性を有しているといえるのである。

また、図-2にはカードとリーダ間通信の通信波形を示してある。図-2には“FeliCa”の他にISO/IEC-14443のType AとType Bの通信波形も示す。Type AおよびType Bはカードからリーダへの通信時に副搬送波を用いているためにカードからリーダへの通信とリーダからカードへの通信が非対称になっているのが分かる。一方、“FeliCa”ではカード、リーダ間の通信は対称形になっている。すなわち、このことは“FeliCa”ではカード、リーダ間のみならずカード、カード間およびリーダ、リーダ間の通信が可能であることを意味している。この点は“FeliCa”の大きな特長の1つであり、携帯電話への内蔵等新たなアプリケーションに広がる可能性を有している。

■ファイル管理

“FeliCa”では図-3に示すように多階層のファイル構造を持つことができ、各々のファイルに対してアクセス制御情報とアクセス鍵を設定することができる。一方、各々のファイルにアクセスするために、各々のファイルについている鍵でファイルの数だけ相互認証を行う必要はない。それは、各々の鍵をまとめて1つの合

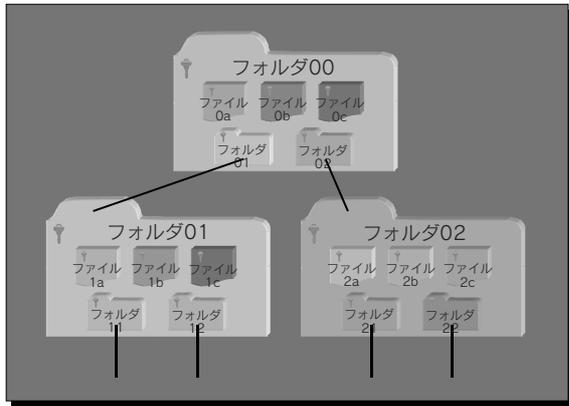


図-3 カード内のファイルのイメージ

成鍵をカード内とリーダー内で作り、その合成鍵を使って1回の相互認証で複数のファイルをオープンできる工夫がなされているからである。したがって、セキュリティレベルを落とさなく複数アプリケーションを同時にアクセスする際のトランザクション時間を大幅に短縮し、高速処理を実現しているのである。

■トランザクション異常時のリカバリー

“FeliCa”の場合は1つのコマンドで複数のファイルに対する処理が可能のため、順次処理が必要なくなる。このことは、非接触ICカードでは大変重要な機能で、一般的にはいつ電力が途切れるか分からない環境で、順次処理を行っている途中で電力が途切れると、各々のファイル間の整合性がとれなくなり、後にリカバリー処理が必要になる。“FeliCa”の場合は、同時処理なので途中で電力が途切れた場合はすべてもとの状態に復帰し、同時にすべてが完了した場合のみ処理終了となる。したがって、リカバリー処理が必要なくなり、上位のアプリケーションソフトウェアの負担が軽減されるのと同時にリカバリー処理を外部の機器が行う必要がなくなるためセキュリティも高い状態を維持できる。

以上のように高い通信信頼性とセキュリティを有した“FeliCa”の通信シーケンスは、①リーダーがカードを検出、②カード、リーダー間の相互認証、③データの読み取り、④データの記録という一連の処理を0.1秒以下で実現できる。

交通用途での応用例 —

現在、“FeliCa”は2001年12月時点で香港向けに約1,200万枚出荷されている。また、シンガポール、中国のシンセン、日本のJR東日本向けにも出荷している。交通用途における非接触ICカードの事業者側のメリッ

トとしては、出改札システムのメンテナンスコストが削減できカードの長期リユースによるコスト削減が可能であること、さらにチケットレス、キャッシュレスなど業務のシステムチェンジが図れることや、新たなビジネスチャンスにつながる点である。一方、利用者側のメリットとしては、1枚のカードで交通機関他(マルチアプリケーション)を利用でき、IC・ネットワーク化の利点として紛失時には残金の返却や再発行が受けられることである。また、非接触による高速処理の実現でパスケースに入れたまま利用(タッチアンドゴー)できるという快適さが大きなメリットである。

香港では、カード運営の専門会社であるクリエイティブスター(Creative Star)社が、オクトパスカード(Octopus Card)という名前で、地下鉄、鉄道、バス、ライトレール(路面電車)、フェリー、ミニバス、ピークトラム(ケーブルカー)等の交通機関向けのストアードバリュータイプの乗車券として運営している。現在、実際に循環しているカードの枚数が約790万枚、平日では1日約650万トランザクション(1回の交通機関の利用を1トランザクションとする)数があり、完全に香港市民の必需品として定着している。

クリエイティブスター社は2000年の末、金融機関としての免許も取得し、オクトパスカードを交通用途以外の領域での汎用電子マネーとしてのサービス拡大に取り組んでいる。たとえば、コンビニエンスストア、ファーストフード店、自動販売機、パーキングメータ、公衆電話等の利用が進んでおり、市民の汎用電子マネーとして発展し続けている。今後は、ETC(Electronic Toll Collection)の領域での利用も検討が始まっている。また、腕時計に非接触ICカードと同じ機能を持たせたオクトパスウォッチも販売されており、形状を選ばないという、非接触ならではの展開へも進んでいる。

香港に非接触ICカードが定着し成功した理由の1つにはそのロケーションがある。すなわち、周りの国から観光および仕事で毎日人の出入りがあり、カードを利用することである。また、人口以上の循環カードがある理由のもう1つに、1人で複数枚持っている点がある。それは、ほとんどの交通機関で利用でき、またコンビニエンスストアでも利用できることで、むしろ忘れた場合は不便であるために複数枚購入するのである。もちろん、不要なカードはあとで払い戻しが可能である。

中国のシンセンは香港の隣の都市である関係から、早い時期から香港の状況をよく観察しており、2000年末より、バスとタクシーで非接触ICカードが使われ始めた。香港とシンセンは鉄道で繋がれており、ま

た香港とシンセンの間は相互に大勢の人が行き来しているため、将来は香港のオクトパスカードとの相互乗り入れを視野に入れた運用が考えられている。今後は地下鉄、鉄道への展開も検討されており、急速に拡大していく模様だ。

シンガポールは、香港で非接触ICカード化の検討が始まったのとほぼ同時期の1993年頃から検討を開始したが、時間をかけて慎重な検討が進められた。1999年の4月に、ソニーが非接触ICカード500万枚とリーダ約22,000台を受注し、2000年の2月から7月にかけて、地下鉄の一部の路線を使ったパイロットテストが行われた。その間、約880万トランザクションのデータが集められ、結果は大変順調な滑り出しだった。このパイロットテストをふまえて、シンガポールは、香港でステップバイステップで進められてきた発展の過程を、2002年のはじめの本格運用開始時期から一気に始めることとなっている。具体的には、地下鉄、バス、タクシー、自動販売機、公衆電話等、学生IDカード、ホテルルームキー等は導入開始時期から一斉に始まる。また、シンガポールではすでに接触式ICカードを使った電子マネー（CashCard）が自動車の通行料金徴収用として使われているが、自動車のような振動や排ガス埃といった悪環境下では非接触ICカードの方が適していることから、この分野での置き換えも検討され始めている。この電子マネーは、一般のショッピングでも使われているため、今後はこの電子マネーとの一体型である接触／非接触形デュアルインタフェースICカードの発行も計画されている。おそらく、半年後には香港と肩を並べるくらいの非接触ICカードの利用都市になっているのではないかと推測される。

日本ではJR東日本が首都圏100km圏内の約450駅で非接触ICカードを電子乗車券（Suica）として本格運用を開始している。

2000年の6月に競走入札が行われ、定期券450万枚、イオカード200万枚、リーダ／ライタ9,100台、携帯表示器12,000個をソニーが受注した。2001年の4月から7月までの3カ月間、埼京線で1万人規模のモニタが実施され、その後2001年の11月18日から本格運用が開始された。JR東日本では、香港やシンガポールでは見られなかったカード表面の印刷を定期券として書きかえる技術や、定期券とイオカードをドッキングしたカードで、改札機での高速な乗り越し精算の実現など、今までにはなかった新しいサービスが開始されている。現在の首都圏の鉄道は、複数事業者間での相互乗り入れや、相互接続が行われている。JR東日本以外の鉄道でも同様のサービスが始まれば、香港やシンガポールのように、1枚のICカードが、す

べての交通機関に使える理想の環境に近づいてくると思われる。

電子マネー他の応用例 —

“FeliCa”は、交通用途向けの要求仕様を満たす非接触ICカードとして開発されてきたものであるが、実際には、小額決済用の電子マネーとしての使い方を前提としているので、金融用途向けのセキュリティの考え方を最初から取り入れて開発している。その結果、香港で実現されたような汎用電子マネーとしても十分なセキュリティを持った使い方が可能となっている。日本でも、このような特長を持つ“FeliCa”を使ったプリペイド型汎用電子マネーとしてビットワレット（株）により運用されている“Edy”がある。2001年の11月から本格的な実用運用を開始している。また、“FeliCa”を使ったクレジットカードとしてソニーファイナンス（株）の“eLIO”カードが発表されている。現在、非接触ICカードとしては、はじめてのクレジットカードである。そして、家庭用のパソコンにソニーの開発した非接触ICカード用のリーダをつなぐことで、インターネット上でのショッピングや、バンキングができるのである。すなわち、実店舗を持ったリアルワールドと、仮想店舗のサイバーワールドの両方で簡単に利用できる利便性こそが、現金社会を徐々に電子マネー社会へ変えていくのではないかと期待している。その上で“FeliCa”の持つマルチアプリケーションを利用することでIDによるアクセスコントロールやコンピュータのログインコントロールなどを組み合わせると、1枚のカードでリアルワールドとサイバーワールドをセキュアに利用できるようになるのである。

今後の展開 —

今後はさらに、携帯電話等への内蔵も考えている。携帯電話の場合は、直接インターネットへの接続が可能となることから、よりいっそう便利になっていくものと思われる。すなわち、“FeliCa”を内蔵した携帯電話は今まで述べてきたあらゆるアプリケーションが利用可能になるため「電子財布」となることができる。また、形状を選ばないという非接触ならではの特長とさらにカードとリーダ間の通信はもとより、カード同士あるいはリーダ同士の相互通信が可能な“FeliCa”の特長を活かして、あらゆる機器に内蔵することで機器間通信の応用が今後さらに期待される。

（平成14年1月16日受付）