❷非接触 IC カード技術の実装例と特徴

1. 非接触 IC カード技術 FeliCa

松尾 隆史　ソニー（株）FeliCa 事業部 グローバル標準化渉外部

交通系・金融系など民需サービスで多く使われている FeliCa 技術に関して説明を行う．基本的な技術スタックの説明に加え，合成鍵を用いた高速認証技術等の FeliCa に特徴的な技術を解説する．また，Type A 規格との融合である NFC (Near Field Communication) や，マルチサービス利用技術等の最新動向も必要に応じて取り込む．以降でサービス例について触れるため，ここでは技術に関する記述を中心とする．

はじめに

現在，さまざまなカードが発行され日常生活で身近に利用されている．これらのカードの多くは磁気カードであるが，最近は IC チップが埋め込まれた IC カードが広く利用されてきている．これは「記憶容量が大きい」「セキュリティが高い」「高い処理能力を備えている」等の IC カードの利点によるものである．

非接触 IC カードは従来の磁気カードや接触 IC カードとは異なり，カードをリーダ／ライタに挿入することなく「かざす」だけでカードの中の情報を送受信できる IC カードである．IC カードとしての特徴を持ちながら，接触 IC カードと比較して

- かばんや財布に入れたままでも通信が可能なため，操作性が向上する
- 接触部がなくカード券面すべてに印刷をすることが可能であり，デザインの自由度が高い
- 形状がカード型だけに制限されることなく，IC カード機能をキーホルダーや時計などに組み込むこともできる
- リーダ／ライタとの通信時における接触不良や静電気による IC チップの破壊の危険性が少ない
- カードの接点や読取装置のヘッドの磨耗がなく，清掃・定期点検などのメンテナンスが軽減される

などの利点があり，交通機関などを中心に採用が進んでいる．

ソニーが開発した技術方式は“FeliCa（フェリカ）”と名付けられており，電子乗車券や電子マネーなど多様な分野で幅広く利用されている．

FeliCa は，高速なデータ転送速度を安定して実現する FeliCa 無線通信インタフェースと，非接触 IC カード用アプリケーションに適した FeliCaOS の採用により，特に処理速度に関して高いパフォーマンスを実現している．一般的な処理であれば，1 回のトランザクションは 0.1 秒程度で処理が完了する．これは非接触インタフェースの特徴である「かざす」ユーザインタフェースを活かすために非常に重要な要素であると考えている．

“FeliCa 無線通信インタフェース ” と ”FeliCaOS”

FeliCa は，非接触 IC カードとして特に交通用途などで要求される高速処理と高い信頼性を共存させることを可能とし，さらに金融用途での使用にも耐え得るセキュリティの高さも持ち合わせた技術である．**表 -1** に FeliCa 開発導入の経緯を示す．

FeliCa の非接触 IC カードは，大きく分けて「FeliCa 無線通信インタフェース」と「FeliCaOS」との 2 つの技術要素で構成されている．FeliCa 無線通信インタフェースは無線通信制御機能を指し，FeliCaOS はコマンド処理機能

1988	宅配便の物流用タグとして開発をスタート
1989	鉄道総合技術研究所と 1 年間の電子乗車券共同研究
1997	香港オクトパスカード サービス開始（FeliCa として初めての採用）
2001	ビットワレット電子マネー Edy 本格稼働開始
	JR 東日本 Suica サービス開始
2002	ソニーファインナンス オンラインクレジット eLIO サービス開始
	シンガポール ez-link サービス開始
2003	JR 西日本 ICOCA サービス開始
2004	NTT ドコモ おサイフケータイ発売
	スルッと KANSAI PiTaPa サービス開始
	三菱東京 UFJ 銀行 スーパー IC カード（デュアル・インタフェース カード採用）
2005	KDDI おサイフケータイ発売
	ソフトバンクモバイル（旧ボーダフォン）おサイフケータイ発売
2007	PASMO と Suica の相互利用開始

●表 -1　FeliCa 開発導入の経緯

やファイル管理機能を指す．非接触 IC カードとしての処理は，FeliCa 無線通信インタフェース経由でリーダ／ライタから受信したコマンドを FeliCaOS 内でセキュアに処理し，さらに FeliCa 無線通信インタフェース経由で結果をレスポンスとしてリーダ／ライタに返す，ということになる．

FeliCa 無線通信インタフェース

FeliCa 無線通信インタフェースでは，FeliCaOS およびリーダ／ライタ側で生成されたコマンドデータ・レスポンスデータを符号化して送受信を行っているが，その際にはシリアル通信などで通常利用される符号化方式とは異なり，Manchester 符号化方式および ASK10% 変調方式を利用して無線通信が行われる．

●符号化方式

FeliCa では Manchester 符号化方式を採用している．Manchester 符号化方式は Ethernet などでも利用されている方式で，電圧レベルの変化を利用して符号化を行う方式である．たとえばビット区間の中央で電圧レベルを「低」から「高」へ変化させることで「0」を表現し，逆に電圧レベルを「高」から「低」へ変化させることで「1」を表現する．

特徴としては，

- 電圧レベルが変動しても必ず 1 ビット内に高低変化があるのでビットを検出しやすい
- 誤り検出能力がある（フルビットで変化がなければ誤り）
- 受信側デバイスは，受け取ったデータ・ストリームから伝送クロックを復元できる（セルフ・クロッキング方式）

が挙げられる．ただし，各ビット区間を 2 つに分割して情報を伝送するため，変調速度は伝送速度の 2 倍必要ということになる．FeliCa では，

- 非接触 IC カード利用時の特徴である「通信距離の変動による電圧の変化」に対して耐性が高い（ビットの検知がしやすい）

という理由により，Manchester 符号化方式を採用している．

●変調方式

搬送波の振幅の変化を利用する変調方式が ASK 変調方式で，振幅の大小と入力信号を対応させることによりディジタルデータの送受信が可能となる．

ASK 変調方式は，構成がシンプルになるというメリットがある反面，ノイズに弱いという欠点もある．ただし，非接触 IC カードでは，「通信時間が非常に短い」「通信距離が比較的短いためノイズの入る要因が少ない」という理由により ASK 変調方式が一般に利用されている．

FeliCa では特に振幅の 10 % 程度を変化させる「ASK10%」という方式でディジタルデータの無線通信を可能としている．

FeliCa で ASK10%を採用した理由としては，

- 電磁波の送出が途切れないため，安定した電源が作りやすく比較的電力の大きい CPU も駆動させることができる
- 副送波を抑えることができるため，電波法の範囲内で，比較的長距離（10 数 cm 程度）の通信距離を確保することが可能

という点が挙げられる．

FeliCaOS

FeliCaOS は非接触 IC カードのために独自に開発された OS であり，以下のような特徴を持っている．

- ファイル管理
- トランザクション時のセキュリティ
- マルチアプリケーションとトランザクション異常時のリカバリ

●ファイル管理

FeliCa のファイル構造では，2 種類のファイルが存在する．1 つは，カード内データの階層構造を可能とするエリアファイルと具体的なデータファイルを意味するサービスファイルである．

エリアファイルは，通常のパソコンなどで利用しているディレクトリ（もしくはフォルダ）と似た概念である．各エリアファイル内には複数のサービスファイルを置くことが可能である．下位階層にさらにエリアファイルを定義することもできる．

サービスファイルは，データ本体をカードに蓄積するために利用する．FeliCa のメモリは，16 バイト単位のブロックとして区切られており，各々のサービスファイルは，複数個のブロックにより構成される．

サービスファイルには大きく分けて 3 つの種類が存在する．サービス提供者は、これらのファイル種別を組み合わせ，自分の提供するアプリケーションに応じて柔軟にサービスファイルの構成を選択することができる．

(1)ランダムアクセスファイル

最も一般的なファイルで，データをそのままのフォーマットで指定した場所に蓄積し読み書きできる．

(2)サイクリックアクセスファイル

新しいデータを 1 つ追加すると最も古いデータが 1 つ消える仕組みを持つ．最新のログを保存する場合に使用する．

(3)パースアクセスファイル

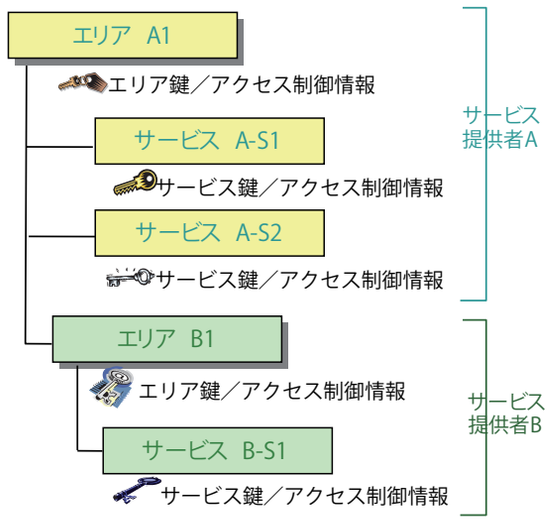
すでにある数字（お金情報など）から減算する機能を持つ．また，1 度減算した数字を再度加算する機能などもある．

●トランザクション時のセキュリティ

各エリアファイルおよびサービスファイルには，それぞれエリア鍵もしくはサービス鍵といったセキュリティ鍵が設定され，セキュリティ鍵が分からないとサービスファイルにアクセスしたり，サービスファイルを追加したりすることができないような仕組みを持つ．エリアファイルおよびサービスファイルにはそれぞれ「読み出し書き込み両用／読み出しのみ」と「セキュリティ鍵なし／あり」といったアクセス制御情報を設定することができる．これにより，各ファイルのアクセス権限を細かく設定することができる．**図 -1** に，FeliCa のファイル構成の例を示す．

また，1 つのサービスファイルに対して複数のアクセス権限の異なる属性を付けることが可能である．たとえば，あるサービスファイルに対して，

- セキュリティ鍵ありでアクセスすれば，読み出し・書き込みともに可能



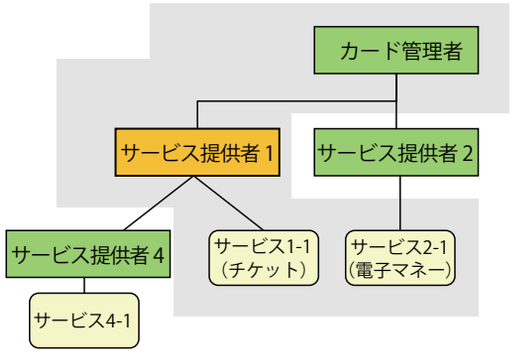
●図 -1　FeliCa ファイル構造例

- セキュリティ鍵なしでアクセスする場合には，読み出しのみ可能

という 2 つのアクセス制御情報を設定することにより，セキュリティ鍵を管理している人のみがサービスファイルに書き込むことができ，その他の人はデータを参照することだけができるサービスファイルを作成できる．

また，FeliCa では，セキュアなトランザクション時にはカードとリーダ／ライタとの間で FeliCa オリジナルの認証方式を利用して相互認証を行う．その際には，複数ファイルアクセス時に複数の鍵から 1 つの「合成鍵」を生成し，合成鍵を用いた相互認証で一括して該当ファイルのアクセスを許可することで，複数ファイルを同時にアクセスする際のトランザクション時間を，セキュリティレベルを落とすことなく大幅に削減している．認証後もトランザクションごとに動的に生成する暗号化鍵でデータを暗号化して送受信することで高いデータ秘匿性を確保している．

たとえば図 -1 でのカード内データ構成の場合，サービス提供者 A がサービスファイル A-S1 とサービスファイル A-S2 をアクセスする場合，セキュリティ鍵は「A1 エリア」「サービスファイル A-S1」「サービスファイル A-S2」に別々に設定されているために，通常は，それぞれのエリア・サービスについて相互認証（鍵がお互い正しいかを確認する処理）を行わなければならない．一般的に相互認証はやりとりの回数が多いために通信時間も含めた処理時間がかかり，3 つのエリア・サービスそれぞれに対して相互認証を行った場合には，高速な処理を望むことができない．そこで FeliCa では，複数のセキュリティ鍵を 1 つのセキュリティ鍵に合成し，この合成鍵を利用して相互認証を 1 度だけとすることで，処



●図 -2　FeliCa の複数サービス同時アクセス機能

理を高速化している．このセキュリティ鍵の合成によりアクセスするファイル数が増えた場合にも高速な処理が実現される．

●マルチアプリケーションとトランザクション異常時のリカバリ

接触 IC カードなどでは，複数のファイルに対してアクセスする場合，

（1）まず，最初のファイルをオープンしデータの読み書きを行いクローズする

（2）その後，次のファイルをオープンしデータの読み書きを行いクローズする

といった作業を行う．

非接触 IC カードにおいては，カード利用者がカードをデータ書き込み処理が正しく完了する前にリーダ／ライタから離してしまうケースが考えられる．この場合，カードがリーダ／ライタから離れ電力が途切れてしまうため，トランザクションの最後まで処理が完了する前に通信ができなくなってしまい，データの整合性が確保できなくなってしまう可能性がある．これを避けるために，FeliCa では 1 度の相互認証で同時に複数のファイルに対して認証を行いファイルをオープンすることで，複数のサービスファイルを 1 回のコマンドで同時に読み書きすることを可能としている．

また，このとき，書き込み処理の途中でどれか 1 つでもアクセスに失敗した場合にはすべての処理が元に戻るという「アンチブロークン・トランザクション」機能を実現している．これにより，たとえば**図 -2** で示すように電子マネーサービスと電子チケットサービスとに同時にアクセスする場合，電子チケット情報を書き込み，その後電子マネーの金額データを引き落とす前にカードを離されてしまうと通常はサービス提供者がビジネス上の被害を被ることになるが，FeliCa の複数サービス同時アクセス機能を利用することにより，安心して IC カードアプリケーションビジネスを展開することができるようになる．

NFC（Near Field Communication）

NFC は，非接触 IC カード技術を応用して，ソニー（株）とフィリップス（現 NXP セミコンダクターズ）が主体となって開発した新しい近距離無線通信規格である．

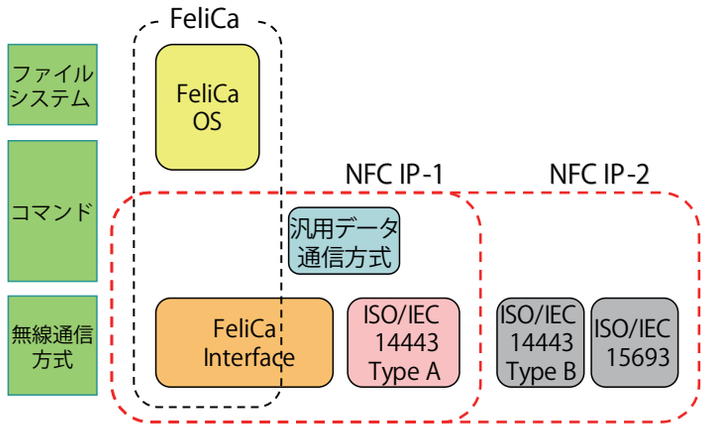
NFC は，以下のような特徴を持つ．

- 非接触 IC カードと同じ 13.56MHz の電波を用いる近距離無線通信規格であり，物理層とデータリンク層から構成されている．この NFC チップが搭載された機器を 10cm 程度の距離に近づけることで，相互に認識し合い情報交換を行う．
- FeliCa 技術および ISO/IEC 14443 TypeA 技術の無線通信技術を含むことで，両者と通信互換性を有している．
- 加えて，近距離無線における汎用的なデータ通信方式としても利用可能である．
- 通信距離は，FeliCa と同じく 10cm 程度を想定し，通信速度は最初の NFC 規格（NFCIP-1）として 106, 212, 424kbps をサポートする．
- FeliCa 対応リーダ／ライタが IC カードに対して常時磁界を生成する必要があるのに対し，電力が供給される端末同士が通信する場合には，データ送信時のみ磁界を生成し送信完了と同時に磁界生成を停止させる「Active Mode 通信」技術が追加された．これにより NFC 技術搭載端末の低消費電力が実現される．

NFC 技術は主として，NFC 技術を利用したチップが CE（Consumer Electronics）機器やモバイル端末などに搭載されることを想定しており，NFC チップを搭載したモバイル端末は，以下のような機能を持つことが可能となる．

- 複数の機器間で，データの無線通信が可能となる．
- FeliCa の非接触 IC カード，および ISO/IEC 14443 TypeA の非接触 IC カードのリーダ／ライタ機能を持つことが可能となる．
- FeliCaOS などのセキュア部分を同時に利用することで，モバイル端末自体が非接触 IC カードと同等の機能を持つことが可能となる．

図 -3 に NFC の技術構成を示す．この技術は，2002 年 12 月に，情報通信システムの標準化機関である ECMA International にて ECMA-340 として登録された．その後 2003 年 12 月に ISO/IEC JTC 1 へ提案され，各国での審議と投票を経て国際標準規格 ISO/IEC 18092 として承認された．また，ノキア，フィリップス，ソニーの 3 社は，2004 年 3 月に，NFC フォーラムを設立するこ



●図 -3　NFC の技術構成

とを発表し，2005 年 3 月に正式に発足した．現在では全世界で 100 以上の会社や団体が加盟している．ノキアやモトローラ，サムソンといった携帯電話メーカ，および VISA や MasterCard といったクレジット事業者，TI やルネサスといった半導体事業者など，多岐に渡る会社が NFC フォーラムに参加し，NFC 技術の推進活動を行っている．

NFC フォーラムは，民生用機器やパソコン，自動車，その他の産業などにおける製品に対して NFC 技術を適用する際の互換性の確保を主軸とし，前述したアプリケーションレベルのプロトコルをはじめ，データをやりとりするためのミドルウェアレベルのプロトコルやデータフォーマットなどを規定し，さまざまな企業・団体とともにオープンな規格として，NFC 技術方式の普及に注力することを目標としている．

今後の展開

「簡単な操作で利用可能」かつ「高いセキュリティを確保可能」な非接触 IC カードは，公共交通機関はもとよりさまざまな分野でよりよいユーザインタフェースを提供する手段として今後ますます利用されていくと考えている．ソニーはこの非接触 IC カード技術方式である FeliCa を，カードのほかにもさまざまな CE 機器やモバイル機器に搭載していくことで，より利便性の高く，かつ安心して利用できるような環境を構築していく予定である．

海外においても，アメリカやヨーロッパなどでの非接触 IC カード技術を利用したクレジットカード市場の立ち上がりとともに，NFC 技術を利用する携帯電話がノキアなどの大手携帯電話メーカから提供され，日本における「おサイフケータイ」のような機能を持つ携帯電話が急速に世界的に増加していくと考えられる．これにより，並行して携帯電話と非接触通信を行うパソコンや TV なども今後増加してくることが予想され，世界的に NFC や FeliCa といった非接触通信技術の一般化が期待される．

参考文献

1）Kurokawa, A. : CONTACTLESS IC CARD TECHNOLOGY “FeliCa” AND NEW APPROACH, International Symposium on Speed-up and Service Technology for Railway and Maglev Systems 2003（STECH’ 03）.

（平成 19 年 5 月 7 日受付）

松尾 隆史

ソニー（株）FeliCa 事業部．1992 年，慶應義塾大学・理工学部・管理工学科卒業．2001 年ソニー（株）入社．現在に至る．専門分野は非接触 IC カード技術とその応用に関する開発・標準化など．