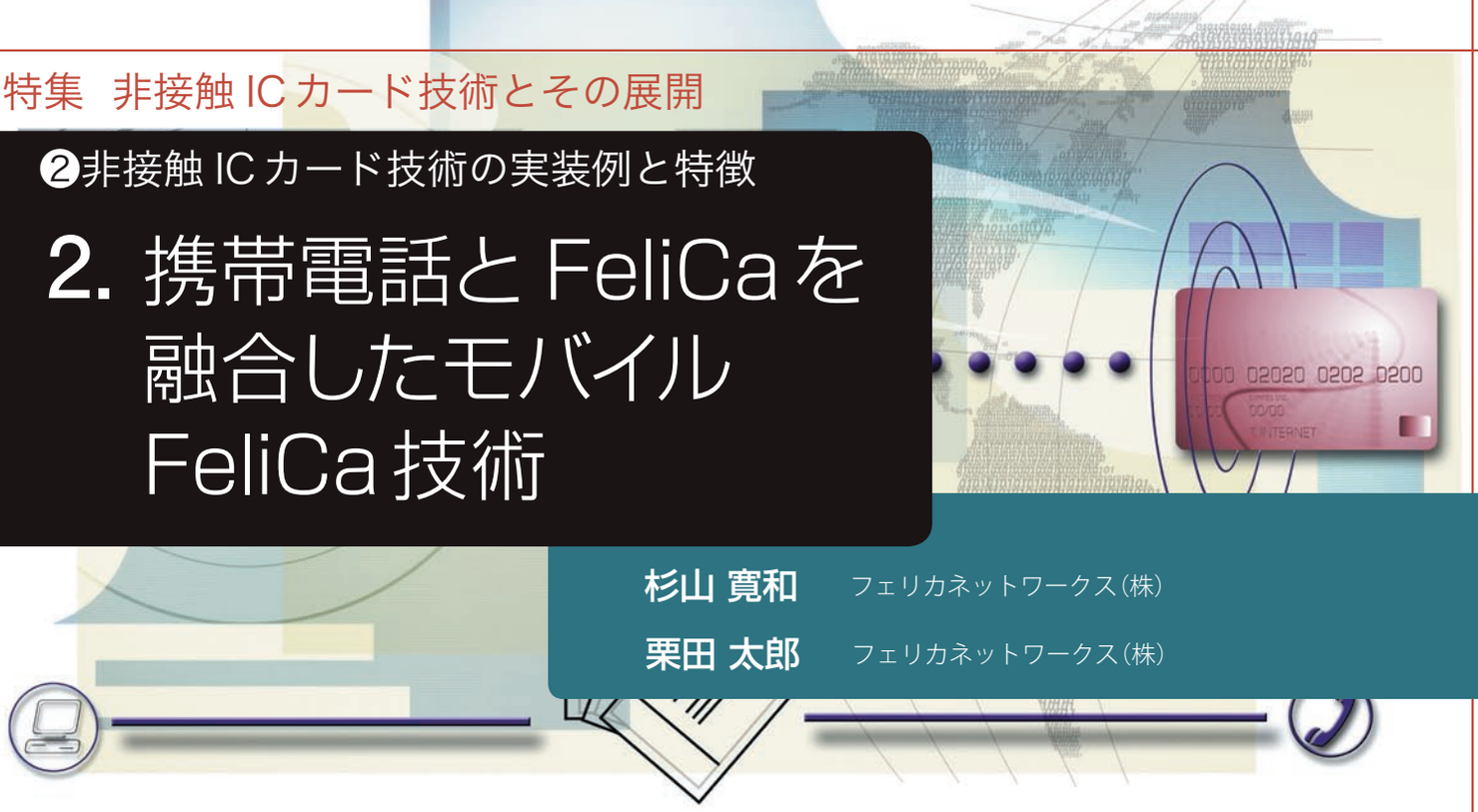
❷非接触 IC カード技術の実装例と特徴

2. 携帯電話と FeliCa を融合したモバイル FeliCa 技術



杉山 寛和　フェリカネットワークス(株)
栗田 太郎　フェリカネットワークス(株)

「FeliCa」はソニー（株）が開発・推進する非接触 IC カード技術の総称です．「モバイル FeliCa」は従来の FeliCa IC カード技術を発展させ，携帯電話に「モバイル FeliCa IC チップ」を搭載することにより実現した，携帯電話を通してサイバー（ネットワーク上の世界）とリアル（現実の世界）をつなぐ，システムとマルチアプリケーションサービスです．携帯電話と非接触 IC カードとの融合を果たした「モバイル FeliCa」には，従来の非接触 IC カードにはない特徴があります．本稿では「モバイル FeliCa」システムを実現する上で利用されている技術について概説します．

はじめに

FeliCa はソニー（株）が開発・推進する非接触 IC カード技術の総称です．電子マネーや公共交通機関の乗車券・定期券・搭乗券などの幅広い用途で，FeliCa の語源である「felicity（至福）」の言葉通り，日常生活をより楽しく便利にするために利用されています．

モバイル FeliCa は，従来の FeliCa IC カード（以下，FeliCa カード）技術を発展させ，携帯電話にモバイル FeliCa IC チップを搭載することにより実現した，携帯電話を通してサイバー（ネットワーク上の世界）とリアル（現実の世界）をつなぐ，システムとマルチアプリケーションサービスです．フェリカネットワークス(株)は，このモバイル FeliCa 技術をチップメーカ，携帯電話メーカ，サービス事業者，通信事業者など幅広い事業者に提供し，モバイル FeliCa の普及に努めています．2004 年 7 月に（株）エヌ・ティ・ティ・ドコモより「おサイフケータイ」としてサービスが開始されて以来，各移動体通信業者と携帯電話メーカから，3,000 万台を超える「モバイル FeliCa IC チップ」搭載携帯電話端末が販売されました(2007 年 3 月末時点)．

携帯電話と非接触 IC カードとの融合を果たした「モバイル FeliCa」には，従来の非接触 IC カードにはない特徴があります．本稿ではモバイル FeliCa を実現する上で利用されている技術について概説します．

FeliCa の特徴

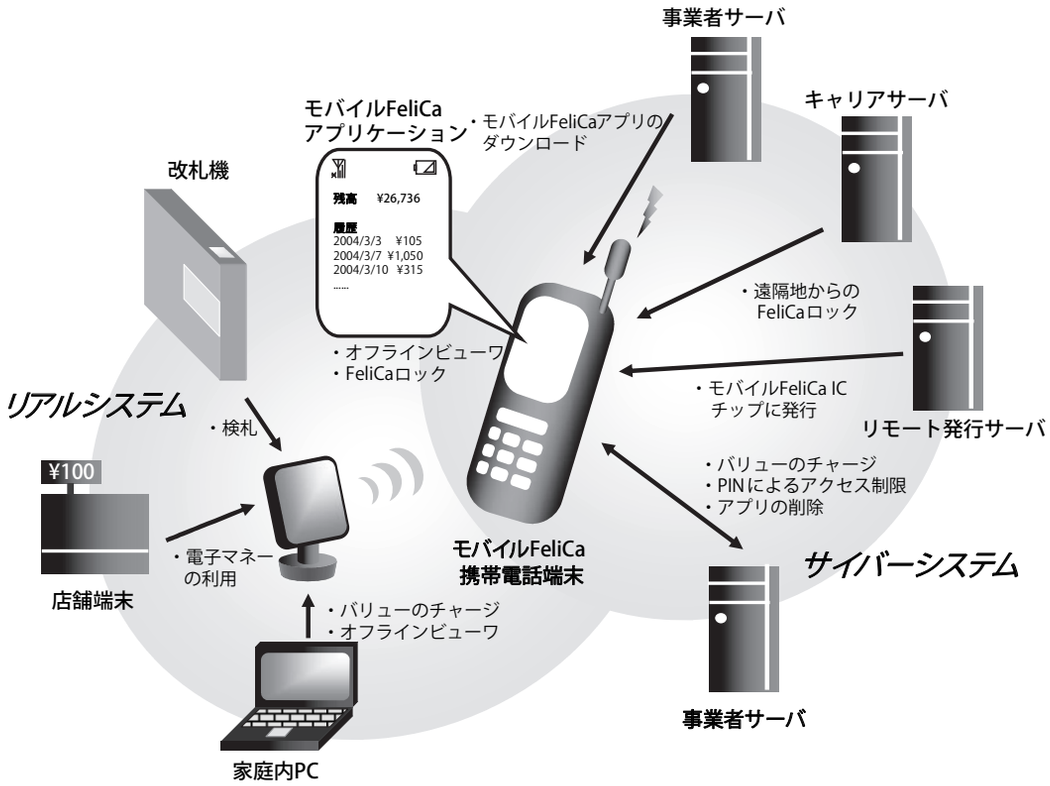
FeliCa は東日本旅客鉄道(株)の「Suica」やビットワレット（株）の「Edy」に採用されて以来，幅広い場面で利用されています．FeliCa 非接触 IC カードの，13.56MHz の搬送周波数を利用した近接型「FeliCa 無線通信インタフェース」と，非接触 IC カードに最適化された「FeliCa OS」により，高機能かつ高セキュリティなサービスが実現できます．FeliCa OS には次の 4 つの技術的特徴があります．

●マルチアプリケーション

1 枚の FeliCa カードには事業者の異なる複数のアプリケーションを登録することが可能です．さらに複数のアプリケーションを同時に利用することが可能なため，異なる事業者間でサービスの連携を行うことができます．

●ファイルシステム

FeliCa では，一般的なファイルシステムのディレクトリに相当する「エリア」と，ファイルに相当する「サービス」の階層構造でデータが管理されます．エリアやサービスには個別に鍵やアクセス権を設定することが可能です．また，トランザクション処理中に電源が断絶してもデータの整合性を確保する，アンチブロークントランザクションアルゴリズムが搭載されています．



●図 -1　モバイル FeliCa

●セキュリティ

FeliCa カードと上位との通信はトリプル DES 暗号アルゴリズムを応用し，「相互認証」と，以降の電文データを暗号化することによって機密化されています．各トランザクションのセキュリティを確保するために，乱数から生成された鍵を用いて相互認証を行います．こうして，非接触 IC カードとしては世界初の ISO/IEC 15408 EAL4 のセキュリティレベルを実現しています．

●処理速度

「FeliCa 通信プロトコル」では，1 回の通信で複数のサービスに対して同時に相互認証やデータの読み書きが行えるため，通信回数を効率化することが可能です．この仕組みを含め，処理速度を高速化することにより，混雑時における鉄道改札口のような高速処理速度が要求される条件下での FeliCa の利用が可能となりました．

モバイル FeliCa の特徴

「モバイル FeliCa」は携帯電話に「モバイル FeliCa IC チップ」を搭載し，FeliCa 無線インタフェースに接続する「リアルシステム」と，携帯電話網を経由しインターネットに接続する「サイバーシステム」の 2 つの系をつなぐことで，新たな価値創造を目指して開発されました（図 -1）．

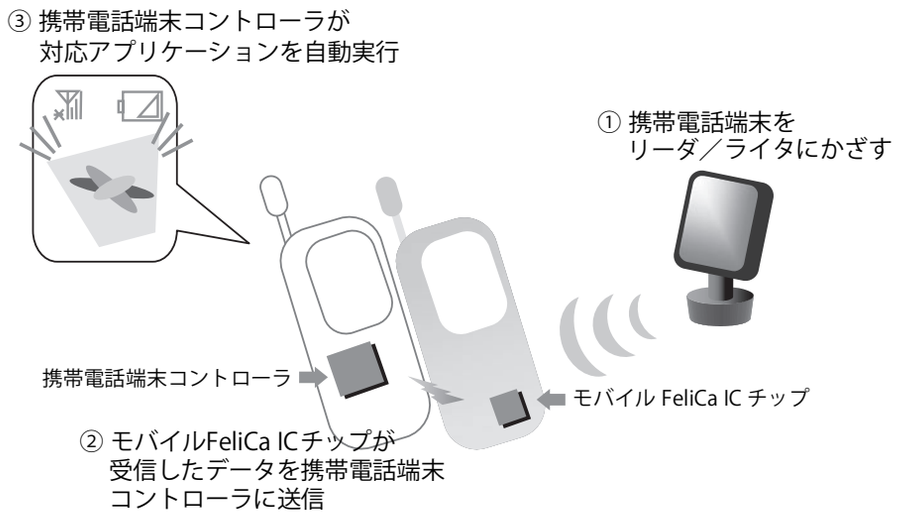
モバイル FeliCa には，従来の FeliCa カードに加え，以下の特徴があります．（1）リモート発行，（2）オフラインビューア，（3）三者間通信，（4）PIN によるアクセス制限，（5）エリア・サービスの削除，（6）FeliCa ロックなどです．ここでは，この 6 つの機能について説明します．

●リモート発行

サイバーシステムに接続することにより，ユーザが携帯電話端末上のアプリケーションから携帯電話網を経由して「リモート発行サーバ」に対して発行処理を要求し，モバイル FeliCa IC チップに対してサービスやエリアを登録する「リモート発行」が行えます．これにより携帯電話端末上から FeliCa に対応した新規アプリケーション用の IC カード情報の発行や，電子マネーやポイントなどのバリューのチャージが可能となります．これにより，たとえば，従来は郵送で申し込んでいた新規カードの発行手続きを，携帯電話から行えるようになりました．

●オフラインビューア

携帯電話端末上のアプリケーションから FeliCa IC チップのサービスにアクセスすることが可能になりました．これにより携帯電話端末から IC チップ内の情報が閲覧



●図 -2　三者間通信の仕組み

できます．たとえば，モバイル FeliCa アプリケーションから認証不要サービスへアクセスすることにより，電子マネーの残高確認や利用履歴の表示などが行えます．

●三者間通信

リアルシステムから送信された通信パケットが，モバイル FeliCa IC チップを介して携帯電話端末上のアプリケーションに送信されること，またはその逆を「三者間通信」と呼びます（図 -2）．これにより携帯電話端末をリーダ／ライタにかざすだけで，携帯電話端末上のアプリケーションをダイレクトに起動することが可能になりました．

この機能により，携帯電話端末をリーダ／ライタにかざすことでクーポンや店舗案内などの情報を携帯電話端末に送信することができます．三者間通信を利用したサービスとして，（株）エヌ・ティ・ティ・ドコモの「トルカ」やフェリカネットワークス（株）の「かざポン」などがあります．

● PIN によるアクセス制限

モバイル FeliCa IC チップには，サービスへのアクセスを制限するための機能として，任意のサービスに対してパスワード認証の機能を持たせることが可能です．このパスワードは「PIN（Personal Identification Number）」と呼ばれます．

●エリア・サービスの削除

リモート発行によりユーザが自由にアプリケーションの発行や削除を行えるようにするため，モバイル FeliCa 上の使わなくなったエリアやサービスを削除する機能が新たに追加されました．

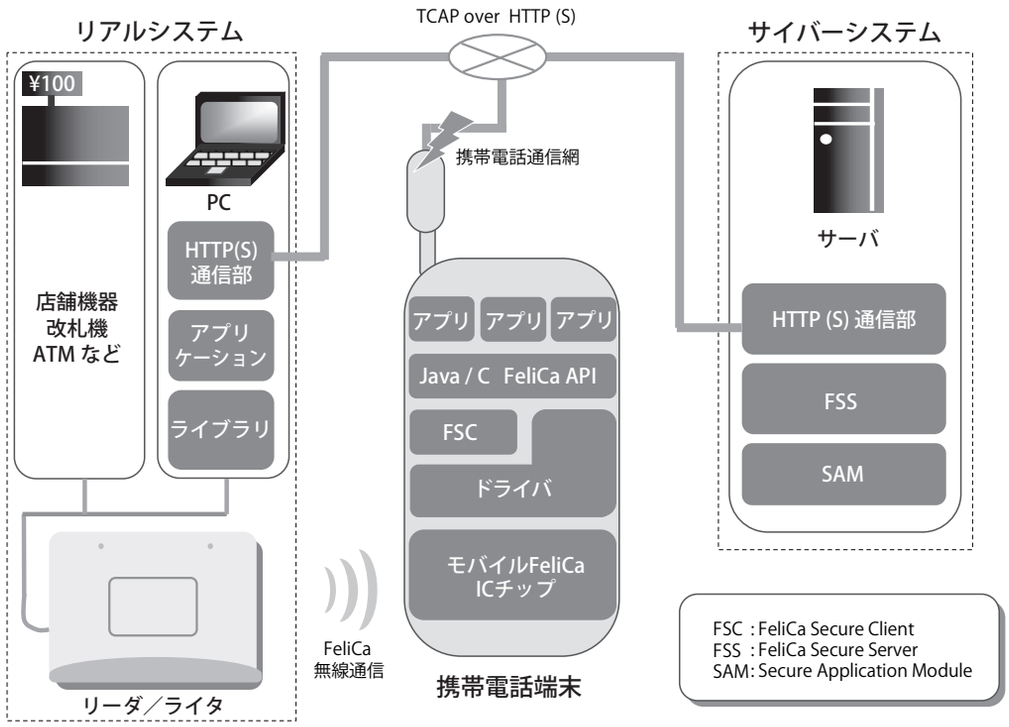
● FeliCa ロック

モバイル FeliCa IC チップへのアクセスを遮断する携帯電話端末の機能です．また，移動体通信業者により遠隔地から携帯電話回線を経由して FeliCa ロックを行うサービスも提供されています．

モバイル FeliCa の仕組み

●モバイル FeliCa システム

モバイル FeliCa のシステムを構成する要素はさまざまです．携帯電話端末に搭載される，FeliCa 技術方式に対応した LSI である「モバイル FeliCa IC チップ」．携帯電話端末に実装されたモバイル FeliCa IC チップへのアクセスを行うクライアントソフトウェア「FeliCa Secure Client（FSC）」．モバイル FeliCa IC チップを用いてユーザにサービスを提供する携帯電話端末アプリケーション「モバイル FeliCa アプリ」．モバイル FeliCa IC チップを使ったアプリケーション開発のために用意された「FeliCa API」．インターネット上で FeliCa サービスを提供する基盤となるサーバサイドアプリケーションフレームワーク「FeliCa Secure Server（FSS）」．サーバサイドの暗号化処理と鍵の管理を行うハードウェアセキュリティモジュール「SAM（Secure Application Module）」．クライアント―サーバ通信プロトコルである「TCAP（Thin Client Application Protocol）」．これらを核にして，さまざまな構成要素が連携することでモバイル FeliCa のシステムが構成されています（図 -3）．



●図 -3　モバイル FeliCa システム構成図

●ファイルシステム

FeliCa の IC チップの不揮発性メモリには，ファイルシステムが記録されています．ここではモバイル FeliCa IC チップのファイルシステムについて説明します．

システム

モバイル FeliCa IC チップのファイルシステムは「システム」と呼ばれる最も大きな論理的構成単位でまとめられます．システムは概念的に 1 枚の IC カードと見なすことができます．モバイル FeliCa IC チップのファイルシステムは複数のシステムに分割が可能です．これにより，1 つのモバイル FeliCa IC チップを複数の IC カードとして機能させることができます．非接触 IC カードに記録されたどのシステムと通信するのかは，モバイル FeliCa IC チップの認識時に決定されます．

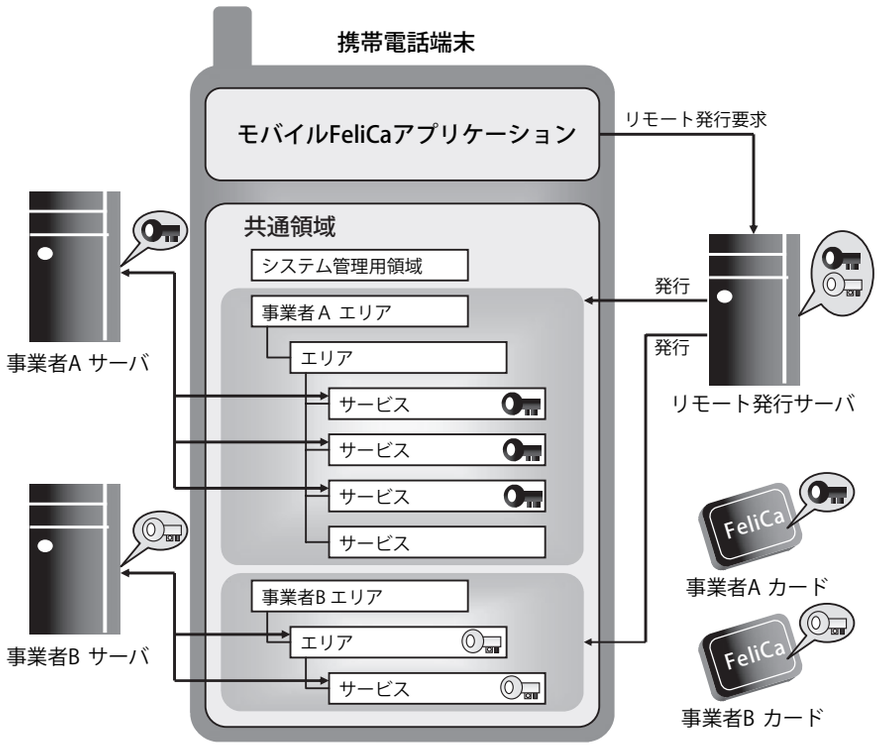
エリア・サービス

システムはエリアとサービスによって構成されます．一般的なファイルシステムに例えると，エリアはディレクトリ，サービスはファイルにあたります．エリアには複数のエリアやサービスを登録することができます．サービスにはデータの実体が記録されます．エリア登録時にエリアには固有の領域が割り当てられ，その領域内でエリアやサービスを登録することができます．これらを登録することにより，モバイル FeliCa IC チップに対してアプリケーション（サービス事業者に割り当てられるエリア群とサービス群）の発行が行われます．

●共通領域

モバイル FeliCa のファイルシステム上には共通領域と呼ばれる領域が確保されています．共通領域には鍵により暗号化されるエリアやサービスの定義情報が登録可能です．エリアに割り当てられる領域は可変です．「おサイフケータイ」としてサービス事業者がモバイル FeliCa を利用する場合には，共通領域にデータを格納するのが一般的です．共通領域に関する情報はフェリカネットワークス（株）が管理することで，FeliCa の整合性が保証されています．これにより，サービス事業者が提供するアプリケーションに対して，FeliCa カードとモバイル FeliCa を同等に利用することが可能になります．

共通領域にエリアやサービスを登録するにはリモート発行を行います（**図 -4**）．携帯電話端末上のモバイル FeliCa アプリケーションからリモート発行サーバに対して処理要求を送信するとリモート発行が開始されます．リモート発行サーバはフェリカネットワークス（株）が管理しており，各事業者のサービス提供に必要なエリアやサービスを，携帯電話通信網を通じて共通領域に登録することを可能にします．リモート発行サーバには各事業者が利用する鍵が管理されており，リモート発行サーバが共通領域に FeliCa カードと同じ鍵や同じ構造のデー



●図 -4　共通領域とリモート発行

タを設定することで，FeliCa カードとの互換性を保証しています．

第 2 世代モバイル FeliCa の新機能

携帯電話と FeliCa 技術の融合による新たな価値創造を目指した第 2 世代モバイル FeliCa の開発を，2006 年内のサービス開始に向けて進めてきました．第 2 世代モバイル FeliCa には，以下の新機能が追加されています．

●リーダ／ライタ機能

第 2 世代モバイル FeliCa IC チップは，外部 FeliCa IC チップ（モバイル FeliCa IC チップを含む）に対して搬送波を出力してコマンドの送受信を行うことができるリーダ／ライタ機能を備えています．

リーダ／ライタ機能には Thru リーダ／ライタ機能と SAM リーダ／ライタ機能があります．Thru リーダ／ライタ機能は，モバイル FeliCa アプリケーション（**図 -5，**①）またはサーバからモバイル FeliCa IC チップを中継して（**図 -5，**②）外部 FeliCa IC チップへのアクセスを可能にする機能です．SAM リーダ／ライタ機能は，モバイル FeliCa IC チップに登録されている鍵または有線コントローラから指定された鍵で相互認証・暗号化された通信により，有線コントローラまたはサーバからモバイル FeliCa IC チップを中継して（**図 -5，**③），外部 FeliCa IC チップへのアクセスを可能にする機能です．

●アドホック通信機能

アドホック通信機能は，リーダ／ライタから送信されたデータを有線側コントローラ，または有線側コントローラからリーダ／ライタに転送する機能です．アドホック通信には「簡易データ転送」と「連続データ転送」の 2 種類があります．簡易データ転送は，従来の三者間通信と互換性を保った方式で通信します．連続データ転送は，第 2 世代モバイル FeliCa より追加された通信方式で，アドホック通信を開始したコントローラが指定する区間内で連続的にデータ転送が可能となります．アドホック通信はリーダ／ライタ，コントローラのどちらからでも開始することができます．アドホック通信を用いますと，携帯電話端末間で電話帳データなどを高速転送することが可能になります．

●データ移行機能

2 つの第 2 世代モバイル FeliCa IC チップ間で FeliCa データの移行が可能になりました．「データ移行」時には専用の相互認証を行い，セキュアなデータ移行を実現しています．これにより，モバイル FeliCa の機能を利用

●図 -5　リーダ／ライタ機能

して，携帯電話端末の機種変更時に電子マネーの残高やポイントなどを含めたファイルシステムを移行することが可能となります．

ますます広がるモバイル FeliCa

国内の携帯電話市場では，携帯電話端末の普及台数が 9,500 万台を超えました（2007 年 2 月末時点）．携帯電話端末はますます高機能になり，携帯電話通信網を利用したサービスはめまぐるしいスピードで多様化し，携帯電話端末は通話端末から情報端末として進化を続けています．すでに各移動体通信業者と携帯電話メーカから，3,000 万台を超える「モバイル FeliCa IC チップ」搭載携帯電話端末が販売され（2007 年 3 月末時点），モバイル FeliCa も携帯電話の情報端末化に大きく貢献しています．

このような流れの中で，携帯電話と FeliCa 技術の融合による新たな価値創造を目指し，2007 年はモバイル FeliCa を使った電子チケットシステムや会員証・ポイントシステムを簡便に導入できる環境を提供するなど，FeliCa の普及に向けたさらなる取り組みを続けています．モバイル FeliCa は日常生活の中に新しい利便性を生み出すことで，新しいライフスタイルの創造に貢献できるよう，日々進化を続けています．

参考文献

1）アスキー書籍編集部，モバイル FeliCa プログラミング，アスキー（2006）．http://www.sony.co.jp/Products/felica/

（平成 19 年 5 月 7 日受付）

杉山 寛和　Hirokazu.Sugiyama@FeliCaNetworks.co.jp

2000 年ソニー（株）に入社し，民生用ディジタル映像機器を開発．2005 年フェリカネットワークス（株）に参画し，第 2 世代モバイル FeliCa IC チップの開発に携わる．現在，次世代 FeliCa の開発に従事．

栗田 太郎　Taro.Kurita@FeliCaNetworks.co.jp

1999 年よりソニー（株）にて各種製品を開発．2004 年よりフェリカネットワークス（株）にてモバイル FeliCa の商用化および第 2 世代の開発に携わる．現在，次世代 FeliCa の開発に従事．