H12-モバイルＥＣ-WG

モバイルＥＣに関わる
決済標準モデルの研究
中間報告書

平成１３年３月

電子商取引推進協議会
モバイルＥＣ-ＷＧ
決済モデル検討ＳＷＧ

目次

図表目次

参　考　資　料

目次

図表目次

メンバリスト

1　決済標準モデルの研究

標準モデル研究にあたり検討すべき対象を以下の**図 1-1** に定義した。

この中で携帯電話本体に関しては次世代携帯電話で導入されるＵＩＭ（Universal Idendtitiy　Module）に加入者の識別情報やそのほかのアプリケーションで利用する情報を記録することができる。加えて決済他のアプリケーションを実現するために自販機やＰＯＳ端末など外部機器（または内部ＩＣチップ）とのローカルワイヤレスインターフェースが実装されることが想定される。

携帯電話上でなくネットワークを経由して決済機能をサーバが管理するペイメントゲートウェイという方式も開発・実用化されている。また、従来のインターネットＥＣとの相互運用性を考慮して場合、認証局を利用した３者間認証を行う方式も対象範囲に含まれる。今年度はこれらのうち IC チップとローカルワイヤレスインターフェースについての調査を行い現時点での中間報告として記載した。

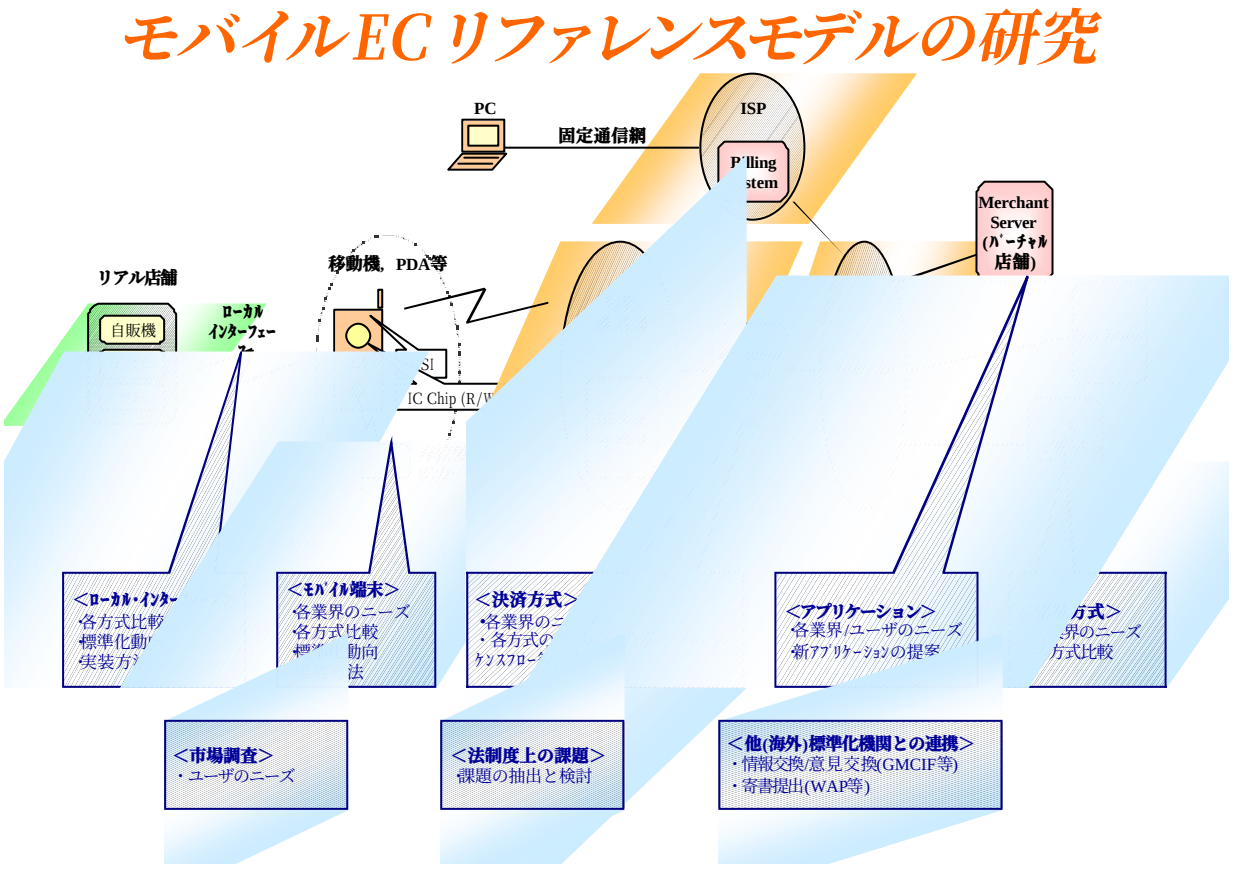


図 1-1 決済標準モデル

2　IC チップに関わる動向

携帯電話を財布代わりに使用するモバイルコマースにおいては、通信事業者が提供する携帯電話サービスと金融系アプリケーションとの連携、及び、携帯端末を中心としたセキュリティの確保が重要となる。この場合には、携帯端末上に IC チップ（耐タンパデバイス）を搭載し、その中で、セキュリティを確保する技術が意味を持つようになってくる。

また、運用面においても、携帯電話サービスと金融系アプリケーションの効率的かつ使い易い連動が重要となる。これに関しても、携帯電話に IC チップが導入されることで、従来型の携帯電話端末の運用に縛られない新たなビジネスモデルが構築できる可能性がある。

そこで、IC チップアドホックでは、今後のモバイルコマース分野における新たなビジネスモデルが創出されて行く上での基盤となると予想される IC チップについての基礎知識としてアドホックメンバー各社より今後の決済モデル検討 SWG での議論の参考になると予想される情報を募集し、その結果を「**参考資料の 1.1 IC チップに関わる動向**」に記述した。

3　ローカルワイヤレスインターフェースに関わる動向

モバイルＥＣ･WGの決済モデル検討ＳWGにて､バーチャル店舗における電子決済だけでなく、コンビニや自動販売機などのリアル店舗における決済の重要性が議論され、これを実現する手段としての「ローカルワイヤレスインタフェース」装備の必要性が指摘された。

モバイル端末に「ローカルワイヤレスインタフェース」を装備して決済を中心とした新しいサービスを実現する際には、どのようなインタフェースを選択利用できるかが重要となる。このためアドホック委員会を設置して、決済モデル検討ＳWGメンバーだけでなく広くWGメンバーの関連の方々に参画いただき､「ローカルワイヤレスインタフェース」の調査検討作業を実施した。具体的な「ローカルワイヤレスインタフェース」として代表的な Bluetooth、IrDA、非接触 IC インタフェースの３つを取り上げて比較検討を行い、その結果をまとめた。比較検討においては、基本技術仕様だけでなく、国際的標準化動向や実装時の消費電力、さらに利用に適した場面や適用の問題点などを含めて、サービス事業者からみても解り易い形をめざした。

3.1　ローカルワイヤレスインタフェース

表 3-1　ローカルワイヤレスインタフェース比較表

評価項目		Bluetooth	IrDA	非接触 IC インタフェース（近接型）
方式概略		Bluetooth は、2.4GHz 帯を使った DFS（スペクトラム拡散方式）の無線通信方式で、機器間のケーブルの代替品として設計され、数年内に大半の携帯電話、ノート PC に搭載されると予測されている。 短距離無線通信の中では比較的長い距離の通信が可能であり、切れにくく、単純で、低消費電力／低コストであることを意図している。また、１対７の同時接続が可能である。 Bluetooth コンソーシアム（全世界 2000 社）の SIG 活動で利用を想定した仕様を作成する。また、機器相互性を保証するロゴ認証制度がある。	IrDA は、赤外線を使ったデータ通信技術の規格であり、既に汎用的なｲﾝﾀｰﾌｪｰｽであり、携帯電話機にも実装実績がある。 光の直進性により、機器の向きを合わせた通信である点と、間に障害物があると通信できなくなる点が特徴である。 IrDA には以下の２つの規格がある。 ・IrDA-Data 規格：１対１ﾃﾞｰﾀ通信向け ・IrDA-Contorol 規格：1 対ｎ機器間通信 携帯電話向けに小型化・低消費電力した IrDA-Data 規格として、IrMC という規格が別途策定されている。IrMC は、IrDA-Data 規格を実装した PC/PDA 等とﾃﾞｰﾀ通信が可能である。 IrDA-Control 規格は、主に家電への実装を目的だが、IrDA-Data 規格との互換性が無く通信も出来ない。以下、IrMC 規格を IrDA として記載する。	非接触 IC インタフェースは電磁誘導結合によってカードへの電力伝送を行うとともに，変調してデータの伝送も行う。IC カードとリーダーライタ間の非接触インタフェースは、交通機関や、公衆電話機の決済カードとしての実績がある。 IC チップは、高セキュリティであり、決済処理に適している。 ISO/IEC14443 には、変調方式の違いにより２種類の Type A と Type B があり、さらにオプションとして日本より Type C が提案され、審議中である。
基本技術仕様	周波数	2.402～2.480GHz の 1MHz を 625μ秒毎に切り替えて使用する周波数ホッピング方式を採用	赤外線（波長 0.76μm～1mm）	13.56MHz
	通信速度	1Mbps　音声 56Kpbs　データ 432.6Kpbs（対称）または 723/56Kbps（非対称） ～１Mbps／Bluetooth1.0 ～２Mbps／Bluetooth2.0（予定）	576kbps/1.152Mbps/4Mbps	通信速度：106kbps (ISO14443 Type A,) 106kbps、×2、×4、×8 (Type B) 212kbps、×2、×4 (Type C)
	同時接続性	全体で８台までの同時通信が可能（ただし１台はマスターで残り最大７台までのスレーブ間通信を中継する）	１対１（通信角度 ±15 度）	１対３程度
	通信可能距離	Class１　最大 100mW（20dBm）　通常 N/A 最小 1mW（0dBm） Class２　最大 2.5mW（4dBm）　通常 1mW（0dBm） 最小 0.25mW（-6dBm） Class３　最大 1mW（0dBm）　通常 N/A　最小 N/A 一般に 1mW（0dBm）で 10m、100mW（20dBm）で 100ｍが到達範囲と言われている。	標準：通信距離 0～1m　省電力 Option：20 ㎝	約 10cm（リーダライタの消費電力が 1W の場合） 携帯電話機に搭載するばあいには、消費電力の面から通信可能距離に制約を受ける。
	セッション確立時間	約 10 秒（推奨値）	約１～２秒	約 5ms
ノイズ・干渉 移動機に実装した場合）		【基板・電波による干渉】 現在 Bluetooth SIG で検証中 短時間に周波数を変更する周波数ホッピング方式のため妨害電波には強いと言われている。	【基板・電波による干渉】 ・基板実装は実績があり、特に問題は発生していない。 ・日光等による干渉の可能性あり。	【基板・電波による干渉】 ・干渉を避けるためには携帯電話機内にシールドが必要であるが、その場合通信可能距離が犠牲になることがある。
実装時の消費電力		待機時１mW で携帯電話への搭載可能	標準：100mW/sr　省電力 Option：9.0mW/sr	Type A, Type B　：不明 TypeC（FeliCa 技術方式）：カード動作時 5mw 以下、 リーダーライタとして動作時 約 160mw、待機時 2μw 以下

セキュリティ	基本的な暗号化（共通鍵方式/DES）は実施。 ※現行のセキュリティとしては一般的な無線部分の暗号化と特定の ID 入力による接続相手の識別機能がある。	上位ＡＰで対応が可能	・物理層・トランスポート層でセキュリティ機能に該当する機能はなく各アプリケーションにてセキュリティ機能を提供する。 ・セキュリティ機能が１チップ内に組込まれているため、耐タンパー性が高い。 ・Type A, Type B ：上位ＡＰで対応が可能 ・TypeC（FeliCa 技術方式）では、OS の機能により、Triple DES 等の暗号化通信を実現している。
標準化動向	・Bluetooth コンソーシアムの SIG 活動で仕様を作成 ・SIG活動の特徴は利用場面を想定した標準化の作成(各種ﾌﾟﾛﾌｧｲﾙにて規定)と機器の互換性を確保するロゴ認証制度である。 ・現在 V1.0 として Generic Access（機器の接続・認証）、Serial Port、FAX 、File Transfer（ファイル転送）等 13 個のプロファイルを制定済み ・V2.0 として Automotive（自動車内のサービス）、Printing（プリンター機器）、Human Input Device（マウス・キーボードなど）のプロファイルを検討中 ・決済については Financial Transaction として SIG 活動の前段階である Study Group で検討中	・1993 年 6 月、標準化活動組織の発足以来，IR 通信を使った応用および IR 通信の市場拡大を目指して，様々なプロトコルの標準化を実施 ・その結果として，様々な製品・応用に IrDA が利用された反面，実装方法の相違による相互通信性の欠如が指摘されている。 ・そこで近距離でのファイルや画像データの転送，印刷，モデムアクセス，データのシンクロナイズといった応用毎に，実装上の規約をガイドラインとして明確にして，相互通信性が保証されるようにした. ・2000 年 4 月には，1 対 1 の機器間でのオブジェクトデータの交換を実現するための"Point and Shoot"プロファイルが策定された．今後もモデムアクセスなどのプロファイルが策定されていく見通しである.	・Type A:リーダ→カード:ASK100%,Modefied Miller 符号化,転送速度 106kbp カード→リーダ負荷変調，副搬送波(847kHz9，OOK, Manchester 符号化 ・Type B:リーダ→カード:ASK10%, NRZ-L 符号化,転送速度 106kbps カード→リーダ:負荷変調，副搬送波(847kHz)，BPSK,NRZ 符号化 ・Type C：変調度 ASK10%,Manchester 符号化(リーダとカードの双方向共), 転送速度 212kbps Type A は変調度が 100%となっている為側帯波出力が大きく、日本の電波法の下で使用する場合に出力に制限を受ける。 現在、これらの標準化の状況は、下記の通り。 ・Type A および Type B:ISO/IEC 14443-1,-2,-3,-4,ISO/IEC10373-6（完了） ・Type C:ISO/IEC 14443-2AMD1（2001 年 3 月 CD 化へのバロットに入り審議中）
特徴	・透過性がある 通信機間に障害物があっても通信可能 ・通信の指向性がない 通信可能距離が広い（10m～100m） ・1 対ｎ接続可能 ・グローバルな標準ワイヤレス技術 PC、携帯電話、ヘッドセット、プリンタ等の機器を無線で接続する標準ワイヤレス技術。世界 2000 社以上が賛同 ・低消費・低価格・小型・軽量 ・ネットワーク構成が容易 アドレスの設定等不要で自動接続が可能 ・利用場面までを想定した仕様をプロファイルとして作成 利用場面から検討してプロファイルを設定しているため、開発に伴う利便性が高い	・通信の指向性がある 通信機同士の向きを合わせる必要あり ・透過性が無い 通信機間に障害物があると通信不可能 ・低消費・低価格・小型・軽量 携帯電話の待受・通話時間を圧迫しない十分な低消費電力化を小型/軽量/低価格で実現可能。実装実績も豊富 ・IrDA-Data が実装されている PC/PDA などとの相互通信が可能 ・ページャなど処理能力の低い端末との通信も可能 ・直射日光下での通信が不安定	・即時性がある。 ・端末捕捉－セッション開始までの時間は約 5ms と短い。 ・位置決め精度が荒くて良い。 通信範囲はリーダ/ライタ・アンテナを中心として半径 10cm 程度の半球状に端末を移動させる事で通信が可能になる。 ・最大 1 対 3 までの通信が可能 ・高い耐環境性 汚れ等の劣悪環境でも使用可能 ・TypeA は、日本の電波法の下で使用する場合に出力に制限を受け、通信可能距離が短く、密着する必要がある。 ・端末の消費電力･アンテナ･基地局の出力により通信可能距離が大幅に変化する。 ・TypeC はリーダとカードの双方向共、同じ符号化方式であるため、外部機器のリーダとリーダ間通信をすることが可能

モバイル利用に適した場面	【利用場面】 ・簡易なデータ通信 ファイル転送/同期など ・比較的距離が離れていて(数十 ㎝～数ｍ)、ケーブルの引き回しが不便な状況 ・移動しながらの利用 ・見通しのない場所にある機器との通信 【用途】 ◇オブジェクト交換 ポイントサービス，クーポン券，会員カード 【その他用途】 ◇オブジェクト交換 PC と携帯電話のワイヤレス接続によるファイル転送/同期 小人数会議での PC 情報交換 LAN ◇データ通信 モデムアクセスによるダイアルアップ接続など ◇外部接続機器のワイヤレス接続 プリンタ，デジタルカメラ，プロジェクター等とＰＣの接続 ◇音声通話 ワイヤレスヘッドセット コードレス電話	【利用場面】 ・簡易なデータ通信 ファイル転送/同期など ・近距離で静止時の利用 【用途】 ◇オブジェクト交換 ポイントサービス，クーポン券，会員カード 【その他用途】 ◇オブジェクト交換 電話帳やスケジュール，メッセージやノートなどの オブジェクト交換 ポイントサービス ◇データ通信 モデムアクセスによるダイアルアップ接続など ◇音声通信 スピーカーとマイクを一体化したヘッドセットに よりワイヤレス化が可能 ※既に国内外で携帯電話などに実装実績がある。PC 上の PIM ソフトウェアからの電話帳・スケジュール転送や、ダイヤルアップ接続が可能。	【利用場面】 ・高速処理が必要とされる状況 ・決済処理等のセキュリティが必要とされる状況 （FeliCa 技術方式は、セキュリティを上位層で規定） 【用途】 ◇認証 改札ゲート(乗車券，定期券，チケット等)、入退室カード ◇決済系データ通信 電子マネー、プリペイド ◇オブジェクト交換 ポイントサービス，クーポン券，会員カード 等 【その他用途】 ◇データ参照 IC カード上のデータ参照(ビューア機能)
モバイルコマース適用への課題	・コマースサービス利用当事者の特定が困難 ⇒ある程度の距離の範囲でセッション確立が可能なため、対面取り引き等ではセッション確立相手がコマースサービス利用当事者か特定する必要がある。 ・決済用には、上位レイヤーでセキュリティを規定する必要あり。 ・店舗側への Bluetooth I/F 対応機器の配備が重要課題である。	・移動しながらの利用(改札等)には不向き ・機器をポケットに入れたままでの利用は不可能（透過性なし） ・セキュリティーの規定がないため、上位ＡＰでの対応が必要 ・店舗側への IrDA I/F 対応機器の配備が重要課題である。	・移動機実装の検討が必要 電磁誘導により電力搬送を行っている為、周辺に金属が存在すると通信距離に制限が生じる場合がある。 ・店舗側への非接触 I/F 対応機器の配備が重要課題である。

3.2　利用シナリオから見たローカルワイヤレスインタフェース

本書では、Bluetooth、IrDA、非接触 IC という代表的なローカルワイヤレスインタフェースを取り上げ、その技術的側面からモバイルＥＣへの適応を考察している。

しかし、ローカルワイヤレスインタフェースのモバイル EC への適用については、それぞれの技術要素からのアプローチだけでなく、実際のサービス/アプリケーション側からの要件というものとあわせて検討する必要があると考えられる。

モバイルＥＣにおける新サービスの調査・検討中間報告書の**５　ユーザニーズに基づくサービス/アプリケーションの抽出**の項では、実際のモバイルユーザに対してアンケート調査した結果から、将来有望なモバイル EC アプリケーションを抽出して、それをモバイル EC の各プロセスに分解、それぞれのプロセスで技術的側面、運用的側面から要件や課題を整理している。

ローカルワイヤレスインタフェースのモバイル EC への適用について検討される場合は、本書とあわせて、モバイルＥＣにおける新サービスの調査・検討中間報告書もあわせてご覧頂くようお願いする。

参　考　資　料

1 IC チップに関わる動向

1.1 IC チップの種類

携帯電話端末に搭載する IC チップに関して、ここでは、次のような決済モデルを前提に、その技術・利用（含、実験等）・標準化、等について整理した。

本アドホックで検討対象とする形態のイメージは以下の通りである。

図 1-1 携帯電話 vs 決済端末

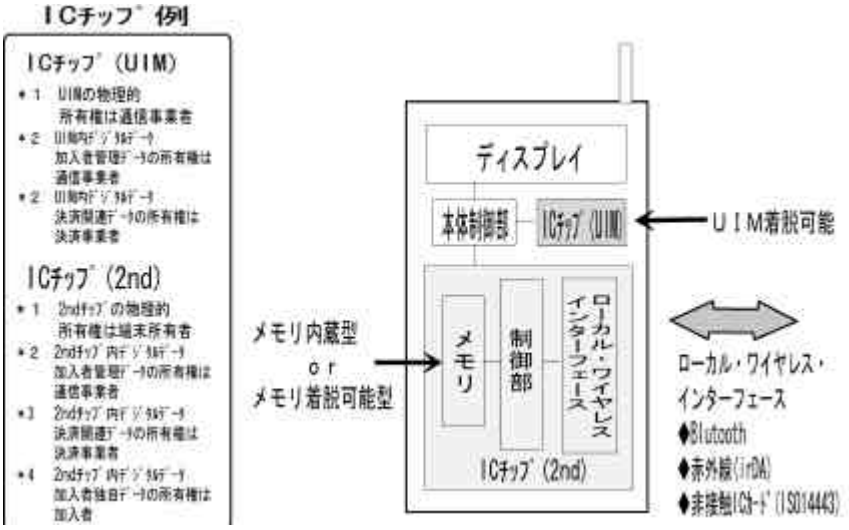


図 1-2 IC チップの構成

このようなモデル形態を利用したモバイル決済を念頭に置いて記載する。

1.1.1 UIM (User Identity Module)

1.1.1.1 定義と概況

W-CDMA では、現在、GSM で使われている SIM の機能を次世代携帯電話向けに拡張したものとして位置づけられている。

（既存 GSM 標準の SIM との互換性が求められる）

cdma2000 でも、中国等を中心に導入が検討されている。

（新規であるが 3GPP2 ではオプション機能として検討中である）

1.1.1.2 UIM の特徴

SIM と比較して、UIM においては、下記の点が特徴となっている；

-IMT-2000 対応の情報処理能力を備えている。

-大容量化、高機能化がなされている。

→Java や MULTOS、Windows for Smart Cards 等のプラットフォームベースが搭載可能である。

これにより、マルチアプリ搭載可能

-多機能化への対応ができている。

→WIM、PKI、非接触、等の付加機能を備えたチップも存在する。

なお、UIM においては、その上で付加価値サービス(VAS)に関する各種試みがなされている。

3G サービスにおける UIM の仕様要件については 3GPP（3rd Generation Partnership Project）3G TS 21.111 に規定され、同 31.101 でインターフェース特性、同 31.102 でアプリケーション特性が規定されており、これを満たすものを USIM と呼ぶ。

一般仕様要件については以下のように規定されている。（抄訳は参考資料：ＵＳＩＭとＩＣカードの要件に記載）

- UICC は USIM を含む取り外し可能なモジュールである。加入者を明確に確認する識別情報が含まれていなければならない。
- 3G のサービスにアクセスする時には必ず有効な USIM を含む UICC が装着されていなければならない。ただし、緊急通報は除く。
- この仕様は、33.107[7]で定義されているセキュリティ要件を満たしていなければならない。

・USIM は必ず加入契約情報と加入者情報の格納を提供しなければならない。
・UICC/USIM は、USIM アプリケーションツールキットの仕様書 3G TS 31.111[6] で規定される機能を使用するアプリケーションを含むこともできる。

この場合の型式認定については、次のとおり定められている。
SIM の HW,SW ともの型式認定のプロセス、空きメモリ領域付加アプリケーション搭載に関して、ファイアウォールのようなセキュリティに関する要求は携帯電話事業者ごとの問題となる。
型式認定は、事業者ごとの要求を満足しているかで判断されるのでファイアウォールも同等の扱いになる。

認定に関しては UIM の発行者、すなわち事業者が行なうことになっている。
ただし、将来的なことはわからない。たとえば、UIM にクレジットアプリを搭載するようなことがあれば、UIM に対してサービスプロバイダであるクレジット会社の認定が必要になることも考えられる。

1.1.2 2nd チップ

ここでは、UIM に搭載できないアプリケーションを搭載するためのチップの存在を仮定する。これは、交通機関やチケッティング、電子マネー等への応用が考えられている。
なお、個々のインプリ固有の技術としては、各々の利用シーンに対する要求に応じて、非接触カード I/F や Bluetooth 等のローカルワイヤレスインターフェースとの連携が考えられる。（本件の技術的詳細はローカルワイヤレスインターフェース部分を参照のこと）

なお、SIM 形状のチップの他に、音楽データ等を携帯電話端末に取り込んで使用することを目的に、著作権管理機能を持ったメモリーカードがある。

1.1.2.1 新しいサービスとセキュリティのニーズ

最近、音楽を始めとしたデジタルコンテンツの配信サービスが、新しいビジネスとして注目を浴びている。デジタルコンテンツとしては、着メロ、壁紙、カラオケ、地図、静止画、動画、ゲーム、プログラム、ニュース、語学教材、電子書籍など多彩である。配信サービス、とりわけ移動体通信端末を用いた配信サービスの利点は、いつでも、どこでも、居ながらにして欲しいコンテンツを入手出来ることである。これらのコンテンツは、ダウンロード端末の中に止まって取り出せない様になっている限り、セキュリティ上の心配はない。しかしこれでは利便性に欠ける。ダウンロード端末のメモリが一杯になってバックアップを取りたい場合や、他の端末で利用したい場合など、リムーバブルなメディアに記録することで、配信サービスの価値が大幅に上がる。ところが、コンテンツを供給するコンテンツホルダーは、

リムーバブルなカードによる違法コピーで著作権が侵害される恐れが出てくる為、コンテンツの供給が出来なくなる。これらを解決する為には、コンテンツ保護機能を搭載したメモリカードが必要となる。このようなニーズを満たす為、大容量メモリカードにセキュリティ機能を付加したメモリカードが使用される。

1.1.3 SD カード

SD カードは、データの不正コピー・不正書き換えを防ぐ高度な著作権保護機能を搭載したメモリーカードである。従来のメモリーカードに比べ、記憶サイズの大容量化（６４MBおよび３２MB）・形状の小型・薄型化（１.６ｃｃ、２.１mm厚、切手サイズ）データの書込み速度の高速化（２MB/ｓ）が実現された。

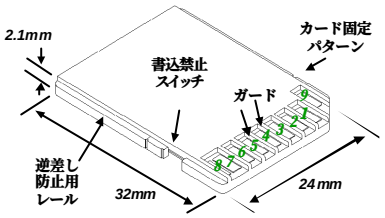
図 1-3 SD カード 写真）

1.1.3.1 技術概要

以下に、SD メモリーカードの技術的内容について説明する。

図１-4 は、SD メモリーカード形状とピン配置である。本形状は、マルチメディアカードに対して上位コンパチであり、SD メモリーカード用ソケットを持つホストには、両方のカードが装着可能である。厚さを２.１mmにすることで、カードの曲げやねじれ強度をより強固にするとともに、同一実装技術でメモリーを実装した時、２倍以上のメモリー容量のカードを同時期に提供可能である。

また、通信速度については、同種サイズのメモリーカードでは初めて４ビットＩ／Ｏを採用し、高速化やＩ／Ｏカード用途等へも十分適用できる仕様とした。さらには、民生用途でのカードの普及を考慮し、ピン間にガードを設けユーザが直接ピンに触れないことでピンの保護を図り、書込禁止スイッチ・カードの固定用切れ込みパターン・逆差しを防止用レール等の新しい機構を持たせてシステムとしての信頼性向上が図られている。



ピン番号	端子名	説明
1	CD/DAT3	ｶｰﾄﾞ検出／ﾃﾞｰﾀ I/O
2	CMD	コマンド
3	VSS	グランド
4	VDD	電源
5	CLK	クロック
6	VSS	グランド
7	DAT0	データ IO
8	DAT1	データ IO
9	DAT2	データ IO

図 1-4 カード形状とピン配置

図１-5 は、SD メモリーカード内部のブロックを示す。回路ブロックとして、主には SD インターフェースコントロール部・著作権保護部・フラッシュコントロール部・レジスタ部・フラッシュメモリー部で構成されている。64MB カードの場合は、コントローラとフラッシュメモリー２チップの半導体で構成される。レジスタ部はコントローラ内にあり、ホストからレジスタを参照および設定することで、カードの特性や機能を把握コントロールできる。

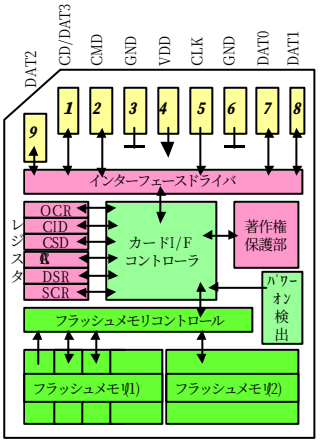


図 1-5 カード内ブロック

また、カードとホスト間の通信については、コマンド信号とデータ信号をクロック信号に同期させて両者がハンドリングしながらやり取りを行うコマンドプロトコルを持った仕様を採用している。この仕様により、将来カード性能が向上し例えばデータ転送の高速化が図られた場合にも、ホストの変更なしで自動的にシステムの性能向上を図ることができる。すなわち、今後の技術の進歩によるカード性能の向上にホストシステムが追従可能で、結果としてホストの製品寿命を延ばすことが可能となる。

1.1.3.2　著作権保護のメカニズム

本著作権保護機能は、下記の特長を持つ。

１．カードとホストが正規の機器であることを相互に確認する（相互認証）。

２．乱数を用いて生成させた鍵を使った通信手段で安全に情報を転送する。

図１-6 は、具体的な音楽録音再生システムでの著作権保護の運用例である。

ここでデータ領域は、自由にアクセスが可能な領域で、プロテクト領域は、相互認証後初めてアクセス可能な領域である。カードとホストの相互認証後、カードに書き込まれる音楽コンテンツは、著作権情報により暗号化された形でデータ領域に格納される。かつ、その著作権情報は、音楽コンテンツと関連付けられてカード固有鍵で暗号化されてプロテクト領域に格納される。

また、音楽コンテンツ再生時には、まず相互認証を行い著作権情報をプロテクト領域から取得する。さらに、データ領域に格納された暗号化された音楽コンテンツを取得後、先の著作権情報で復号し音楽の再生を行う。

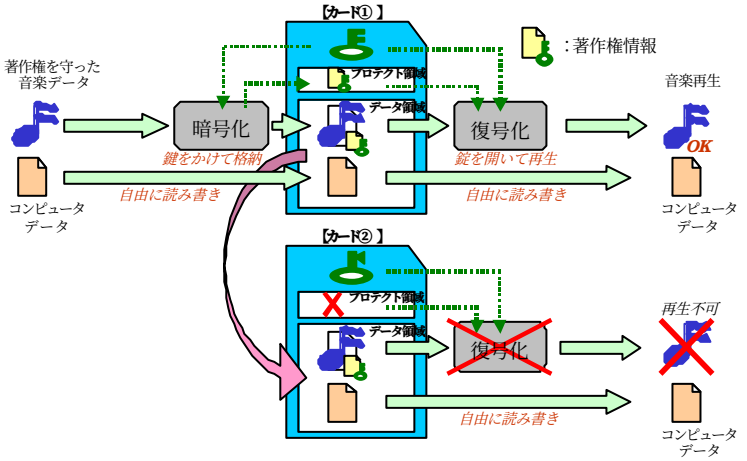


図 1-6 著作権保護の仕組み

ここで、データ領域にある暗号化された音楽コンテンツは、カードユーザが自由にアクセス可能であり、この情報を異なるカードのデータ領域にコピーすることは可能である。しかし、プロテクト領域に格納された著作権情報はコピーできない為、不正なコピーは不可能である。また、プロテクト領域の著作権情報の受け渡しにおいては、カードとホスト間では、相互認証のたびに更新される鍵を使った転送を行う為、カードとホスト間の電気信号を操作して、著作権情報を改竄したり、不正に取得したりすることができない仕組みを実現している。

1.1.3.3 標準化状況

SD カードは、SD アソシエーションにおいては、オープンな場で世界標準を目指しており、参加メンバーによる協議により最も適切で汎用性のある SD カードとそのアプリケーション仕様を提案し、拡張性と発展性のある SD ワールドを構築しつつある。

1.1.3.4 応用例

図 1-7 は、現在想定している SD メモリーカードの応用製品群である。

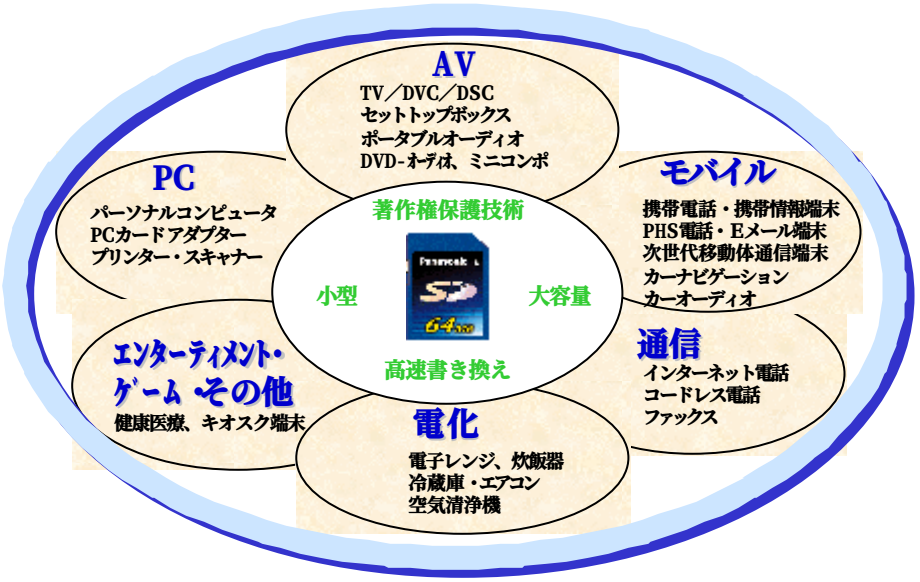


図 1-7 SD カードの応用分野

1.1.4 SMMC(Secure Multimedia Card)

音楽の他に、コンテンツ保護を必要とする他のサービスとしては、電子チケット、電子宝くじ、電子株取引、電子定期券、プリペイドカードなどがある。一方、クレジットカード、

デビッドカードなどでは､本人であることを確認するためのユーザー認証機能が必須となっている。ホームバンキング、個人財産管理なども同様である。

更に、デジタルコンテンツの購入と購入代金の決済を同時に行うＥコマースにおいては、コンテンツ保護機能とユーザー認証機能の両方を兼ね備えたメモリーカードが必要になる。これら両方の機能を必要とするサービスとしては､医療記録やホームセキュリティなどの個人情報の保護、イントラネットへのアクセスなど企業情報の保護、電子選挙などがある。

図 1-8 SMMC カード

マルチメディアカード（以下、ＭＭＣ）では、これらのセキュリティのニーズに対応するため、セキュアマルチメディアカード（以下、ＳＭＭＣ）のシリーズとして、コンテンツ保護セキュアマルチメディアカード（ＣＰ－ＳＭＭＣ）を製品化し、Ｅコマース・セキュアマルチメディアカード（ＥＣ－ＳＭＭＣ）の仕様策定を行っている。

1.1.4.1 SMMC の技術概要

(1) 著作権保護技術

Ａ．ハードウェアタンパーレジスタンスモジュール(ハードウェアＴＲＭ)

ＣＰ－ＳＭＭＣの記憶領域は大きく二つに分類される。暗号化コンテンツや非セキュアデータなどを格納するフラッシュメモリ、ＣＰ－ＳＭＭＣの秘密鍵やコンテンツ鍵などを格納するＴＲＭ領域である。ここで、ＴＲＭ領域は、外部からのソフトウェア的およびハードウェア的攻撃による内容の改竄や秘密データの取り出しを防ぐ為、ハードウェアＴＲＭ構造を採用している。

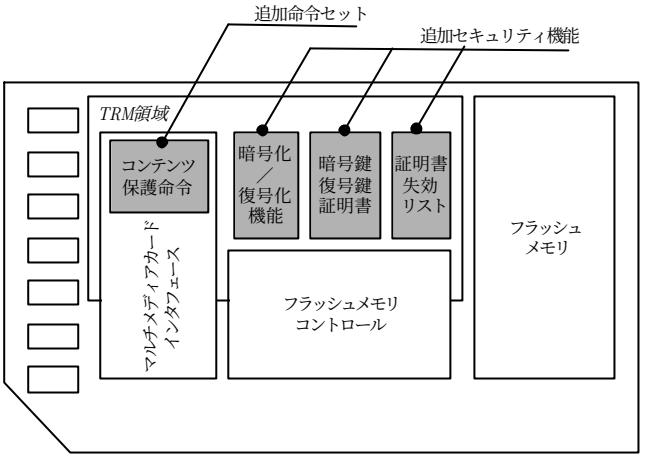
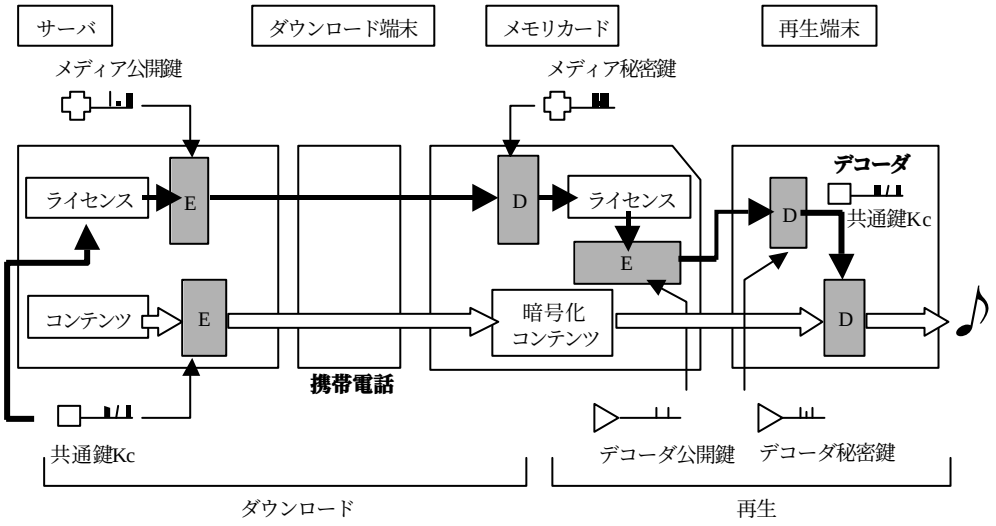


図 1-9 SMMC 内ブロック

(2) ＰＫＩ(Public Key Infrastructure)と X.509

ＰＫＩは、ＩＣカード、ＳＩＭカードで実績のあるオープンなセキュリティ方式で、セキュリティレベルの高い方式として銀行カードや、ＧＳＭ 仕様の携帯電話に広く使われている。ＣＰ－ＳＭＭＣは、コンテンツ保護を実現する為に楕円ＤＨ(Diffie Helman)をＰＫＩとして使用している。

また、ＣＰ－ＳＭＭＣには、認証局が発行したルート公開鍵で署名認証できるメディアの証明書(X.509 形式)が格納されており、この証明書を署名認証することで不正なメディアのなりすましを防いでいる。署名方式としては楕円ＤＳＡ(Digital Signature Algorithm)を使用している。



E:暗号処理　D :復号処理

図 1-10 暗号･復号の様子

ＣＰ－ＳＭＭＣは、ダウンロード／再生時の暗号・復号機能を内蔵しており、メディアそのものが直接ネットワーク上のサーバーや再生装置の暗号･復号チップと直接暗号処理を行う。

この為、ダウンロード端末は暗号処理機能を持つ必要がなく、モバイルに非常に適した方式と言える。また、ＣＰ－ＳＭＭＣを音楽プレーヤーの記録メディアとして採用する場合、この著作権保護技術は、ＳＤＭＩ（Secure Digital Music Initiative）準拠である。

(3) 超流通技術（合法的コンテンツコピー技術）

コンテンツは、コンテンツ固有のコンテンツ鍵で暗号化されている為、暗号化コンテンツの流通は柔軟性に富んでいる。ネットワーク経由でＣＰ－ＳＭＭＣにダウンロードした暗号化コンテンツは、自由にコピーすることが出来る。どんなにコピーしても、コンテンツ鍵がなければ再生出来ないので、利便性を損なうことなく合法的にコピーすることが出来る。また、暗号化コンテンツをＣＤ－ＲＯＭに記録して配布することも出来る。配布されたＣＤ－ＲＯＭの内容をＣＰ－ＳＭＭＣにコピーすれば、コンテンツダウンロードに伴うネットワーク接続料金を節約することも出来る。さらに、ＫＩＯＳＫ端末やインターネットから暗号化コンテンツをダウンロードすることも可能である。コンテンツを再生したい時にコンテンツ鍵を購入すれば、いつでもどこでも再生することが出来る。

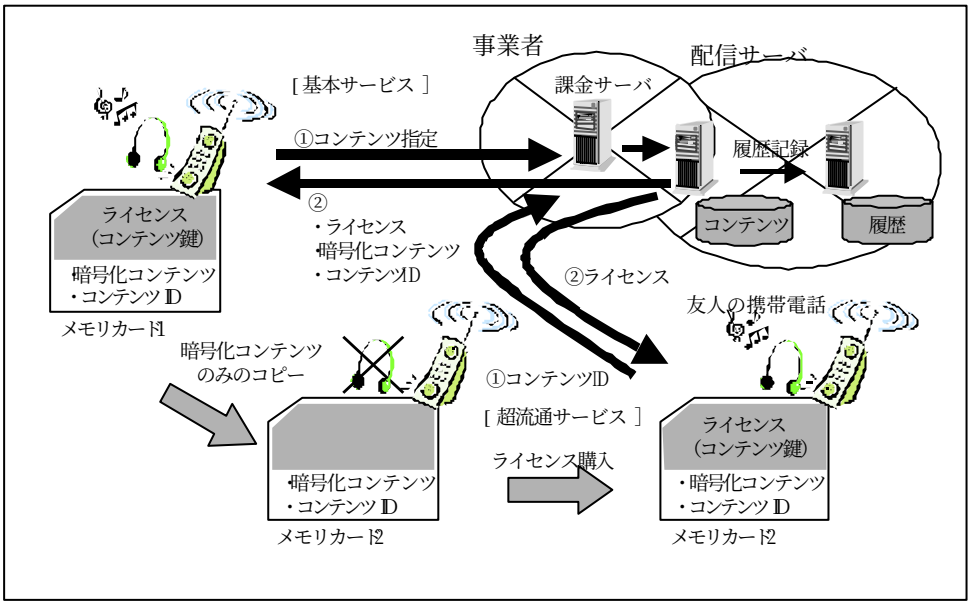


図 1-11 超流通技術 合法的コンテンツコピー技術）

1.1.4.2　ユーザー認証技術(WIM)

更に、もう一つのセキュリティ機能であるユーザー認証機能を取り入れたのがＥＣ－ＳＭＭＣである。ＥＣ－ＳＭＭＣでは、ＷＡＰフォーラムで規定されているＷＩＭ（WAP Identity Module）のセキュリティ命令を採用し、汎用性の高いセキュアなメモリカードを実現する。内部構造は、ＩＣカードとマルチメディアカード（以下、MMC）を一体化したものである。このカードに、アプリケーションの実装と鍵の書き込みなどのパーソナライゼーションを行うことで、専用の機能を持ったセキュアなカードになる。例えば、特定の銀行のアプリケーションを実装すれば、銀行カードになる。音楽配信用コンテンツ保護のアプリケーションを実装すれば、音楽カードになる。両方のアプリケーションを実装すれば、ダウンロードした音楽の購入代金の決済を、自分の銀行口座で行える様になる。すなわちＥコマースの実現である。

ＥＣ－ＳＭＭＣは、ＣＰ－ＳＭＭＣと同様に、ＰＫＩとハードウェアＴＲＭを採用し、更にＩＣカード並みのタンパーレジスタンスを実現するための技術を取り入れている。

1.1.4.3　標準化の状況

ＳＭＭＣの標準化は、マルチメディアカードアソシエーション（以下、ＭＭＣＡ）で行われている。ＭＭＣＡは、携帯電話メーカーを中心とする小型カードの標準化団体で、2001 年 2 月現在の会員数は 99 社である。

ＣＰ－ＳＭＭＣは、2000 年 11 月に標準化が承認され、現在手続き中である。

ＷＩＭをベースとしたＥＣ－ＳＭＭＣは、2000 年 5 月よりタスクオリエンテッドグループ（以下、ＴＯＧ）にて仕様書作成作業を開始し、2000 年 11 月に正式提案された。現在詳細仕様を詰めている段階である。

1.1.4.4　ビジネス例

ＳＭＭＣは、世界初の移動体通信端末を用いた音楽配信サービスとして、ＤＤＩポケット社が 2000 年 11 月 30 日から開始した「SoundMarket」の記録メディアとして採用されている。

本サービスでは、レコード会社などのコンテンツホルダーから提供されたコンテンツを、ＭＰ３方式のエンコーディングを行った後、暗号化を施し、ダウンロードサーバーに蓄積する。暗号化されたコンテンツとコンテンツ鍵（「SoundMarket」では「パスキー」と呼ぶ）は、ダウンロードサーバーからＤＤＩポケット網を通して、ＰＨＳの一種であるフィールエッジ端末でＳＭＭＣにダウンロードされる。

コンテンツは、音楽だけではなく、鳥の声や川のせせらぎなどの自然音、英会話などの語学教材が提供されている。コンテンツホルダーの数は、2001 年 2 月 21 日現在で１５社、コンテンツの数は 1000 曲強である。「SoundMarket」対応のフィールエッジ端末は、三洋電機、京セラより販売されており、端末と接続して音楽を再生するプレーヤーは、三洋電

機より販売されている。一方、ＳＭＭＣは、日立製作所にて製造・販売されている。

1.2　アプリケーションサポート技術

ここでは、ＵＩＭや２ｎｄチップ上に金融等のアプリケーションを搭載できるようにするための技術であるマルチアプリケーション搭載プラットフォームに着いて記述する。

1.2.1　Java カード

1.2.1.1　技術概要

(1) はじめに

Java カードとは Java アプリケーション環境の考えを IC カードに摘要したものでアプリのカード発行後の追加が容易になるなどの特徴を持っている。

(2) 特徴

・プラットフォームに独立なこと

Java カードアプリケーション環境を使用して開発されるため異なるベンターのカードであっても互換がある。

・複数のアプリケーションを搭載可能なこと

Java の特徴として１つのカードで複数のアプリケーションが動作しても安全問題は無い。

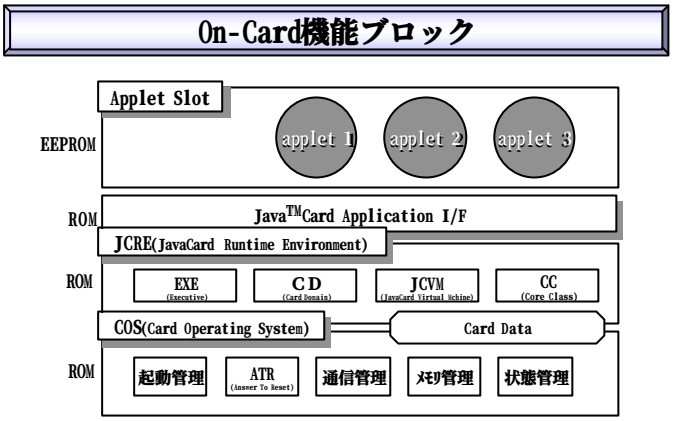
・カード発行後のアプリケーションの追加が可能なこと

これまでの IC カードのアプリケーションは ROM 領域に置かれるため、発行時に書きこむ必要があったが、Java アプリは EEROM 領域に置かれるため、カード発行後の追加･変更･削除が可能である。

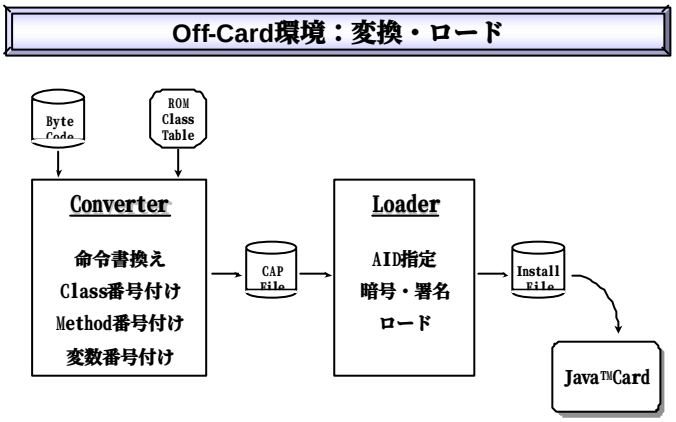
・既存の IC カードの標準と互換があること

Java カード API は ISO07816 や EMV との互換を有する。

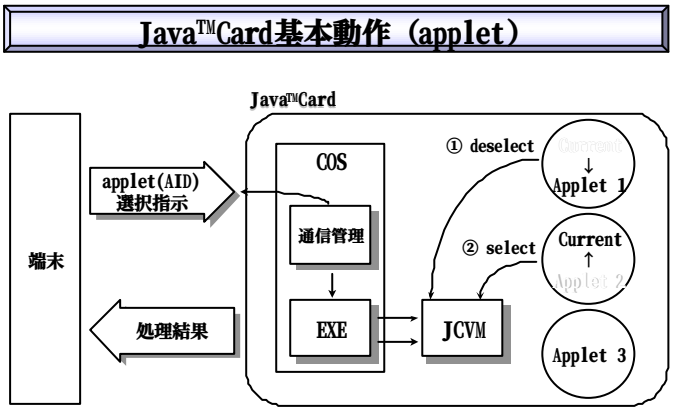
(3) 概要



カード OS とアプリの間に JCRE（Java Card Runtime Application Environment）があり Java アプレットと OS の間のインターフェースを取ることで Java アプレットの動作環境を実現している。



アプリ Java 言語で記述するが、Java カードの機能が小さいこと等から Converter で一度変換し Loader で実際のカード上にロードする。



動作としては端末からはアプレットの選択指示が与えられ、OS 経由でカード上の JCVM(Java Card Virtual Machine)に伝えられアプレットを起動する。

図 1-12 Java カードの概要

(4) 標準化状況

① Java Card Forum

Java カード API の標準化は Java Card Forum（http://www.Javacardforum.org）で推進している。Java Card Forum はジェンプラスとシュルンベルジェにより 1997 年 2 月に設立され、主なメンバーはブル、ド・ラ・リュ、IBM、日立、Oberthur、東芝である。

1998 年 10 月に標準化プロセスと産業用途向けの拡張を発表した。Java Card Forum の通信グループは GSM API を定義しこれをベースに ETSI SMG9 は標準化を決めるとのこと。ETSI SMG9 は GSM に IC カードとモバイル機器インタフェースの仕様を決める責任ある団体である。

② GLOBAL PLATFORM

Java Card の Applet の互換については Global Platform （http://www.globalplatform.org）が IC カードのアプリケーションの標準として推進している。Global Platform は 1999 年 10 月に設立され、主なメンバーは VISA、British Telecom、ジェンプラス、JCB、マイクロソフト、モトローラ、ノキア、NTT、 Oberthur、サンである。NEC、ニューメディア開発協会、東芝は賛助会員である。

目的は VISA が開発する Open Platform のカード仕様と端末の移転により共通カード仕様を推進することである。Open Platform 技術はサンの Java カードプラットフォームとマイクロソフトの Smart Card for Windows で実現することができる。

(5) ビジネス関連

① 開発・運用形態

現時点では特に情報は無い

② アプリ認定

現時点では認定はないようである。

③ ライセンス形態

現時点では Java カードとしてのライセンスベンターに対するライセンスが必要である。

(6) 利用規定

現時点ではない。

1.2.1.2 応用事例・実験紹介

(1) SCJ（スマートコマースジャパン）での実証実験

神戸地区で電子マネー、IC クレジットカードの実証実験を行っている SCJ（スマートコマースジャパン）の実験のひとつとして、2000 年秋に顧客会員に Java カードを

発行し、Java カードの機能としてアプレットが書きかえられる特徴を活かして、来店頻度・回数によりゲームが顧客に有利となる仕組みを作り Java の有効性を検証した。

(2) 慶応大学と NTT データの共同プロジェクト

2000 年 9 月 18 日に NTT データと慶応大学より Java カードを次世代キャンパスカードとして位置付け、学生証・教職員証として展開していくとの発表があった。

1.2.2 MULTOS

1.2.2.1 技術概要

MULTOS（Multi-application Operating System）とは、MAOSCO コンソーシアムによって仕様が管理されているセキュリティの高いマルチアプリケーション OS である。異なる IC チップ（ハードウェア）間におけるアプリケーションのインタオペラビリティを実現し、チップ内の ROM(読出し専用メモリ)に MULTOS を持ち、同じくチップ内の EEPROM（電気的に書換え・消去可能なメモリ）にアプリケーションやデータを持つ構造になっているため、MULTOS カードはカード発行後にアプリケーションの追加・削除を行なえるのが特徴である。また、ファイアウォールと呼ばれる仕組みを使っており、IC カード上のアプリケーションがお互いに不正アクセスできないようなアーキテクチャになっていることから、各アプリケーションの独立性とセキュリティを保つことが可能である。（図 1.13、1.14 参照）

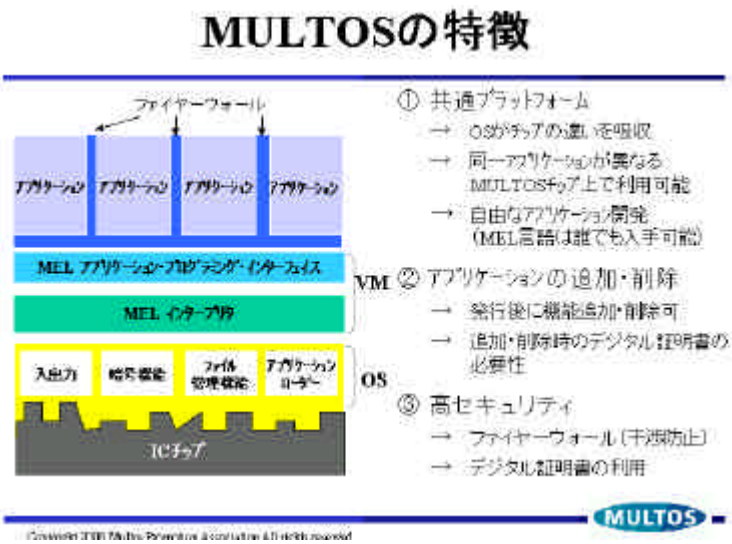


図 1-13 MULTOSの特徴

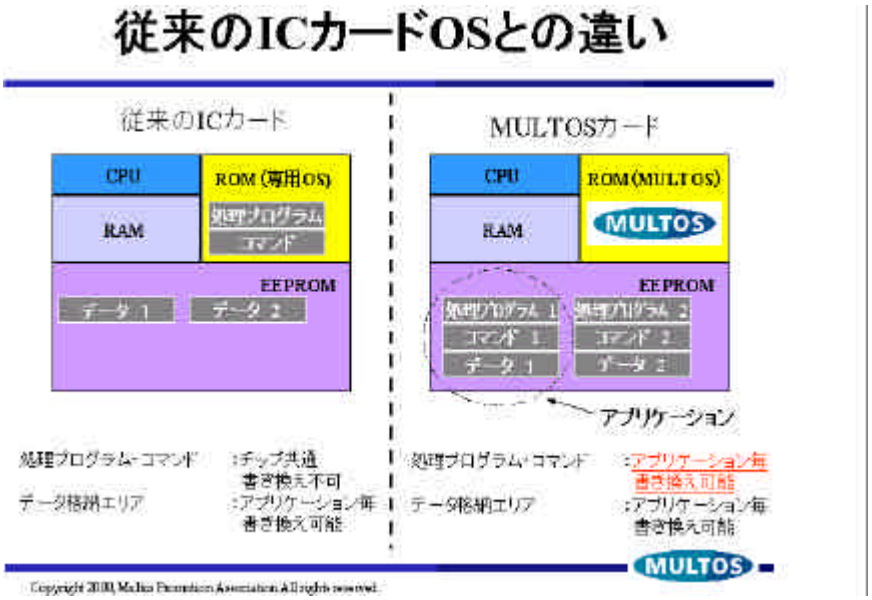


図 1-14 従来の IC カードOS との違い

MULTOS のアプリケーションは、MEL（MULTOS 実行言語）をベースに開発され、一般的には C 言語等 MULTOS 専用の RISC（縮小命令セット計算機）形式である MEL 言語にコンパイルされる。アプリケーション開発から MULTOS シミュレータでの実行試験、デバックに至るまで、全てパーソナルコンピュータの Windows 環境で実行できるので、開発やテストに無駄な時間をかけない。現在の MULTOS 仕様はバージョン４である。

(1) 非接触インターフェース（無線式）

MULTOS バージョン５では、ISO14443TypeA 及び Mifare 仕様の非接触（コンタクトレス）インタフェースを採用したことによりチケット・交通などに関連するアプリケーションの持つ可能性を大きく広げている点が特長である。

(2) 携帯電話、GSM

MULTOS プラットフォームが GSM　SIM をサポートすることになったことで、M－コマースは大きな転換期を迎えつつある。銀行業務、支払い業務、PKI（デジタルによる身分証明）、ロイヤルティプログラムなどのあらゆる機能を MULTOS GSM SIM カードに組み込むことで、既存の電話機を使って行なうことが可能となり、携帯電話の役割が劇的に広がってきている。MULTOS バージョン５では、ネットワーク事業者が GSM 携帯電話で採用している暗号化アルゴリズムをサポートしている。バージョン５のテクノロジーはデュアルスロットの電話と（U）SIM 専用電話のどちらにでも仕様可能で、ネットワーク事業者にとって主に３つの利点がある。

- マルチアプリケーション

高度なセキュリティが保証されたことにより、１つのチップにそれぞれが機密性の

高い複数のアプリケーションが、相互に干渉しあうことなく搭載される。アプリケーション間にファイアウォールが設定されており、ネットワーク事業者や銀行業者や銀行関係者の心配の種であったクロスハッキングを確実に防止できる。MULTOS バージョン５を使えば、金融業界ですでに確立されている高い安全性をネットワーク事業者にも提供できる。

- アップデート可能

  ネットワーク事業者は、SMS メッセージサービス技術や将来のデータベアラーを使って SIM カードにアプリケーションを追加したり削除したりすることで、既存の加入者向けサービスをアップデートできる。これにより、顧客はネットワーク事業者にも提供できる。

- 互換性

  他のスマートカードプラットフォームと異なり、MULTOS バージョン５はどの半導体メーカー（日立製作所、Infineon、フィリップス）とも互換性があるため、各 MULTOS のビジネスモデルを完全にサポートしている。したがって、ネットワーク事業者が半導体メーカーを変更しても、アプリケーションコードを書き直す必要がない。さらに、MULTOS は標準オペレーティングシステムを提供するので、発行後のカード管理も容易になる。

(3) 楕円曲線暗号方式（ECC）

MULTOS API は、アプリケーション開発者が最新の非対称 ECC 暗号化の利点を活用できるよう拡張してきた。PKI や WAPWIM などのアプリケーションに加えて、RSA を使用した既存アプリケーションでもこの最新技術を活用できる。

1.2.2.2 標準化状況

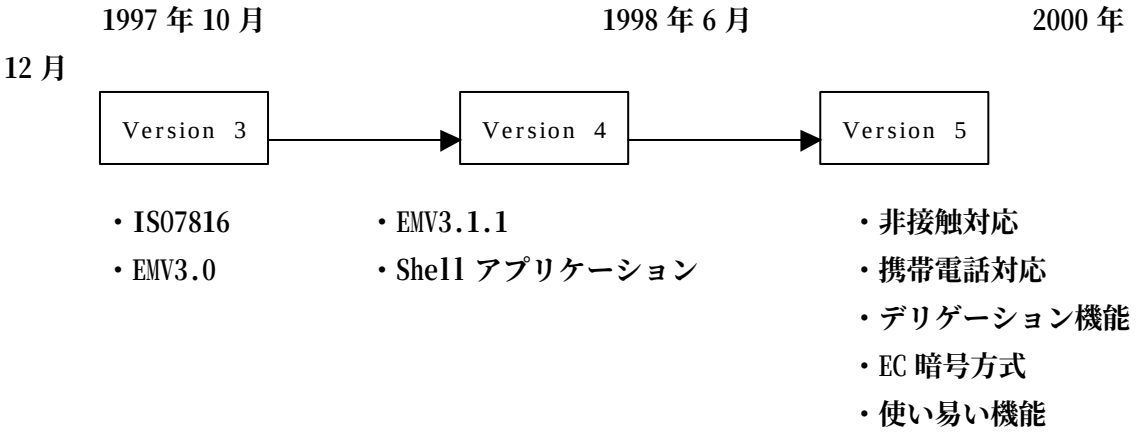


図 1-15 標準化状況

1.2.2.3　ビジネス関連

(1) 開発・運用形態・アプリ認定

MULTOS のビジネス・モデルはカード発行者を中心とした構造になっている。発行者は、カード保有者ごとのアプリケーションやサービスを提供するか（つまり、保有者のカードに対する追加・削除）を管理する。ただし、カード発行者は任意に、自身による管理を拒否できる。それには、２つの方式がある。

１．発行者が第三者のサービス提供者と契約を結び、カード発行者所有のドメインにアプリケーションを追加する作業をそのサービスの提供者に委託する。

２．同じ要領で一連の処理をサービス提供者に委託し、保有者が希望するサービスを選ぶ。

カード発行者の管理権限が MULTOS スキームの中で果たす役割はもう一つある。MULTOS では各種プラットフォーム間でアプリケーションを相互運用することができるので、カード発行者は調達ソースをカード・メーカだけに頼らず、複数の調達ソースを利用できる。その結果、必然的に価格競争力がつき、製品引渡しに伴うリスクも軽減できる。同様に、MULTOS に常駐するアプリケーションは、所有権に保護された OS やシリコンに依存せず、既製品から調達してもよいし、また、好みのアプリケーション開発者に依頼したり、発行者が自分で開発したりすることもできる。

MULTOS の特長は､アプリケーションの追加や削除をダイナミックにかつ安全に実行できるという点にある。カギを握るのは「アプリケーション証明書（ALC）」と「アプリケーション削除証明書（ADC）」である。この２つの証明書は、MULTOS のカードとアプリケーションに特有のもので、つぎのプロセスで実行される。

１．アプリケーションがカードを認証する。

２．カードがアプリケーションを認証する。

３．アプリケーションがカードに追加されると、アプリケーションのコードとデータが解読される。

４．認証プロセスが実行したこと、そしてアプリケーションとデータが正しく追加されたことをカードが検証する。

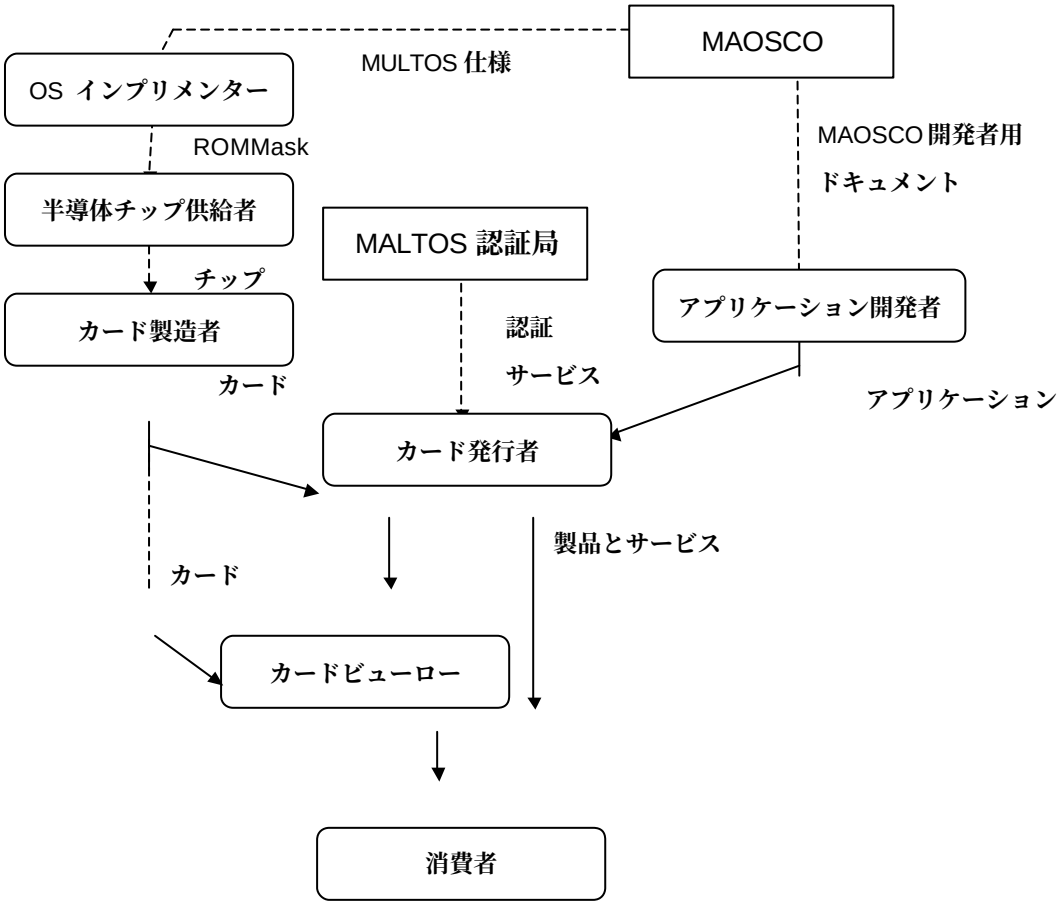


図 1-16 フレームワーク

1.2.2.4 応用事例

(1) **日立製作所社員証**

2000 年 2 月から実施されている接触型 IC「MULTOS」と非接触 IC「Mifare®」を搭載したハイブリッド IC カード。Mondex とクレジットカードによる社用キャッシュレス、ネットワークアクセス管理、入退室等に利用している。大日本印刷（株）は、カードの製造から発行、発送までを行っている。

(2) **マイカルカード**

1999 年 8 月から実施されているマイカルカードはクレジット機能と後払い式電子マネーを搭載した多機能 IC カード。プラットフォームに「MULTOS」を採用したカードでは、実用上世界初の発行となった。大日本印刷（株）はカードの製造、アプリケーションの開発、発行処理までを行なっている。

1.2.3 Windows for Smart Cards for UIM Card Applications

1.2.3.1 機能概要

Windows for Smart Cards は、次世代の IC カードで主流となると思われるマルチアプリケーションに対応した IC カード用の、汎用オペレーティングシステム（OS）で、米国 Microsoft Corporation が提供している。特徴としては、業界標準の各種インターフェース、アプリケーションを装備していることに加え、Windows を中心としたコンピュータ環境との親和性がある。適用が想定される業務領域としては、当文書で中心となる、次世代携帯電話の SIM、UIM カードなどの IC チップ向けの OS としての機能のほか、企業情報システムなどの安全なネットワーク認証、セキュアな企業取引（オンライン バンキング、デビットカード、クレジットカードなど）、住民カードや保健医療情報などの公共情報のデジタル化、電子マネー、双方向デジタル TV のプリペイドカード、カスタマー ロイヤリティ プログラムなどがあり、あらゆる分野での次世代の IC カードに対する汎用 OS として、業界標準を目指している。現在提供されているバージョンは 1.1 で今年夏頃に次バージョンの 1.5 を発表予定である。

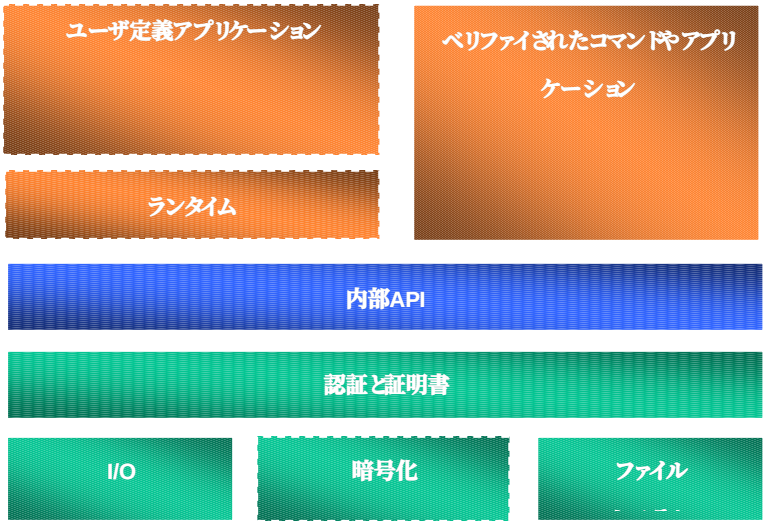


図 1-17 Windows for Smart Cards

1.2.3.2 機能

Windows for Smart Cards は様々な IC カードアプリケーションに対応できるよう柔軟なコンポーネント構造をとっており、**図 1-17** のように、必要に応じて、OS やアプリケーションのコンポーネントを構成できる機能を持っている。また、マルチアプリケーションに必須のアプリケーション間のデータ領域の保護が完備しており、異なる領域のメモリーにはアクセスがブロックされている。ファイルシステムに FAT を採用し柔軟なデータ操作を可能にしている。

(1) ファイル構造

- ■ 階層構造
- ■ FAT ベース
  - ➢ FAT8,12,16
- ■ SEC8,16,32 サポート

■ データ領域としてのファイルは作成、削除、サイズ変更可能。すべてのファイルは ACL(Access Control List)により保護。セキュアなマルチアプリケーション構築が可能

(2) 主な機能

① 選択可能なコマンドセット

必要な機能に応じて、OS にコマンドセットの実装を構成可能。

② PC/SC インターフェース準拠

PC との標準インターフェースに対応、PC へのセキュリティログオン、アプリケーションなどのりソースアクセス制限、電子商取引などのアプリケーション開発が容易に可能。

③ Unicode(16bit)キャラクタ採用

カード内で英語などのシングルバイトキャラクタと日本語のようなダブルバイトキャラクタを混在でき、世界共通のカードの作成が可能。

④ On Card API

カード上でのアプリケーション実行が可能。

⑤ 認証，オーソライゼーション、証明を統合した ISO 7816-4

セキュアなメッセージング接触型 IC カードをサポート、業界標準の認証、証明書をサポート。将来のバージョンでは非接触 IC カードのサポートの予定。

⑥ SIM Card Tookit サポート

GSM 対応の携帯電話の SIM カードのアプリケーション開発用のツールキットがサポート。業界標準のインターフェースも装備。

⑦ 容易な開発を可能にする開発環境

現行バージョンでは開発言語に Visual Basic が次バージョンで Visual C++もサポート予定。Visual Studio6.0 の VB 環境をベースに動作する開発ツール「Windows Smart Card Tookit1.0」が無償で提供中。

（http://www.microsoft.com/japan/smartcard/）

⑧ 金融アプリケーションのサポート（次バージョン）

Europay Mastercard Visa (EMV '96 3.1.1)

Third party application availability:

Proton/CEPS

VSDC

M/Chip

Visa Open Platform support

Visa Level 1 Certification

Global Platform 2.0.1 + Annex B extensions

サポートされている H/W スペック、コマンドの一覧は下記の通りである。

表 1-1 機能一覧

Windows for Smart Cards　機能一覧(Version1.1)	
プロトコル/通信	
ＡＴＲ　　ＴＳ	0x3F/0x3B
Historical Byte **数**	**最大** 15 **バイト**
外部クロック最大値	
ボーレート	9600bps **以上**
ＡＴＲ　TD(I) T=15	Class A
プロトコル	T=0/T=1
T=0　**拡張** LE	**将来対応予定**
拡張 LC	**将来対応予定**
応答延長要求	**対応**
T=1　**拡張** LE	**将来対応予定**
拡張 LC	**将来対応予定**
応答延長要求	**対応**
IFSC **のサイズ**	0x10 - 0xFE
チェイニング	**対応**
SAD=0 DAD=0	**以外にも対応**
PPS（PTS）**対応**	**対応**
デュアル ATR **（ウォームリセット）**	**対応**
マルチアプリ	
アプリケーション選択方法	ISO7816 **規定の方法**
コマンド一覧	
	READ BINARY
	WRITE BINARY
	UPDATE BINARY
	VERIFY
	INTERNAL AUTHENTICATE
	EXTERNAL AUTHENTICATE
	GET CHALLENGE
	WRITE FILE

	SELECT FILE READ RECORD WRITE RECORD UPDATE RECORD APPEND RECORD 他に GSM11.11/GSM11.14 をサポート

1.2.3.3 SIM, UIM カードサポート

Windows for Smart Cards では次世代携帯電話をターゲットとした、SIM カード、UIM カードのサポートを行っており、現行バージョンでは GSM に対応した機能を実現している。

- ESTI スタンダード：SIM Toolskit API for GSM
- Windows PKI
- SSL サポート
- PC 上での Phone Simulator(PC 上で、携帯電話アプリケーションのシュミレーションが可能)
- 開発言語として Visual Basic, Visual C++(次バージョン)のサポート
- インターネットアプリケーション、メールアプリケーション、グループスケジュールアプリケーションのためのサーバー連携の機能のサポート
  - SIM Outlook
  - SIM Explorer
  - 携帯電話向け WAP/cHTML ブラウザとの連携（Microsoft Mobile Explorer）

1.2.3.4 開発環境

開発者が使い慣れている特定言語に依存しないランタイム環境や Microsoft Visual Basic(R) 開発システムなどの認知度の高いツール、さらにそれらの言語を利用した専用の開発ツールである Windows Smart Card Toolkit を無料で提供しており、これまでコンピュータの世界で培った Windows 向け開発モデルの利点を最大限に拡大できる。これにより、カード発行会社や Windows プログラマーは、既存の専門知識を生かして、既存の IC カード/スマートカードのプラットフォームを利用した場合と比べてより広範なスマートカードソリューションやアプリケーションを低コストで容易に開発、導入することが可能にしている。

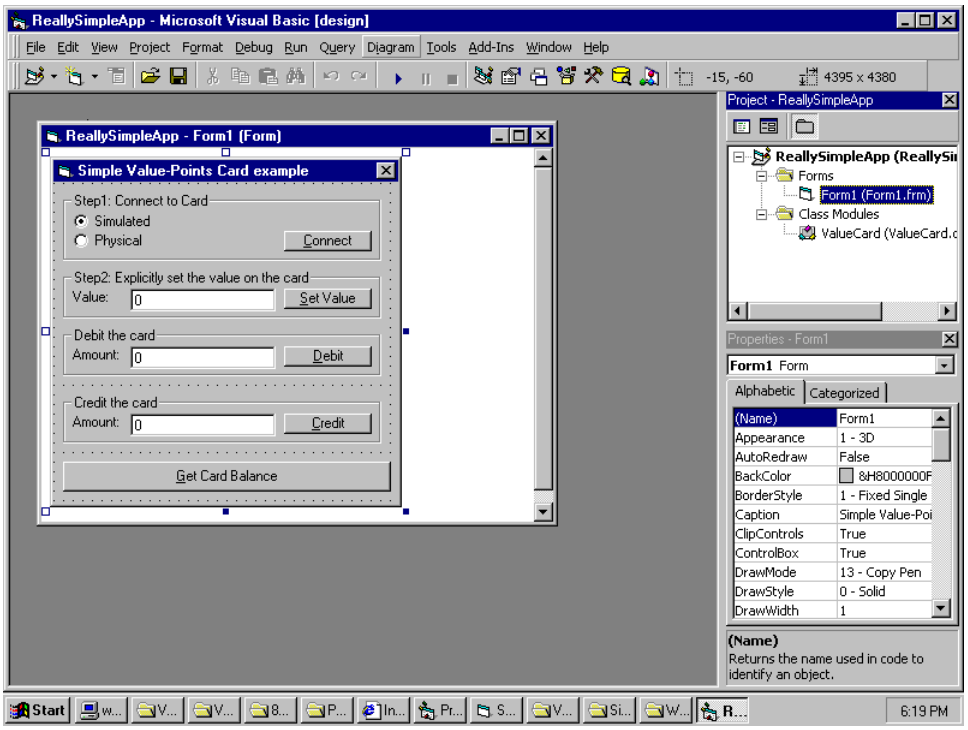


図 1-18 アプリケーション開発環境例

(1) 主な機能

- OS の構成ウィザード-PC 上でのシュミレーション、繰り返しのダウンロード、テストが可能
- アプリケーションが容易に開発、デバッグ、ソリューションの実装が可能
- 開発言語として VB、 C が選択可能
- シュミレーターとデバッガ装備
- コストと必要とされるパフォーマンスに沿ってＯＳをファイルシステムをカスタマイズが可能
- 豊富なサンプルアプリケーション

1.2.3.5 スマートフォンサポート

SIM，UIM カードの OS とあわせて、IMT-2000 以降の次世代のスマートフォン(多機能携帯電話)へのサポートとして、さらに携帯電話のサービスが高度化することを予測し、現在高機能型の PDA（パーソナルデジタルアシスタント：携帯情報端末）などで実現している WEB ブラウジング、マルチメディア機能、電子メール機能、スケジュール機能、などと携帯電話を統合し、次世代のワイドバンドに対応した機能を実現する次世代スマートフォンプラットホーム“ Stinger”を開発中である。すでに、2001 年春以降に欧州市場の GSM, GPRS 向けに Sendo,三菱電機、サムソンなどが複数のメーカーの端末が開発意向表明や製品の発

表を行っておいる。今後日本でも W-CDMA.,CDMA2000 のサポートも視野に入れて投入予定である。

SIM、UIM のサポートとしては現行の欧州向けバージョンで、GSM で規定されている SIM の機能をサポートしている。

また実装方法として、無線プロトコルの抽象化レイヤー上に SIM Manager コンポーネントと API(Spec 11.14 規定の仕様を実装)を実装し、これらの API を利用することによりアプリケーションを構築するという手法を実現している。これら API はマイクロソフトが独自に規定しているものではなく、あくまで GSM の仕様を実装しているにすぎない。また、これらの SIM　Manager の機能はコンポーネント化されており、今後の SIM 仕様の拡張および UIM 仕様にも柔軟に対応する事が可能である。

1.2.3.6　サーバーとの連携

マイクロソフトでは、Short Message Service(SMS)をサポートするゲートウェイサービスの提供も計画している。サポートを予定しているプロトコルは SMPP, UCP, CIMD2, SMTP などで、企業情報システムで構築されている、メールサーバーとの連携や、他アプリケーションとの連携、モバイルアプリケーション、アプレットなどのダウンロードなどの機能の実現をサポートする。また、企業サーバーからのプッシュ型のメッセージ送信やデバイスの管理を可能にするサーバーも計画しており、暗号化された Phone Applet などの SIM カードへの送信なども可能にする計画である。

1.2.4　AP ダウンロード・管理・チップ間連携（SIM Tool Kit 等）機能

携帯電話端末に搭載する IC チップ上で動作するアプリケーションのダウンロード、管理、2nd チップ間連携の仕様について以下に記述する。

なお、3GPP では、現在 SMS を利用する形態のみが規定されており、それ以外の形態については議論中の段階にある。

1.2.4.1　技術概要

(1) USAT アプリケーションダウンロード概要

3GPP での IC カード用アプリケーション(USAT)仕様は、3GPP TS31.111 V4.1.0 (2000-12) : USIM Application Toolkit (USAT) に規定されている。

- 3GPP では、通信用 IC チップを UICC (USIM Integrated Circuit Card) と呼んでいる。
- UICC へのデータダウンロードは、ENVELOPE コマンドによって行われる。
- ENVELOPE コマンドは、UICC と携帯電話端末間のインタフェース仕様書で規定されている。

ネットワークからユーザの UICC へ、アプリケーションをダウンロードするには、SMS-PP と SMS-CB の 2 つの方式がある（図 1-19 参照）。

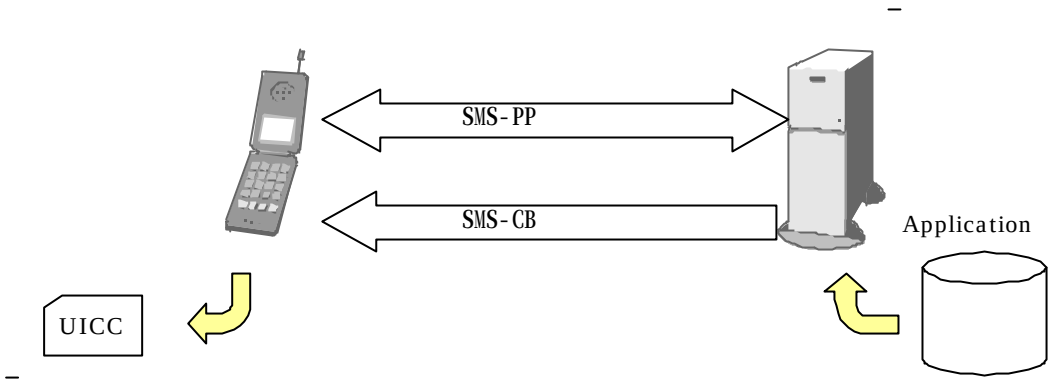


図 1-19 ネットワークからUICC へのアプリケーションダウンロード方式

- SMS-PP:3GPP TS23.040: Technical realization of the Short Message Service (SMS) Point-to-Point (PP)
- SMS-CB:3GPP TS23.041:Technical realization of Short Message Service Cell Broadcast

(2) SMS-PP（ショートメッセージ ポイント－ツウ－ポイント）方式

携帯電話端末は、SMS-PP データダウンロード機能を保有していることが必要になる。このデータダウンロード機能の保有状態は、ターミナルプロファイル情報として UICC Service Table に存在する。

- 携帯電話端末は、ネットワークから SIM データダウンロード識別が付与された SMS を受信する。
- 受信後、データダウンロード用メッセージを UICC に転送する。転送には、ENVELOPE（SMS-PP DOWNLOAD）コマンドを用いる。
- 携帯電話端末は、UICC から正常終了の応答を受けて、ネットワークに対し RP-ACK メッセージを送信する。

下図に、SMS-PP 方式のダウンロードシーケンスを記述する。

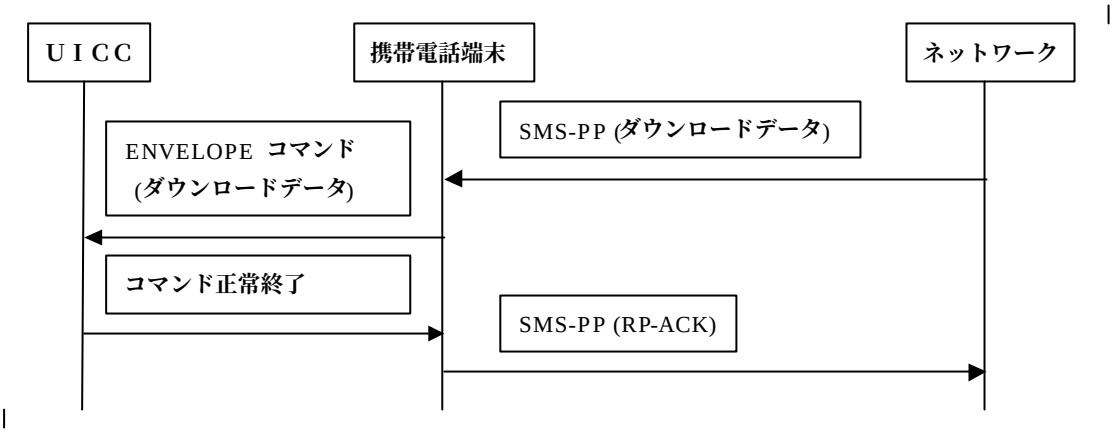


図 1-20 SMS-PP 方式のダウンロードシーケンス

ダウンロード情報には、次のような項目がある。

- SMS-PP ダウンロードタグ
- 情報長
- デバイス識別 （ネットワーク もしくは UICC）
- アドレス （サービスセンタアドレス）
- ダウンロードデータ

(3) SMS-CB（ショートメッセージ セルブロードキャスト）方式

携帯電話端末は、SMS-CB データダウンロード機能を保有していることが必要になる。このデータダウンロード機能の保有状態は、ターミナルプロファイル情報として UICC Service Table に存在する。

(a)携帯電話端末は、ネットワークから CBMID（セル識別番号）が付与された SMS を受信する。

(b)受信後、UICC 内に記録してある CBMID と送られてきた CBMID を比較し、同一の時に、SMS メッセージを UICC に転送する。

(c) UICC への転送には ENVELOPE (CELL BROADCAST DOWNLOAD)コマンドを用いる。SMS-CB 方式の場合、ネットワークへの ACK メッセージは送信しない。

下図に、SMS-CB 方式のダウンロードシーケンスを記述する。

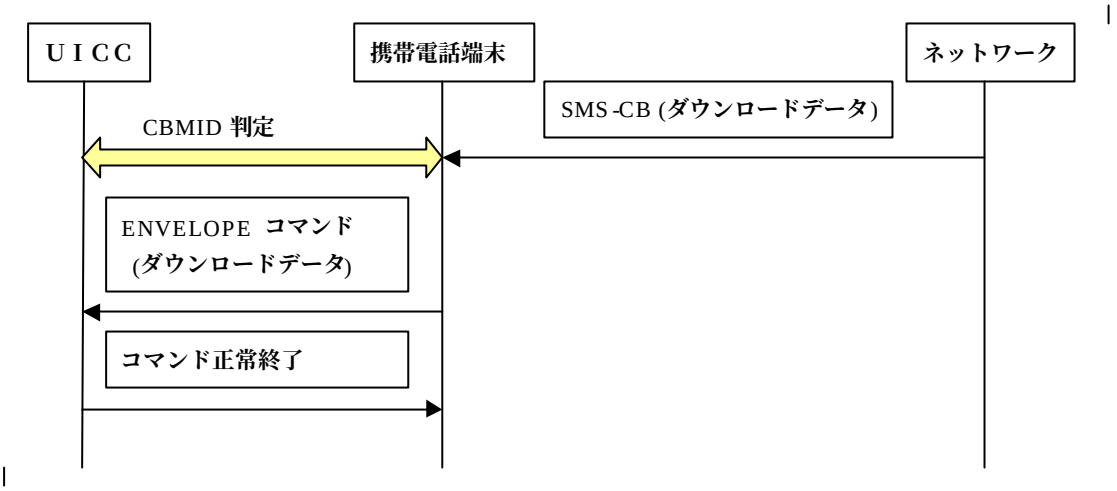


図 1-21 SMS-CB 方式のダウンロードシーケンス

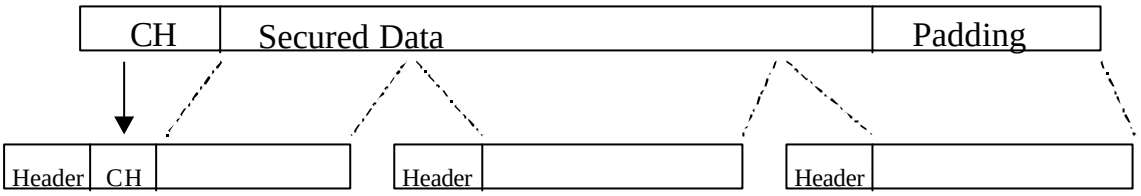
ダウンロード情報には、次のような項目がある。

- Cell Broadcast ダウンロードタグ
- 情報長
- デバイス識別 （ネットワーク もしくは UICC）
- アドレス （サービスセンタアドレス）
- ダウンロードデータ

(4) アプリケーション転送セキュリティ

USAT アプリケーション転送セキュリティ仕様は、3GPP TS 03.48 V8.4.0 (2000-10) : Security Mechanisms for the SIM application toolkit Stage 2 (Release 1999) に規定されている。

アプリケーションデータは、TS 03.48 に規定されているセキュリティメカニズムにより、サービスセンタからユーザの UICC にダウンロードされる。アプリケーションデータは暗合化（例：DES）され、コマンドヘッダを付与されたものが、さらに SMS のデータサイズに分割され、ユーザの UICC に転送される。（**図 1-22** 参照）



First SMS in the sequence　　Second SMS page　　Third and final SMS page

CH = Command Header

図 1-22 SMS を用いた USAT アプリケーションの転送フォーマット

(5) **リモートアプリケーション管理**

USAT アプリケーションの運用（ダウンロード、インストール、削除）は、USIM の管理者であるネットワークオペレータもしくはサービスプロバイダによって管理される。

① **アプリケーションデータのダウンロード**

新たな USIM アプリケーションを UICC にダウンロードする場合、ローディングセッションと呼ばれる流れにより処理される。（**図 1-23 参照**）

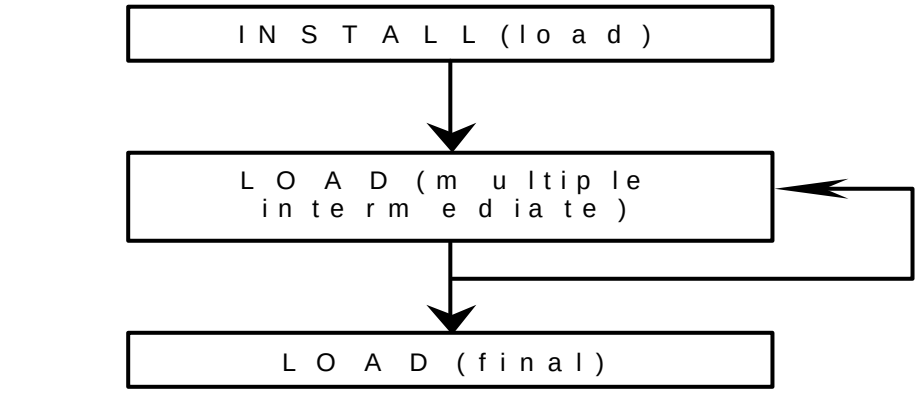


図 1-23 ローディングセッションのシーケンス

② **アプリケーションのインストール**

アプリケーションのインストールは、UICC へのダウンロード完了後、ネットワークオペレータまたはサービスプロバイダからの INSTALL(install) コマンドにより実行される。

③ アプリケーションの削除

アプリケーションの削除は、ネットワークオペレータまたはサービスプロバイダからの DELETE コマンドにより実行される。

④ アプリケーションのロック／ロック解除

アプリケーションのロック／ロック解除は、ネットワークオペレータまたはサービスプロバイダからの SET STATUS コマンドにより制御される。

ロック状態のアプリケーションは、ユーザにより起動できない（メニュー選択しても起動しない、もしくは、選択メニュー上にアプリケーションが表示されない）状態である。

(6) アプリケーション動作規定

USAT アプリケーションの動作仕様は、ETSI TS 102 221 V4.1.0(2001-02) : Smart cards, UICC-Terminal interface, Physical and logical characteristics (Release 4) に規定されている。

① USAT 初期動作

USAT を提供している携帯電話端末は、UICC に対して TERMINAL PROFILE C-APDU コマンドを送信する。

USAT 機能のある UICC は、携帯電話端末に対して正常応答を返信する。

② アプリケーション動作

SAT アプリケーションと USAT の動作は、論理的に独立する。

USAT アプリケーションより発行されるコマンド／レスポンスの対と、USIM データ操作のコマンド／レスポンスの対は、同時に発生することがあり、それぞれ独立に管理される。

1.2.5 標準化状況

1.2.5.1 3GPP TSG-T WG3 / ETSI SCP

モバイル通信システム用の IC カードの共通プラットフォームを構築する目的で ETSI SCP が結成され、コマンド仕様、セキュリティ機能が議論されている。

2001 年現在のテーマは、「全てのモバイル通信システム用の IC カードの共通プラットフォーム仕様の作成」および「モバイルコマース等に向けた通信アプリケーションの拡張セキュリティ機能の IC カード標準仕様の作成」である。

1.3　提供形態等の運用上のルール等の制約条件

1.3.1　GSM における SIM の提供形態

GSM における SIM の提供形態の現状を調査した結果、調査対象事業者では殆どが HW は事業者が貸与していることが判明した。具体的には、以下の状況である。

表 1-2 SIM の提供形態

電話会社	国	SIMの提供形態	解約時返却義務	その他
Hutchison Telephone	香港	Hutchison Telephone からの貸与	―	Rechargeable Stored Value SIM
Cable & Wireless	香港	Cable & Wireless からの貸与	あり	
Mandarin Communications	香港	Mandarin Communications からの貸与	あり	
Singapore Telecom	シンガポール	Singapore Telecom からの貸与	あり（30日以内）	
Hutchison Telecom	ドイツ	Hutchison Telecom からの貸与	あり（14日以内）	
One2One	英国	One2Oneからの貸与	なし	
France Telecom	フランス	明記なし	あり	返却例は少ない（システムで対応）

1.3.2　その他の動向

1.3.2.1　カードブランド選択

電子商取引において、IC カードや各種の端末上に異なるカードブランドのアプリケーションを搭載した場合、決済時に店舗の契約するカードブランドとユーザの保有するカードブランドとのマッチングを行ったうえで合致したブランドのアプリケーションを選択する必要がある。ここではクローズド環境における応用に対してのカードブランド選択の事例を扱う。なお、ここでクローズド環境とは、利用者（IC カード・PC/Wallet）と店舗端末・店舗サーバ間における一連の処理のための環境を言う。

当該の一連処理につき、通常の IC カード（EMV）利用時、SET 利用時および chip EC 利用時を参考に実施フローを検討する。

(1) **IC カード（EMV）リアル利用時のブランド選択フロー**

店舗端末側より自己の決済可能なブランドをカード側に提示し、カードに搭載されているブランド（AP）と一致したブランド（AP）を店舗にて選択し、決済処理を行う。

※詳細は EMV 仕様書を参照のこと。

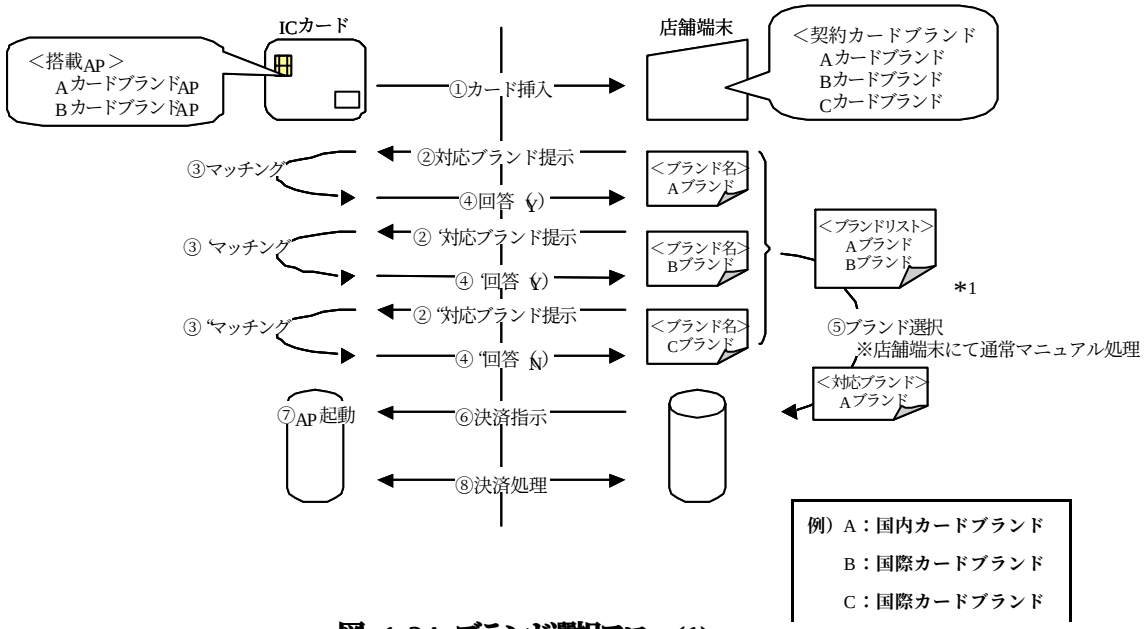


図 1-24 ブランド選択フロー(1)

*1 ⑤ブランド選択：店舗端末において、クレジットアプリの場合は自動選択、それ以外の場合はマニュアル選択となる。

(2) SET Secure Electronic Transaction **利用時のブランド選択フロー**

店舗サーバ側より自己の決済可能な全ブランドを PC/wallet ソフトに提示し、マッチングしたブランド（証明書）を<u>ユーザが選択し、決済処理を行う。</u>

※詳細は SET 仕様書を参照のこと。（Book2，External Interface Guide 等）

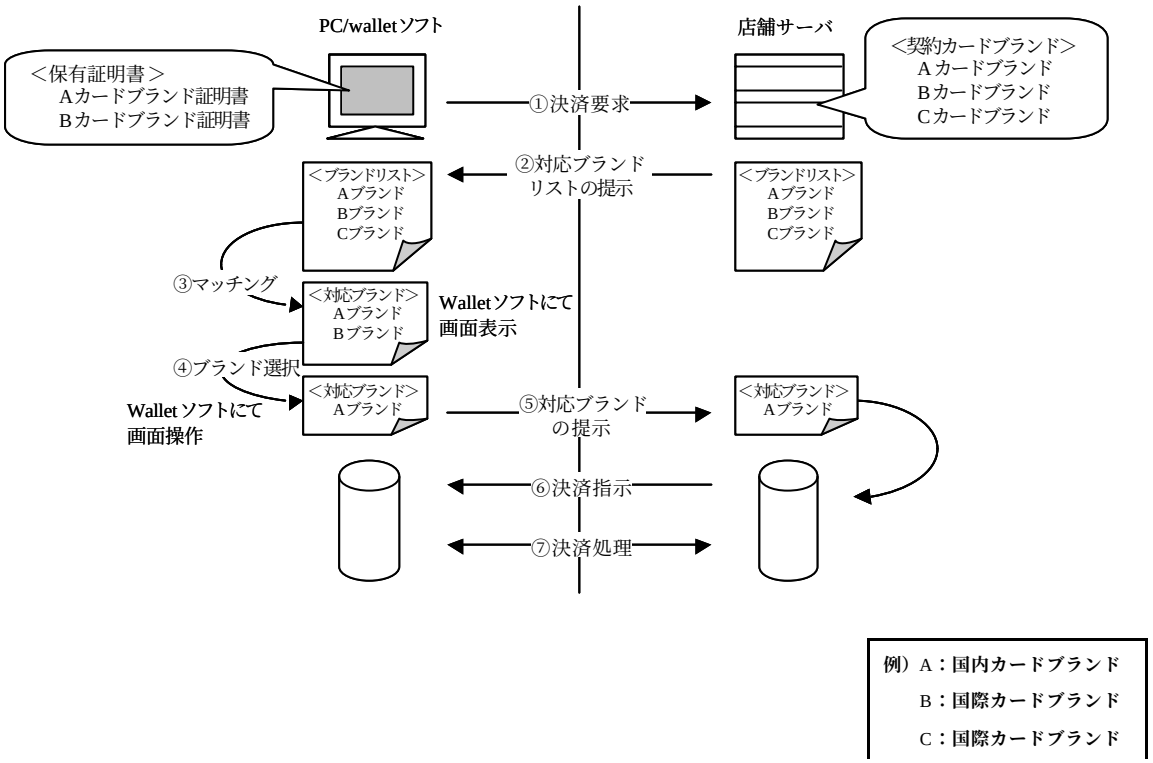


図 1-25 ブランド選択フロー(2)

(3) chip EC 利用時のブランド選択フロー

EMVCo，SETCo にて仕様化されている chip EC（Common Chip extension）を利用した場合。

※詳細は EMVCo，SETCo，GMCIG 等の仕様書・関連資料を参照のこと。

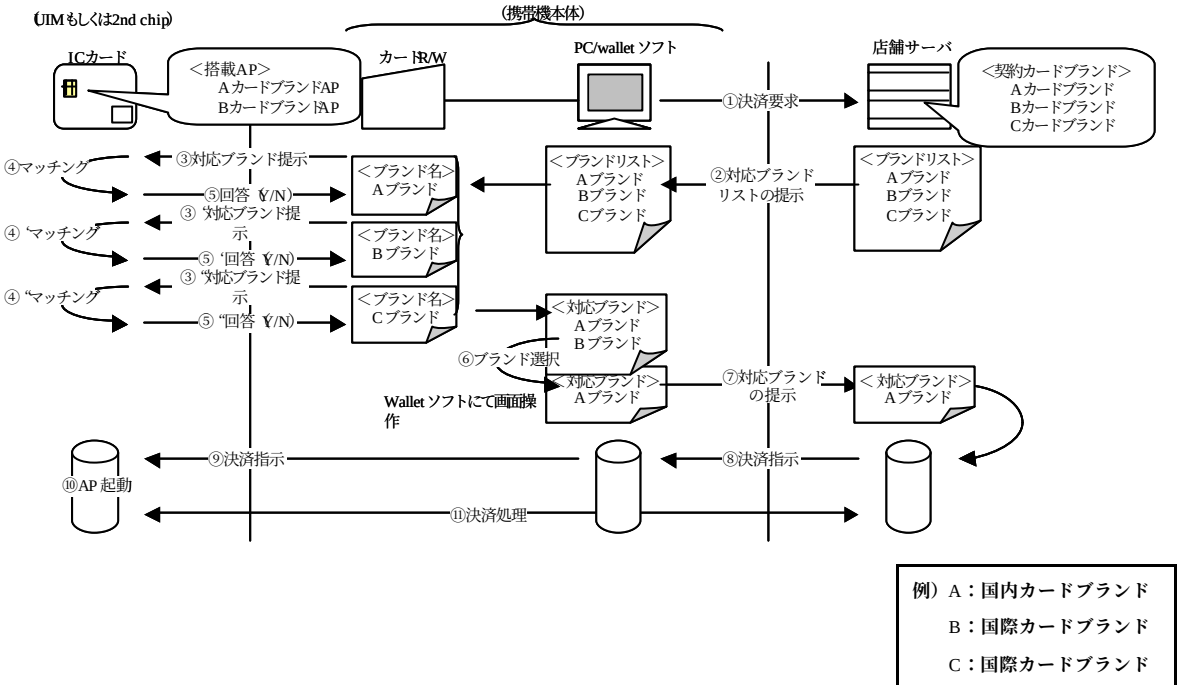


図 1-26 ブランド選択フロー(3)

1.3.2.2　多目的 IC カード標準仕様

なお、IC カードでの多目的チップの状況については、日本における公共的利用などを中心としたマルチアプリケーション IC カードの検討事例として、ニューメディア開発協会がＩＣカードシステムの標準仕様を作成し、セキュリティ、拡張性、開発容易性等の課題や、従来のカードとの上位互換性を確保する諸機能の体系化を行ったものがある。

この「共通コマンド仕様書」は、ＩＳＯ、ＪＩＣＳＡＰ仕様、ＥＭＶ仕様などの既存の業界標準仕様との互換性を確保した上で､カード内にファイル構造を構築するための発行コマンド、および署名作成・検証、セキュアメッセージング機能などのセキュリティ機能を国際規格と整合性を図りながら仕様としてまとめた。

なお「カードプラットフォーム仕様書」は、共通コマンド機能の活用や、複数のアプリケーションプログラムのダウンロード機能等のカードプラットフォームの仕様をとりまとめている。また､開発者向けにカードプラットフォームをＰＣ上で擬似可能な参照実装（リファレンス・インプリメンテーション）を開発し、相互運用性の向上を図った。

また「近接型通信インタフェース実装規約」ではＩＳＯ/ＩＥＣ１４４４３　に補足すべき仕様、およびその試験方法を定義し､近接型ＩＣカードとリーダライタの互換性の向上を図った。上記技術開発において実施した実装規約検討作業の成果をとりまとめている。

上記の他に、金融やクレジット等の分野においても、2001 年度からマルチアプリケーション IC カードの導入が予定されている。

1.3.3　関連主管庁との連携の必要性

今後、モバイルコマース分野において、日本が世界のリーディングエッジを担ってゆくためには、関連省庁とも十分に連携した取り組みが必要である。この点に関しては、今後の検討課題と考えられる。

1.4　利用者関連：認証に関わる IC チップ関連事項

携帯電話を財布代わりに使うモバイルコマースでは、これまでの PC を用いたコマースに比べて、端末の紛失・盗難等の問題が加わることから、より一層利用者個人の認証が重要になってくる。

ここでは、このような観点から、現在、検討が進められている、携帯電話に搭載を想定された、IC チップに関連する認証系の技術動向について整理した。

1.4.1　IMT-2000 における加入者認証技術

IMT2000 には、標準化組織３GPP によって標準化が推進されている UMTS (Universal Mobile Telecomunications System) または W-CDMA(Wideband　CDMA)と、３GPP２によって標準化が推進されている Cdma2000 の２つの方式があり、各々について、USIM

（Universal Subscriber Identity Module）及び UIM（User Identity Module）とネットワークとの認証技術として規定されている。本節では、これらの内容について説明する。

先ず、UMTS／W-CDMA と Cdma2000 での認証技術の特徴を以下の表に纏めた。

表 1-3 セキュリティメカニズム上の特徴

機能	W-CDMA	Cdma2000 ＊
ユーザ（端末）認証	• NW と端末（UIM）の相互認証：認証ベクタ方式 • パーマネントID／テンポラリ ID（位置登録エリア内） • 端末（UIM）移動に伴うMSC 間認証情報引継ぎ • 認証用の同期がとれなくなった場合には再認証 • 通信時の端末（UIM）～無線ネットワークローカル認証	• NW と端末（UIM）の相互認証：SSD 方式 • パーマネントID／テンポラリ ID（位置登録エリア内） • GCR:位置登録、発着信時に RAN 乱数による端末（UIM）認証（位置登録エリア内） UCR:GCR 失敗時、通信時に HN 乱数による端末（UIM）認証 GCR : Global Challenge Response UCR : Unique Challenge Response
データ秘匿	・KASUMI	・ストリーム暗号
完全性保証	・KASUMI	・なし

＊認証、鍵生成メカニズムを総称して CAVE(Cellular authentication and voice encryption)と称するが、詳細は米国政府管理下にあり、一般には非公開である。

1.4.1.1 UMTS/W-CDMA での認証手順

ネットワークが端末を認証するために、認証鍵（K）と呼ばれる情報が用いられる。認証鍵は個々の端末（MS＋UIM）に書き込まれており、これと同一の鍵値がホームネットワークの HLR にも記録されている。認証鍵はまた、無線区間の通信データを暗号化するための暗号鍵を生成するためにも用いられる。

認証鍵は、無線区間と有線区間とを問わず、制御信号に載せて転送されることはない。そこで、端末の認証と暗号鍵の生成は次のような手順で行われる。

（ｉ）在圏ネットワークの VLR（または SGSN）は、端末（UIM）認証に用いる「認証ベクタ」を、あらかじめホームネットワークの HLR から複数個まとめて取り寄せておく。UMTS 用の認証ベクタは Quintet (Q)と呼ばれ、次の 5 つの情報が含まれる。

・認証乱数：RAND（ホームネットワークで生成したもの）

・認証演算結果：XRES（認証鍵と RAND から認証演算アルゴリズムで導出）
・暗号鍵：CK（同じく暗号鍵生成アルゴリズムで導出）
・完全性鍵：IK（同じく完全性鍵生成アルゴリズムで導出）
・認証トークン：AUTN（認証鍵と RAND とシーケンス番号 SQN から導出）
（ちなみに GSM 用の認証ベクタは Triplet (T)と呼ばれ、最初の 3 つの情報を含む）

（ii）端末（UIM）の認証動作が必要になると、在圏ネットワークは VLR 上に蓄積された認証ベクタの 1 つを選び、RAND と AUTN を無線経由で端末（USIM）へ送る。

（iii）USIM は AUTN から SQN を復元してその値を検証した後、自身が持つ認証鍵およびネットワークから受信した RAND を認証演算アルゴリズムに入力し、得られた演算結果 RES を無線経由でネットワークへ返送する。

（iv）在圏ネットワークは USIM から受信した RES と認証ベクタ内の XRES とを照合し、同一値であれば認証成功と見なして、認証ベクタ内の CK と IK を保持する。これらは通信時の暗号化に用いられる。なお、一度認証に使った認証ベクタは廃棄される。

（v）USIM は認証鍵と RAND をもとに CK と IK を生成する。

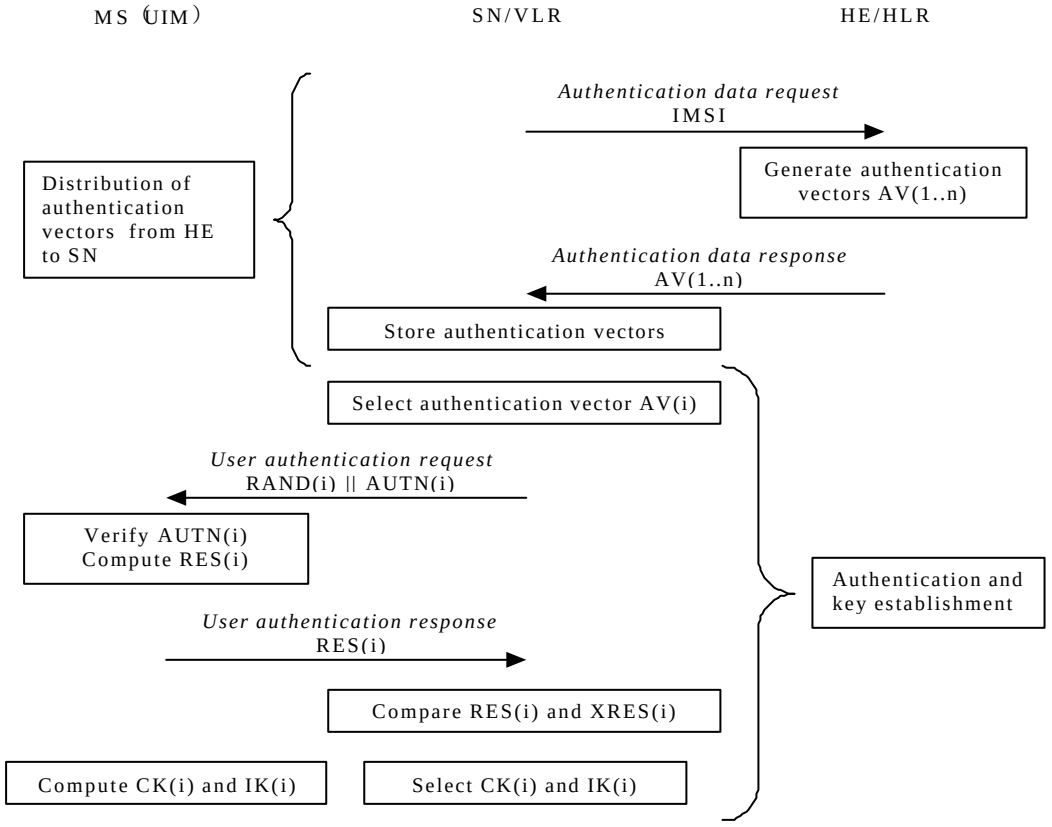


図 1-27 Authentication and key agreement

（3G TS 33.102 の Figure 5 より）

1.4.1.2 cdma2000 の認証手順

(1) Shared Secret Data の使用

端末（UIM）の認証には、端末（UIM）ごとの認証鍵（A-key）を直接使用するのではなく、代わりに Shared Secret Data（SSD）と呼ばれるデータを用いる。SSD は認証キーと SSD 生成用乱数（RANDSSD）を、SSD 生成アルゴリズムに入力することによって得られる。

RANDSSD はホームネットワークの認証センタ（AC）で生成され、在圏ネットワークを介して端末（UIM）へ送られる。認証センタと端末（UIM）の両者は認証鍵と RANDSSD を用いて SSD を生成し、これを記憶する。

SSD は 128 ビット長のデータである。このうち上位 64 ビットを SSD_A と呼び、認証手順に使用する。また下位 64 ビットを SSD_B と呼び、暗号化マスクや private long code を生成するための入力の一部として使用する。

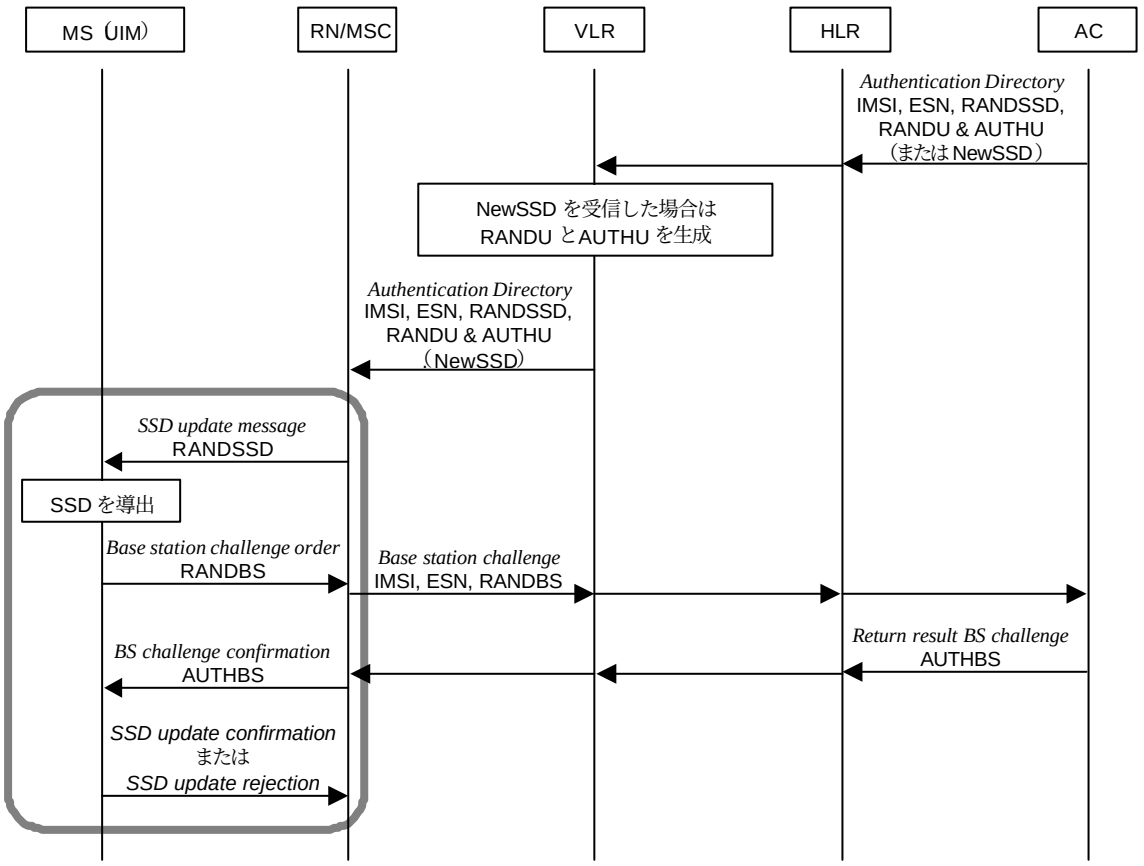


図 1-28_SSD の生成･更新手順

なお、ネットワーク機能のオプションとして、SSD そのものを認証センタから VLR へコピーすることもできる。この場合、VLR は認証センタの代理として動作する。

上記の SSD を用いて、次の 2 通りの認証手順が準備されている。

(2) Global Challenge-Response

在圏ネットワークは、すべての基地局（MS）から常時、32 ビット長の認証乱数（RAND）を放送形式で送出している。

位置登録、発信、着信などの際に、端末はこの RAND と SSD を基に認証演算を行い、ネットワークへ送信する最初の制御信号上に、認証演算結果を載せて送信する。

認証演算結果は、認証センタ（あるいは SSD を保持する VLR）において照合される。

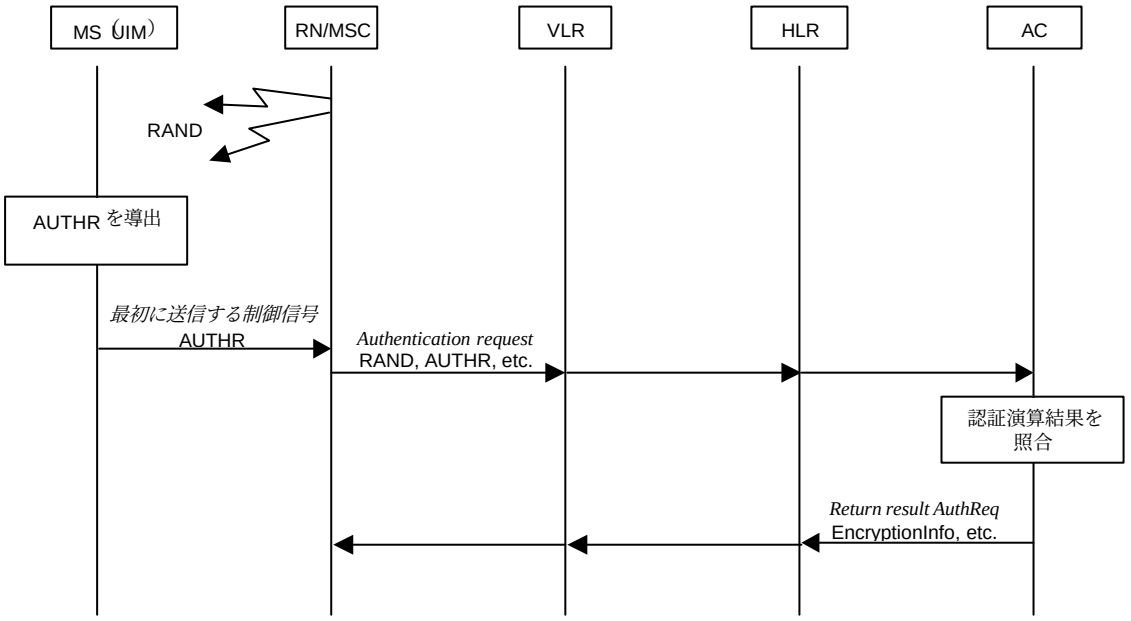


図 1-29 Global Challenge-Response

(3) Unique Challenge-Response

ネットワークは、上述の Global Challenge-Response とは別に、特定の端末（UIM）に対する認証を実行することができる。例えば次のような場合の実行が想定されている。

・Global Challenge-Response が失敗した場合

・通話中認証を行う場合

Unique Challenge-Response では、ネットワークが生成した 24 ビット長の認証乱数（RANDU）と、IMSI から導出された 8 ビットのデータ（IMSI_S2）を結合して、32 ビット長の乱数として用いる。

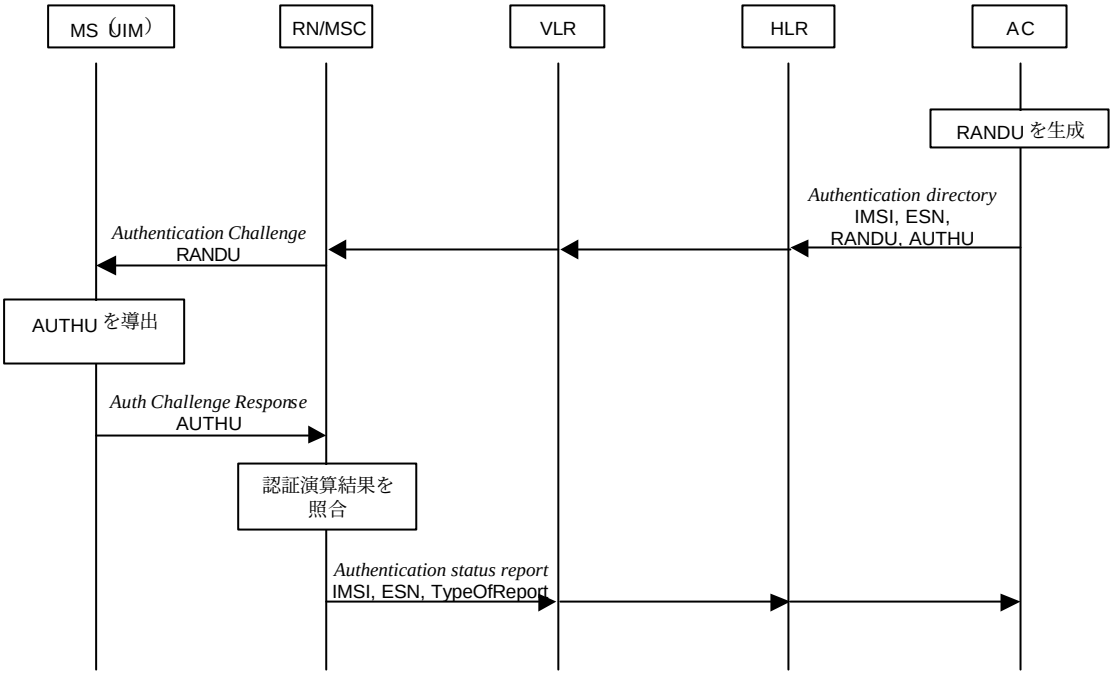


図 1-30 Unique Challenge-Response

1.4.2 WIM （WAP Identity Module）

WIM は WAP Identity Module の略であり、WAP で規定されているクライアント端末の Identity Module である。WIM は耐タンパデバイスであり、WAP のセキュリティレイヤーの実装や、アプリケーションレイヤーの機能のセキュリティを高めるために使用される。

WIM の機能は、スマートカード上で実現することが可能であり、また、WIM は、一つの独立したスマートカードアプリケーションとして定義できる。WIM だけが搭載されたカードとして、又は、マルチアプリケーションカードのアプリケーションの一つとして実装することができる。したがって、GSM SIM と共に、一つのスマートカードモジュール上に実装することも可能である。

WIM の機能は大きく分けて以下の２つがある。

- WTLS Operations
  WTLS※のセッション確立の際のハンドシェイクやユーザ認証の際のクライアント側の暗号処理
- WAP Application Security Operations
  デジタル署名や暗号鍵の復号化などのアプリケーションレベルのセキュリティ処理

※WTLS：Wireless Transport Layer Security の略であり、WAP の暗号通信プロトコル。

パソコンにおける SSL に相当する。

また、これらの機能を実現するため、WIM には、公開鍵暗号方式の秘密鍵と公開鍵の鍵ペアが、WTLS の認証用とデジタル署名用に、それぞれ、１組ずつ格納される。（１組以上の鍵が格納されていても良い。）これらの処理は、耐タンパデバイスである WIM の中で行われるため、高いセキュリティが実現される。

1.4.3 ＷＰＫＩ

WPKI は、既存の PKI モデルをベースにした WAP 環境における PKI モデルに関する仕様であり、現在、WAP フォーラムにおいて、標準化が進めされている。

WPKI によって、WAP 環境において以下のような機能が実現される。

- WTLS のセッション確立の際のサーバ認証
- WTLS のセッション確立の際のクライアント認証
- デジタル署名／署名検証
- CA 証明書のオーバー・ザ・エアーでの取得
- クライアント証明書のオーバー・ザ・エアーでの取得

既存の PKI モデルとの違いとしては、通信環境として、WAP 環境を想定している以外に、クライアント側に格納されるクライアント証明書のデータ形式として、X.509 等の他に Certificate URL という形式を認めている点がある。これは、CA に登録されているクライアント証明書の URL であり、この形式でクライアント証明書を管理することにより、クライアント側に必要とされるメモリを削減することができる。

1.4.3.1 MeT における WIM と WPKI

MeT(Mobile Electronic Transactions)は、携帯電話での E コマース機能の標準化とその促進を目的とする団体であり、現在、ノキア、エリクソン、モトローラ、シーメンス、松下通信工業、ソニーがスポンサー企業となっている。MeT と ECOM の間では、２００１年５月に、東京において、コンタクト・ミーティングが行われる予定である。

MeT において、WIM と WPKI は、WTLS や signText と共に重要なセキュリティ技術の一つであり、MeT では、これらの機能を備えた携帯電話を、バンキングや電子決済、チケッティングといった各種の新しいサービスやアプリケーションを扱う能力を備えたデバイスとして、PTD(Personal Trusted Device)として定義しており、ユーザはクライアント端末として、PTD を使用することを想定している。ただし、MeT では、PTD が備えるセキュリティ・モジュールを SE(Security Element)と定義しており、WIM は、その SE の実現形態の一つとしている。

PTD は、サーバ側との相互認証を伴うセキュア通信の機能と、デジタル署名の機能を備

えており、これらの機能により、安全性の高い、E コマースサービスが実現されるとしている。

1.4.3.2　MeT の口座決済のシナリオ（ＰＫＩ技術応用例）

MeT の仕様に基づく、具体的な E コマース機能の一例として、クレジットカード決済に代表される口座決済(Account-Based Payment)のシナリオを以下に示す。

①PTD とマーチャント間での、WTLS による相互認証に伴うセキュアセッションが確立以降、両者間でセキュア通信が行われる。
②ブラウジングによる商品の選択
③マーチャントから PTD に（売買）契約書を送信
④PTD に（売買）契約書が表示される
⑤ユーザは支払口座を選択
⑥PIN の入力
⑦選択された支払口座に対応する秘密鍵によって、（売買）契約書にデジタル署名
※ SE(e.g. WIM)の中でデジタル署名が行われる
⑧デジタル署名された（売買）契約書をマーチャントに送信
⑨Acquirer を介し、Issuer においてデジタル署名を検証
⑩領収書を PTD に送信して、決済を完了

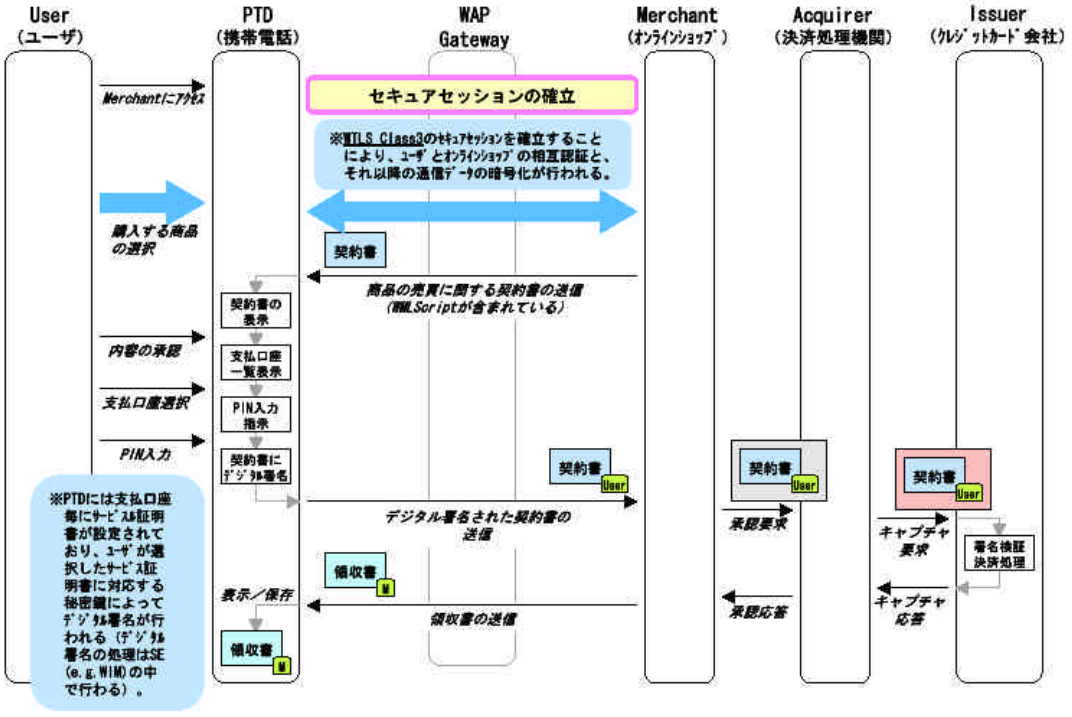


図 1-31 Account-Based Payment のシナリオ

1.4.4　バイオメトリクス認証

モバイル EC におけるサーバ側から見た認証では、端末を特定するための端末認証と端末を操作する人物を特定するための個人認証とが存在する。本資料で主に述べている IC チップにおける認証とは、サーバ－端末間の認証であり、ここでいう端末認証にあたる。これに対して、個人認証は、現在のモバイル EC では、ユーザ ID および PIN コードの入力などでおこなわれているのが現状である。

ユーザ ID および PIN コードによる個人認証は、利用者の記憶に頼るため忘れるという問題点、他人に知られる危険性が高いという問題点がある。

これに対して、いわゆるバイオメトリクス照合は利用者本人の身体的特徴などを照合の対象とするので、これを個人認証に利用すれば、これらの問題が解消される。

従って、モバイル EC に関わる認証にも、個人認証を確実におこなうことの出来るバイオメトリクス認証が導入されることが期待される。本章では、バイオメトリクス認証についてそのモバイル EC への適用について述べるものである。

1.4.4.1　バイオメトリクスの主な方式と特徴

現在、研究もしくは実用化されているバイオメトリクス認証について、主な方式を挙げて、その特徴等について比較する。

以下に幾つかのバイオメトリクス認証に用いる方式とその特徴を挙げる。

表 1-4 バイオメトリクス認証方式と特徴

方式		方式の説明と課題
指紋		特徴点照合： 指紋にある特徴的な情報、例えば指紋を構成する隆線の特徴点（端点や分岐点）、更に特徴点間の隆線の数などをとらえ、これらの情報から判別する方式
		パターンマッチング： 指紋を画像として取り込み、画像同士を重ね合わせて照合をおこなう方式 （課題は別途記述）
目	網膜	眼底の毛細血管の模様を用いる方式。 （認証精度は高いとされるが、センサ部を覗き込み、目の奥まで光を当てられるという動作にユーザが抵抗感を感じたり、慣れが必要であるなどの制約がある。）

	虹彩（アイリス）	瞳孔の外側にある虹彩の模様を用いる方式。 （外部から見えやすく、非接触で撮像できるという長所を持っている。正確に虹彩を取り込めれば精度が高いといわれている反面、現在はセンサなどシステムが高価であるという欠点があり、個人用に使いやすくて小型で安い製品が実現出来るか否かが課題となっている。）
顔		顔の形や特徴を読み取り照合する方式。 （常時露出しているため、抵抗感なく自然に入力できるという利点があるが、一卵性双生児の識別は不可能であるなどという欠点がある。使いやすいので限定された場面で使用されつつある。）
音声		音声としての特徴や声紋などから判別する方式。 （周囲の雑音、音声の品質、本人音声の変動、録音音声への対応などさまざまな技術的課題がある。一方、心理的抵抗が少ない、特殊なセンサ等を必要としないため安価に実現できるなどの利点がある。）
手形・掌紋		手形： 手の大きさや形を読み取る方式 （精度はやや劣るものの、利用のしやすさが特徴であり、入門管理などに利用される。）
		掌紋： 手のひらにある紋様を用いる方式。（手相ではない） （大きな指紋と見なしても良いが、大きなセンサーが必要であり、個人認証には特に経済的な面で問題）
筆跡		文字の書き方や筆圧、筆を離す方向などから判別する方式。 （精度が劣るという欠点があるが、ペン入力を基本とする携帯端末へは適用しやすいという利点がある。）
打鍵		キーボードなどから入力するときのスピードや、キーと別なキーとを押す間の間隔などから判別する方式。

表に挙げた方式のうち、指紋は、

(1) 万人不同

指紋は二人とは同じ人が存在しない

また、同一人物の他の指や双子の兄弟でも同じ指紋は存在しない

(2) 終生不変

身体の成長や歳月の経過によっても紋様は変化しない
という特性を持っており、価格面、小型、認証精度等の面で最も実用化の面で優れている。

以降の節では、バイオメトリクスの中でも指紋認証を特に取り上げて詳細を説明する。

1.4.4.2 指紋認証技術の詳細

指紋認証について、更に詳細を説明する。
ここでは、指紋認証を実現する要素として、
①センサ技術
②照合アルゴリズム
について説明する。また、指紋を利用した認証システムについても述べる。

(1) センサ技術

指紋認証に用いる指紋データの入力センサとして実用化されているものには、以下の２つの方式が存在する。

表 1-5 センサ技術

方式	特徴
光学式センサ	プリズムの表面に置いた指の凹凸を、下方から光を当てて反射率の違いに反映させ、デジタル画像化する方式
静電式センサ	半導体チップの表面に直接接触させた指紋の凹凸を静電容量の差に反映させデジタル画像化する方式

光学式センサはその方式によりセンサ部が複雑で、高価になりやすく比較的サイズが大きくなるのに比べ、静電式センサは比較的低価格で、小型化・薄型化できるため、システムの応用範囲を広げることが可能となっているが、逆に小型化、低価格化を志向するあまりセンサー面が狭くなり、光学式に比べ、使う時に制約が大きくなっている。

(2) 指紋照合アルゴリズム

指紋照合を実現する方式には大きく分けて、以下の２つの方式がある。

表 1-6 指紋照合アルゴリズム

方式	特徴
特徴照合方式	指紋隆線およびその端点と分岐点（マニューシャと呼ぶ）を抽出し

	て、それらの位置や方向を元に２つの指紋特徴間の一致を調べる方式や、更に特徴点間の隆線数などを追加情報として２つの指紋特徴間の一致を調べる方式がある。 特徴抽出処理の計算量が大きいという欠点があるが、指紋画像入力時に発生する画像の歪みなどの変形に強いという利点がある。
画像マッチング方式	画像としての隆線パターンの単純な一致を調べる方法もしくはフーリエ変換した指紋画像同士の位相相関を評価する方式などがある。 照合処理が高速であるという利点があるが、指紋画像入力時に発生する画像の歪みや、位置ずれ、回転、品質劣化などに弱いという欠点がある。

特徴照合方式は、昨今の計算機の能力向上により、計算量が大きいということは特に欠点とはならず、登録データの量が少なく、認識率が高いことから実用システムとしても主流となりつつある。

(3) 認証実現のための方式

指紋照合により認証を実現する方式には、以下の方式がある。

表 1-7 実現方式

方式	
スタンドアロン型	ユニット型： センサーと同じハードウエアの中に指紋画像取り込み、登録、照合など全機能を持たせて、専用機器に組み込めるようにしたもの。
	ＰＣ内埋め込み型： あらかじめ PC に登録されているサービスを許可されているユーザの指紋情報と、サービスを要求する人間によって入力される指紋情報とがＰＣ内で照合され、一致すれば認証成功とするもの。 PC へのログイン時の認証や OS ロックなどに利用されることが多い。
ネットワーク対応型	ユーザが入力した指紋情報からクライアントで抽出された指紋特徴がネットワークを介してサーバに送信され、サーバに保存されているテンプレートと照合され、一致すれば認証成功となる。 ネットワークの安全度が比較的高い、イントラネットを主体とした社内システムに利用されることが多い。

ネットワーク対応型の構成では、指紋特徴がネットワークを介して送信されるため、比較的安全度の高いネットワークでのみ利用可能である。従って、インターネットなど一般ユーザを対象とする場合、照合自体はユニット内や、クライアント内でおこない、照合結果だけをネットワークを通じて送信するという方法が多い。この場合、指紋情報のテンプレートは IC カードなどのセキュアな環境に保存される必要がある。

1.4.4.3 PKI との連携

先に述べた通り、モバイル EC における認証には、端末認証と本人認証とがある。本書で想定するモバイル EC の端末モデルでは、端末は UIM もしくは 2nd チップとしてセキュアメモリ（IC チップその他）が搭載されている。端末認証に使用する鍵は、UIM やセキュアメモリなどに格納され利用されるのが一般的である。この格納された鍵の利用に際して、バイオメトリクスなどの個人認証を利用することで、モバイル EC における認証をより強固なものとして、利用することが可能となると考えられる。

バイオメトリクス照合（ここでは指紋認証を例として挙げている）による個人認証と公開鍵暗号方式による端末認証を組み合わせた認証方式の実現例を、以下の**図 1-32** に示す。

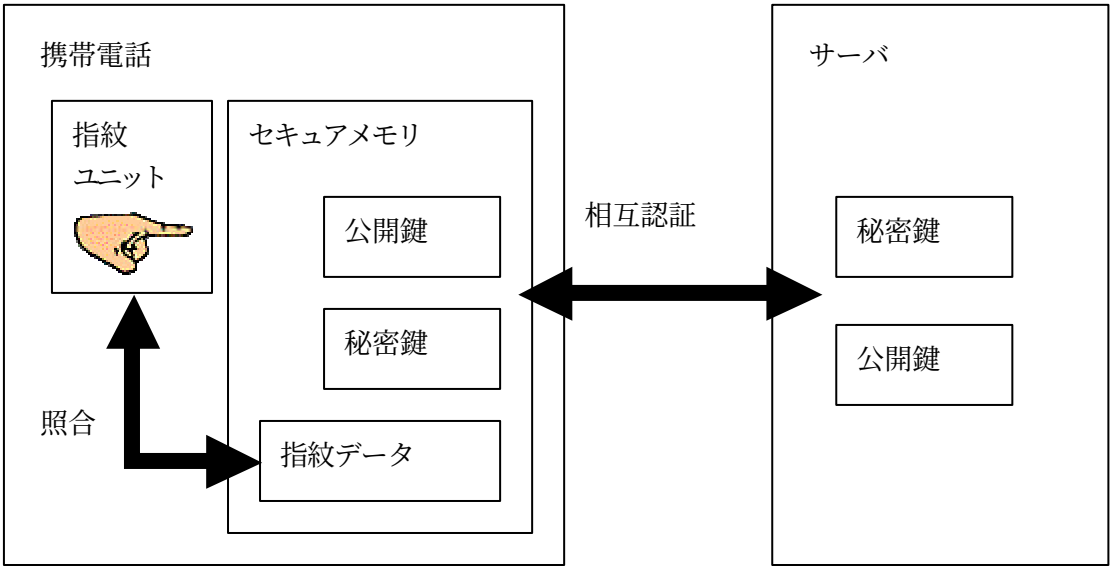


図 1-32 認証方式の実現例

図 1-32 に示す通り、指紋照合によって本人認証に成功した時にのみ秘密鍵にアクセスすることで、使用者＝本人であることを保証することができる。これによりサービスの利用者が本人であることが確認できる。

1.4.4.4　モバイルへの適用の課題

ここでは、これまで取り上げたバイオメトリクス認証のモバイル EC への適用に際した、技術面、運用面、社会的側面の課題について説明する。

(1) 照合精度の問題

モバイルへのバイオメトリクス認証の適用に関する第一の問題として、個性の豊かな生体をアナログ的にセンサーで取り込み、デジタル化して識別するいわゆるパターン認識に常につきまとう精度（照合精度あるいは識別精度）の問題がある。照合精度を比較する場合、一般に以下の２つの尺度を用いられる。

表 1-8 照合精度

照合精度	意味
他人許容率	登録されていない情報を登録していると誤って認識してしまう率
本人拒否率	登録している情報なのに登録していないと誤って認識してしまう率

通常、これらの率は相反する率になる。例えば、他人による「なりすまし」を厳しく防ごうとする、すなわち他人許容率を小さくしたいとすれば、本来合うべき本人も拒否される、すなわち本人拒否率が大きくなる傾向がある。逆に本人拒否率を小さくしたいとすれば、他人許容率は大きくなる。

本人拒否率が高いと、何度も認証をしなおす必要があって、使い勝手が悪くなるだけではなく、認証実行者に、本人なのに認証が受け入れられなかったという心理的な悪影響を与えかねない。しかし、認証システムにとって他人受入すなわち「なりすまし」を許すことは最も避けなければならない状況である。

特に指紋認証を例とすると、他人受入率が 0.01%ということは１万分の１ということであるが、これは１個を登録しておき異なる指を 10,000 回入力しても１回以下の他人受入しか起きないということである。逆に 10,000 個の指紋を登録した場合、登録してない指を１回入力して、10,000 個の指紋のどの指にも誤認されないということである。つまり 0.01%の他人受入率ということは、１対 10,000 指照合、つまり１対 N（10,000）照合方式が実現可能であるということを意味する。この１対 N 照合とは、識別に際して、これから識別をおこなう識別実行者が誰であるかあらかじめ提示することなく、システムに登録した複数の識別対象との照合を可能とする照合のことである。

この照合精度は入力する指紋の品質に大きく依存する。指紋を入力する人の皮膚の状況、汗が多いか、乾燥肌か、すり減っているかなどは大きく精度を左右する。あいにく各照合システム提供ベンダーが数百人の同じ被験者集団で照合評価する事は不可能に近く、従って仮に同じ照合装置でも異なる精度にもなるし、実際に異なる精度の

装置でも評価数字上は同じになることもある。

この様な比較するにはかなり問題がある照合精度の意味をユーザやシステムインテグレータが理解して、適用する認証の要求精度レベルに合った指紋照合システムベンダの製品を採用する必要があると考えられる。

これらの問題は、現在、電子商取引標準化研究委員会のバイオメトリクス標準化 WG（平成１３年度より委員会の予定）でＪＩＳ化のための検討中の課題であり、その結果が期待される。

(2) センサの問題

バイオメトリクス認証に用いるセンサには、同一の認証方式であっても、照合に用いる装置が幾つかあり、それぞれの装置により、データの採取に関する向き不向きがある。

例えば、**1.4.4.2 指紋認証技術の詳細** で紹介した通り、指紋認証に用いるセンサの主なものには、

（ｉ）光学式（CCD）センサ

（ii）静電容量型半導体センサ

の２種類がある。

どちらもデータ採取時の指の状態、例えば汚れや汗のかき具合、皮膚の荒れ具合などの影響を受けやすい。

また、機器が小型であるという特徴を持つモバイル端末への適用に際しては、センサや照合のための専用 CPU などを搭載することの可否の問題も存在する。

（iii）バイオメトリックスへのアタック問題

バイオメトリクス認証の各認証方式に対しても、他の認証と同様にそれを不正に侵入するための方法が考案されていることも事実である。

例えば、指紋認証に対して、参考文献[1]は人工指による指紋認証装置の認識に関する論文であり、本論文に提示された方法により作成された人工指を用いることにより、指紋認証装置が認識可能なことが報告されている。この人工指は指を約１０分間、じっと動かさないようにする必要があるので、人工指を作ることを本人の了解を得るか、暴力的に指の切断とか、薬品で眠らせるなど、家の玄関のドアや、窓のガラスを破って家に侵入する以上とも言える犯罪行為を前提としている。

セキュリティは 100%保証しようとすれば如何なるセキュリティ製品も存在することは不可能であり、セキュリティを高めようとすればするほど価格や、大きさ、使い勝手に問題が生ずる。

これら不正侵入に関する報告に対して、これらの要因をいかに解決していくかは、バイオメトリクスの各認証方式をはじめ、認証方式全般に重要な課題である。

(3) バイオメトリクス認証のモバイルへの応用例

ここでは、バイオメトリクス認証をモバイルに適用した場合の応用例を紹介する。幾つかのバイオメトリクス認証のうち、認証の対象を複数持つことが出来る方式がある。特に指紋認証では、認証の対象となる指紋は一個人に複数存在する。認証の対象が複数あることを利用して、以下のような応用例が考えられる。

表 1-9 モバイルへの応用例

方式名	概要	モバイルへの適用
指先コマンド	個人の各指に仮想的にコマンドを割り当て、「どの指で押すか」で動作を決定できる。ボタン数削減、入力部を見ないでの操作などの効果がある。	指に相手先電話番号を対応させ、どの指を使って認証するかによって、接続先を決定する方法などに使用できるのではないかと考えられる。
指先セーバ	指紋によるログインと同時に、ユーザごとに用意された個別環境を設定し、さらにはどの指かに応じて異なる環境設定の中から選択できるようにすることが可能である。	認証に成功した各人の携帯端末環境を設定可能とするなど、電話端末の共有に利用できるのではないかと考えられる。

これらの考えが実際にモバイルＥＣに実現して、実際に使用される時期を想像することは非常に興味深い。

(4) バイオメトリクスのモバイル EC への適用の課題

バイオメトリクスのモバイル EC への適用については、認証用の指紋データの管理等や、プライバシーの問題などによるユーザから見た親しみ易さ等について、社会的合意形成等も含めて、今後さらに議論が必要である。

参考文献

[1]山田浩二他, “ 指紋照合装置は人工指を受け入れるか ”, 電子情報通信学会情報セキュリティ研究会, 2000/7/25

1.5　マルチアプリケーションサービスの提供形態について

ＩＣメモリを利用したマルチアプリケーションサービスの登場は将来想定される。今後のモバイルＥＣの健全な発展のためには、その提供形態については十分に議論されるべきであり、今後の検討課題である。

1.6　その他関連資料

1.6.1　ＳＩＭカード提供形態の調査

1.6.1.1　香港

(1) Hutchison Telephone Company Ltd

① 概要

Hutchison Telephone Company Ltd が提供する「Orange Rechargeable Stored Value SIM Card」は、ＧＳＭの 3 バンド、もしくはデュアルバンドのモデルやＰＣＳモバイル電話機で使用できる。Rechargeable（リチャージ）とは通話度数を再補充することを意味する。同じ電話番号を引き続き使用できる。このカードでは市内通話やＩＤＤ国際電話に使用でき、次ぎのいずれかの方法でリチャージできるようになっている。

・リチャージ・バウチャを購入する
・電話サービス（プッシュ式電話）による支払（PPS）
・JETCO 端末を介した Jet 支払（Jet Payment）
・請求書の支払サービスがある HBBC および Hang Seng 銀行からのＡＴＭ

図 1-33 カードホルダー証明書「Cardholder Certificate」

このリチャージアブルなＳＩＭカードは、パッケージのなかに入っている。

「Cardholder Certificate」(**図１-33** 参照)に記載されている満期日前に初期起動して携帯電話機に挿入して使用する。（この「Cardholder Certificate」利用については C.項参照）

② Orange Rechargeable Stored Value SIM Card の提供形態

次の**図１-34、5-35**（写真）に「Orange Rechargeable Stored Value SIM Card」の表面と裏面の図を示すが、ＳＩＭカード裏面に次の表記により、ユーザにその旨明確に中文と英文にて次ぎ旨明示している。

『<u>このカードの所有権は Hutchison Telephone Cmpany Ltd(HTLC)にあります</u>。発見したときは同社に返却してください。このカードの利用者は HTLC が提供するサービス提供条件に従うものとします。その条件は改訂されることがあります。』

なお、この図のＳＩＭカードの額面は 200 ドルで有効期限は使用開始から 180 日のものである。

Orange Rechargeable Stored Value SIM Card-表側

図 1-34 SIM Card-表側

Orange Rechargeable Stored Value SIM Card－裏面

図 1-35 SIM Card-裏面

③　その他の使用・契約条件

「Orange Rechargeable Stored Value SIM Card」**の利用説明書には概ね次項などについて記載されている。**

１）ＳＩＭカードを利用するときにまずはじめに

「Cardholder Certificate」**のシールを剥がして起動番号**（Activation Number）**を確認し、**SIM **カードを携帯電話に挿入して、**1750175 **をダイヤルして音声ガイドに従う。音声指示にて起動番号を押下するとシステムが割り当てられた携帯電話番号、**SIM **カードの使用期限を通知してくるので控えること。**

２）リチャージする方法

３）ＳＩＭカードを使用してＩＤＤを利用する案内

４）ＳＩＭカードの紛失あるいは置換について

ＳＩＭカードを紛失し新たなカードを購入するときは「Cardholder Certificate」**をハチソンテレコムカスタマーセンターに持参する必要がある。ＳＩＭカードが不調のときも同様である。**

５）個人ＩＤ番号(PIN:Personal Identification Number)

ＳＩＭカードの不正利用を回避するために、各ＳＩＭカードは“ 888 **”のディフォルト番号でプリセットされている。一度、ＰＩＮ機能を起動すると携帯電話機を使用するたびに** PIN **を入力する必要があり、ユーザ自身で４～８桁の** PIN **コードを設定することができる。**

6）契約条件

Hutchison Telephone Cmpany Ltd**が提供するこの**SIM**カードは次ぎの契約条件で利用することができる。**

（ｉ）SIM **カードの利用者はここに規定する契約条件に従うものとします。**

（ii）この SIM **カードの払い戻しはできません。**

（iii）SIM **カードは、パッケージに記載された有効期日もしくは期日以前に起動（**activate**）する必要があります。有効期限までに最低限のリチャージをしなかった場合、カードの全ての未使用分は無効となり、払い戻しもできません。**

（iv）ローカルな通話はハチソンが随時規定する分単位の料金体系で課金されます。

以上、結論として、「Orange Rechargeable Stored Value SIM Card**」の所有権は** Hutchison Telephone Cmpany Ltd **に帰属する。**

(2) Cable ＆ Wireless HKT CSL Limited

Cable ＆ Wireless HKT CSL Limited**（以下、会社）は、その唯一かつ独占的な販売代理店である** One2Free PersonalCom Limited **社(**One2Free**)と「携帯電話サービスおよび電話機購入に関する提供条件書」**(TERMS AND CONDITIONS FOR THE PROVISION OF MOBILE RADIO TELEPHONE SERVICE & HANDSET PURCHASE--**表１-10)にて概略以下の内容に合意している。**

表 1-10 携帯電話サービスおよび電話機購入に関する提供条件書

「携帯電話サービスおよび電話機購入に関する提供条件書」 **１．携帯電話サービス** **２．携帯電話機**
３．携帯電話サービス **会社が提供する携帯電話サービスとの接続に使用する携帯電話機は通信省が型式認定したものでなければならない。** **この契約に基づく携帯電話サービスは、会社が現行の料金体系を随時変更することを拘束しない、など８項目。** **４．加入者識別モジュールカード（**SUBSCRIBER IDENTITY MODULE CARD**）** **4.1 会社は、携帯電話サービスに使用する携帯電話機用の加入者識別モジュールカード（“ＳＩＭカード”）を加入者に発行する。**

4.2 ＳＩＭカードの所有権はいかなるときも会社（Cable & Wireless HKT CSL Limited）に帰属し、要求次第あるいは携帯電話サービスの解約のいかなる時にも会社に返却しなければならない。

4.3 会社は、通常の消耗にて損傷したＳＩＭカードを自己の裁量で加入者に対し無償で交換することができる。

５．モバイルローミングサービス

６．支払

７．預託

８．解除

会社は、この契約を速やかに解除したり、ここに列記する事情が発生したときは随時携帯電話サービスの提供を中止することができる、など。その事情の一つに顧客（ここでは代理店）がプリ・プログラムされたＳＩＭカードを改竄、複製、あるいは第三者に改竄や複製を許諾したとき、と記されている。

９．携帯電話機/ＳＩＭカードの盗難、紛失

9.1 顧客は携帯電話機あるいはＳＩＭカード、あるいは両者を紛失したときは如何なる場合も警察署、あるいは当該ローミング地域においては同様な機関にその旨届け、かつ会社もしくは One2Free にその事実を 24 時間以内に通知しなければならない。

9.2 前項の通知を会社が受けるまでの間に紛失した携帯電話機および/またはＳＩＭカードが使用されて発生した全ての利用料金は顧客が負担しなければならない。紛失した携帯電話機および/またはＳＩＭカードに対する携帯電話サービスは会社が停止する。

9.3 紛失した携帯電話機および/またはＳＩＭカードが回収された場合、会社もしくは One2Free は、顧客が回収された電話機あるいはＳＩＭカードへの携帯電話サービスの再接続を要請し、かつ全ての未払い料金、会社の現行の再接続費用、会社もしくは One2Free が自己の裁量で決めるサービス再開前の機器および/またはＳＩＭカードに対する検査費用の支払を行なった時点で再接続することができる。

9.4 会社は、紛失した電話機の MEI 番号あるいはＳＩＭカードにプリプログラムされたデータもしくはページャが改竄されていた場合は前 9.3 項に定める顧客による携帯電話サービスの再開要請を拒否する権利を留保する。

10．再接続

11.署名と文書証明

12．責任制限

13. 変更
14. 譲渡と代理権
15. 準拠法
16. 免責条項
17. 通知
18. 非免責条項
19. 可分性
20. 個人データの使用
21. 完全合
22. 解釈

結論として、ＳＩＭカードの所有権はサービスプロバイダー（オペレータ）側に帰属し、返却（解約時）する義務を規定している。

(3) Mandarin Communications Limited

香港でＳＵＮＤＡＹというブランド名で携帯電話サービス（ＰＣＳ）を提供している Mandarin Communications Limited は、1997 年でサービスを開始し、2000 年第二四半期末に約 30 万加入者を有するオペレータである。

同社はサービスに関する「一般サービス提供条件書」（**表１-11**）で次ぎの条項を規定している。

表 1-11 Mandarin Communications の一般サービス提供条件書

「一般サービス提供条件書」

上記第 1 項の「定義」のなかでは、「ＳＩＭカード」の用語の定義もあり、次のように記述されている。

「ＳＩＭカードは、加入者識別モジュールカードのことである。マイクロプロセッサーを内蔵し、サービス提供に関連したデータが蓄積されている 1 枚のプラスチック板である。」

そして上記第６項の「ＳＩＭカード」の条項にてＳＩＭカードの提供形態について、以下のとおり規定している。

ａ）ＳＩＭカードの所有権は、常に Mandarin Communications Limited 社（当社）にある。要請があったとき、あるいはサービスの解約時には速やかにＳＩＭカードを当社に返却すること。当社は、当社料金表で公示するＳＩＭカードの価格を請求する権利をもつ。

ｂ）当社は、通常の消耗によって損傷したＳＩＭカードを独自の裁量で交換することができる。だたし、その交換は、顧客側あるいは第三者による誤用、不注意あるいは故意の過失に起因した損害、もしくは結果として生まれた損傷を対象としない。

以上、結論として、ＳＩＭカードの所有権はサービスプロバイダー（オペレータ）側に帰属し、返却（解約時）する義務を規定している。

1.6.1.2　シンガポール

(1) シンガポールテレコム

シンガポールに本拠をおく Singapore Telecom Mobile Pte, Ltd.（以下、「シングテルモバイル」）はＧＳＭサービスを提供しており、日本のある代理店（以下、ＡＢＣ社と表記）とＳＩＭカードローミングサービスについてＳＩＭカード契約書を交わした経緯がある。

表 1-12　SingTel Mobile による SIM Card Roaming Agreement

SIM Card Roaming Agreement
～
ＡＢＣ and SingTel Mobile have hereby agreed to implement a SIM Card Roaming Service based on the Terms and Conditions for interalia provision of SIM cards to Carrier attached herewith.
～
Terms and Conditions for Provision of GSM Roaming Service（GSM ローミングサービスに関する条項および条件）
Article 1.　Definitions and Interpretation（定義と内容）
Article 2.　Singtel Service（Singtel のサービス）
Article 3.　Tariffs（料金）
Article 4.　Settlement of Charges（精算）
Article 5.　Customer Care（顧客サポート）
Article 6.　Confidentiality（守秘義務）
Article 7.　Term and Termination（期限と解約）
Article 8.　Dispute Resolution（紛争の解決）
Article 9.　Jurisdiction（裁判管轄）
Article 10.　Force Majeure（免責条項）
Article 11.　Amendments（修正）
Article 12.　Governing Law（準拠法）
Article 13.　Schedules（スケジュール）

その契約書（守秘義務もあり全内容は非公開）の一部を入手したが、次ぎの英文にて表記されている。翻訳を（ ）書きで列記する。

上記契約書の「2. Singtel のサービス」の部分のさらなる詳細な条項を翻訳すると、次のようにＳＩＭカードの所有権が、常にシングテルモバイルの所有物であることが明記されている。

表 1-13 Singtel のサービス 翻訳）

2．Singtel のサービス

２．１　シングテルモバイルの GSM サービスは Schedule-1 に基づきＡ社に提供される。

２．２　シングテルモバイルはＡ社に対し両当事者が合意した数のＳＩＭカードをその都度、Schedule2 で定めた価格にて提供する。

２．３　シングテルモバイルはＡ社から依頼のあった日より５営業日以内にＳＩＭカードを郵送にて送付する。但し、不正使用を防ぐために、すべてのＳＩＭカードが郵送中は利用不可とする。また、SIM 番号、電話番号、PIN 番号、PUK 番号を含むリストは SIM ｶｰﾄﾞの発送とは別にファックスにて通知するものとする。

２．４　シングテルモバイルは、Ａ社よりＳＩＭカード、SIM 番号、電話番号、PIN 番号、PUK 番号受領の通知を受け次第、ＳＩＭカードを登録する。

２．５　Ａ社が GSM サービスを一時的に停止、解約する場合は、サービスの停止、解約をシングテルモバイルへ申請するものとする。

２．６　シングテルモバイルは、下記の条件に合致した場合、Ａ社に対し、事前通知の上ローミングサービスのすべてまたは一部を停止または解約することがある。

(a) Ａ社が不正な利用、または法令に違反している場合。

(b) Ａ社がシングテルモバイルのﾈｯﾄﾜｰｸに対し技術上またはその他の問題を生じさせる場合。

(c) 利用者の認識ができない場合。

(d) シングテルモバイルの GSM ネットワークのメインテナンス、または拡張の場合。

２．７　Ａ社は提供されたＳＩＭカードが 2.8 条、2.9 条に基づき不良、故障、紛失、盗難のいずれかの理由によりＳＩＭカードの停止についてシングテルモバイルに通知するまでに発生した通信料金等の費用について、責任を負うものとする。

２．８　シングテルモバイルはＡ社から特定のＳＩＭカードの登録解除を依頼された場合、１営業日中にその登録を解除する。尚、その通知はファックスにても行うことができる。

２．９　Ａ社はＳＩＭカードが不良、故障、紛失、盗難の場合にシングテルモバイルにその解除を要請する。シングテルモバイルは 2.4 条、2.7 条及び 2.8 条に基づき、不良、故障、紛失、盗難の届けのあったＳＩＭカードを新しいＳＩＭカードにて同じ電話番号で登録、提供する。Ａ社は Schedule2 の条項に従い、取替えのＳＩＭカードの代金を支払うことにより、新しいＳＩＭカードを受け取ることができる。

２．10　２.１の条項に基づいて提供されたすべてのＳＩＭカードは常にシングテルモバイルの所有物である。Ａ社は、本契約を解約する場合は、解約日より３０日以内にシングテルモバイルに返還するものとする。

２．11　下記の項目については実施してはならない。

(a)シングルモバイルから提供されたＳＩＭカードを第３者に転売すること。

(b)シングルモバイルに有害の有無にかかわらず、ここで提供されていない条項に基づくＳＩＭカードの利用。

以上、結論として、ＳＩＭカードの所有権はサービスプロバイダー（オペレータ）側に帰属し、返却（解約時）する義務を規定している。

1.6.1.3　ドイツ

(1) ハチソンテレコム有限会社と各事業者との代理店契約

ハチソンテレコム有限会社が、ドイツテレコム社、マンネスマン・モビールフンク社、イープルス・モビールフンク社の携帯電話サービスを代理提供するにあたっての取引条件書（**表１-14**）は次の構成になっている。

そして、下記、一般取引条件書の「Ⅱ．契約の成立と履行」の「携帯電話」の条項では次のように記述されている。

『ハチソンテレコム有限会社（以降、ハチソン）は、携帯電話サービス（D1, D2, E-Plus）のプロバイダーである。ハチソンは、ドイツテレコム社の D1 サービス、マンネスマン・モビールフンク社のD2サービス、イープルス・モビールフンク社のE-Plusサービスに関し、これら３者の契約義務の履行の代理を行う。』

さらに、そのなかの２．５項においてＳＩＭカードの扱いについて次ぎのように規定している。

『ハチソンは、契約期間の間、顧客に一枚のカードを渡す。このカードは、各キャリアの所有に属す。有効期間経過の際、もしくは契約終了の際、２週間以内にこのカードが返却されない場合には、顧客はハチソンに対して有効な価格表の金額を支払う。

カードが第三者に渡された場合でも、当該顧客が契約当事者として留まる。契約義務の譲渡は、ハチソンの同意があった場合のみ可能である。』

表 1-14 ハチソンテレコム社による通信サービス一般取引条件書

ハチソンテレコム有限会社に対する通信サービス一般取引条件書
Ⅰ．適用範囲
Ⅱ．契約の成立と履行
・携帯電話
・固定網
Ⅲ．固定網サービスの提供
Ⅳ．対価（報償）
Ⅴ．支払条件

以上、結論として、ＳＩＭカードの所有権はサービスプロバイダー（オペレータ）側に帰属し、返却（解約時）する義務を規定している。

(2) ドイツテレコム

日本の法人、日本に在住している人ならＧＳＭのサービスに加入することができその業務を行なっている Deutsche Telekom K.K.Tokyo（東京都千代田区一番町 29-1 番長ハウス）から、加入申し込み資料などを得たが、その「サービス提供条件書」では特にＳＩＭカードの所有権帰属については記述されていない。

しかし、同営業所のコンシューマ営業部（村川女史）との談では、「解約時にはＳＩＭカードは返却してもらっている。紛失など事故時は回線をブロックするなど対処している。」旨の回答を得た（平成 13 年 2 月 1 日１４：50 分）このことから、条件書での記述はないものの、SIM カード自体の所有権は Deutsche Telekom にあるとの認識がプロバイダー側にある。

1.6.1.4 フランス

フランステレコム携帯電話約款（表１-15）によると、直接その所有権帰属の明記がなされていないが、解約時には返却する旨、記述されている。このことは間接的にＳＩＭカードの所有権は通信事業者側にあると判断される。

また、ＫＤＤＩフランスからフランステレコムに確認してもらったところ、次のような回答を得た。（メール文をそのまま記す）

表 1-15 フランステレコムからの回答

（省略）
先週、フランステレコムに連絡してお問い合わせの件について確認したところ、以下のような回答でした。
・ＳＩＭカードの所有権は、一応事業者側にあるので、
解約した際には、原則カードを返してもらう必要がある。
ただし、解約の時点で、事業者側のシステムによりその
カードを利用不可としてしまうため、その後ユーザーが
そのカードを持っていても意味がないことから、ほとんどの
場合返してもらっていない。

1.6.2 ニューメディア開発協会

1.6.2.1 アドバンスドＩＣカードシステムの開発

（財）ニューメディア開発協会では、平成１０年度第一次補正予算によって、（財）日本情報処理開発協会が実施する「先端的情報システム開発実証事業」の一環として、ＩＣカードシステムにおいて、セキュリティ、拡張性、開発容易性等の課題を解決し、従来のカードとの上位互換性を確保する諸機能の体系化を実現する標準仕様の作成と、アドバンスドＩＣカードシステムのコアとなる基盤技術の開発を行った。

特に、ドキュメントとしてとりまとめた、「共通コマンド仕様書」は、ＩＳＯ、ＪＩＣＳＡＰ仕様、EMV仕様などの既存の業界標準仕様との互換性を確保した上で、カード内にファイル構造を構築するための発行コマンド、および署名作成・検証、セキュアメッセージング機能などの高度なセキュリティ機能を最新の国際規格と整合性を図りながら仕様としてとりまとめた。

1.6.2.2 新世代ＩＣカード共通システム

（財）ニューメディア開発協会では、平成１０年度第三次補正予算によって、（財）日本情報処理開発協会が実施する「産業・社会情報化基盤整備事業」の一環として、現状の多様なカード仕様の体系的統合化を図り、新たな機能要求および多様なセキュリティレベルに

対応することができる先駆的アーキテクチャに基づく「新世代ＩＣカード共通システム」の開発を行った。

そこでは、「カードプラットフォーム仕様書」において、アドバンスドＩＣカードシステムの開発成果である、共通コマンド機能の活用や、新たにカードに複数のアプリケーションプログラムの安全なダウンロード機能を実現する等カードプラットフォームに関する仕様をとりまとめている。また、そのカードプラットフォームをＰＣ上で擬似可能な参照実装（リファレンス・インプリメンテーション）を開発し、新規にカードプラットフォームを開発しようとする方々への便宜を図るとともに､相互運用性の向上を図ることをねらいとしている。

また、「近接型通信インタフェース実装規約」を定め、国内の電波法の遵守を前提に、近接型ＩＣカードとリーダライタの互換性を確保するため、ＩＳＯ/ＩＥＣ１４４４３　に補足すべき仕様、およびその試験方法の定義を追加し、より互換性の向上を図るべく工夫を加え、上記技術開発において実施した実装規約検討作業の成果をとりまとめている。

1.6.3　USIM と IC カードの要件

ECOM モバイル EC･WG 内で、USIM と IC カードの要件に関する情報共有を目的として、関係する ARIB 標準規格（原文は英文のみ）を ECOM が独自に翻訳し、参考情報として掲載する。なお、本手続きは(社)電波産業会殿の許可を得たものである。

・文献名：ARIB 標準規格“ IMT-2000 DS-CDMA System ”
ARIB STD-T63 Ver.1.30
ARIB STD-T63-21.111V3.3.0
“ USIM and IC Card Requirements ”

・詳細については原文を参照されたい。原文の Web アドレスおよびアクセス方法は以下のとおりである。

(1) Web アドレス：
http://www.arib.or.jp/IMT-2000/V130Jan01/T63/21/A21111-330.pdf

(2)アクセス方法：
ARIB の HP（http://www.arib.or.jp）の IMT-2000 関連事項の中の
ARIB STANDARD の中の
IMT-2000 DS-CDMA system Specifications(ARIB STD-T63 Ver.1.30)の中の
1 standard の中の
ARIB STD-T63-21.111 V3.3.0　“ USIM and IC card requirements ”

《参考情報 - 訳文 - 》

1　適用範囲

本書では、USIM (Universal Subscriber Identity Module)および 3G(UICC)用 IC カードの要件を定義している。これらの要件は、3G の TS（技術仕様書） 22.100 [1] および 3G の TS 22.101 [2]で定義されているサービスとセキュリティの要件から導き出される。USIM は、IC カードの 3G アプリケーションである。USIM は、3G 端末で相互運用され、3G サービスへのアクセスを提供する。本書は、USIM と UICC、および 3G 端末へのインターフェースに関する詳細な仕様の基盤となるように意図されている。

2　参考文献

2.1　規定としての参考文献

本文中には参考文献からの規定があるが、以下の文献には本書を構成している規定が含まれている。

- 参考文献は、特定（発行日、版番号、バージョン番号などが分かる）または非特定のいずれかである。
- 特定の参考文献には、その後の改定は適用されない。
- 非特定の参考文献には、最終バージョンが適用される。

[1] 3GPP TS 22.100: "UMTS phase 1 Release 99".

[2] 3GPP TS 22.101: "Service principles".

[3] 3GPP TS 31.101: "UICC-Terminal Interface; Physical and Logical Characteristics".

[4] 3GPP TS 31.102: "Characteristics of the USIM application"

[5] 3GPP TS 31.110: "Numbering system for telecommunication IC card applications".

[6] 3GPP TS 31.111: "USIM Application Toolkit (USAT)".

[7] 3GPP TS 33.102: "3G Security: Security Architecture".

[8] 3GPP TS 11.11: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

[9] 3GPP TS 11.12: "Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM- ME) interface".

[10] 3GPP TS 11.18: "Specification of the 1.8 Volt Subscriber Identity Module-Mobile Equipment (SIM -ME) interface".

[11] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[12] ISO/IEC 7816-4 (1995): "Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[13] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

2.2 情報としての参考文献

[20] 3GPP TS 02.48: " Security Mechanisms for the SIM application toolkit; Stage 1".

[21] 3GPP TS 03.48: "Security Mechanisms for the SIM application toolkit; Stage 2".

3 定義、シンボルと短縮形

3.1 定義

本書では、以下のように定義する。

UICC USIM を含む取り外し可能な IC カード

USIM IC カードの 3G アプリケーション

3.2 シンボル

Vpp プログラミング電圧

3.3 短縮形

本書では、以下の短縮形を適用する。

ADN Abbreviated Dialling Number（短縮ダイヤル番号）

ATR Answer To Reset（リセット信号に対する応答）

DF Dedicated File（専用ファイル）

EF Elementary File（基本ファイル）

FFS For Further Study（更なる検討が必要）

ICC Integrated Circuit Card（IC カード）

IK Integrity Key（完全性鍵）

IMSI International Mobile Subscriber Identity（国際移動加入者アイデンティティ）

ME Mobile Equipment（移動機器）

MF Master File（マスター・ファイル）

PIN Personal Identification Number（暗証番号）

PPS Protocol and Parameter Selection（プロトコルとパラメータの選択）

SIM Subscriber Identity Module（加入者アイデンティティ・モジュール）

UIA 3G Integrity Algorithm（第３世代完全性アルゴリズム）

USIM Universal Subscriber Identity Module（汎用加入者アイデンティティ・モジュール）

４　一般要件

UICC は、USIM を含む取り外し可能なモジュールである。USIM には、加入者を明白に確認する身元情報が含まれる。

有効な USIM を含む UICC は、3G サービスにアクセスするために常に存在するが、緊急呼び出し時には存在しない。

この仕様書は、33.102 [7] で定義されているセキュリティ要件に対応している。

USIM は、加入契約と加入者に関連する情報の格納を提供する。

UICC/USIM は、USIM Application Toolkit の仕様書 3G TS 31.111 [6]で定義されている機能を使用するアプリケーションを含むこともできる。

５　セキュリティ要件

USIM を使用すれば、セキュリティ機能を提供できる。UICC が 3G 端末から取り外された場合、そのサービスはただちに終了してしまう。USIM には、USIM そのものをネットワークに対して認証させる機能（その逆も）、ユーザーを認証する機能、3G TS 33.102 [7] で定義されている追加のセキュリティ機能を提供する機能がある。

USIM は、前払い式（プリペイド）加入契約の場合にも明白に識別される。

盗難にあった IC カードの不正使用を防止する方法を提供する。

USIM の内部使用の、例えば認証鍵用の、データにアクセスすることは、不可能である。

以下の要件についての詳細は、33.102 [7]に記述されている。

5.1　ファイル･アクセスの条件

UICC データに対する READ、UPDATE などのアクションは、アクセス条件によって制御できる。この条件を満たしてから、アクションが実行される。

UICC には複数の(3G および 3G 以外の)アプリケーションを含むことが可能なため、ファ

イル･アクセスを制御する柔軟な方法が提供される。

5.2　ユーザーの認証

USIM では、例えば、盗難にあったカードの使用を防止するために、ユーザーを認証する方法をサポートする。USIM では、認証は 4 桁から 8 桁の 10 進数の数字の暗証番号の確認によって実行される。

ユーザーの認証を禁止する機能は、アプリケーション・メーカー側の禁止機能である。アプリケーションを使用する場合、ユーザーは必ず暗証番号を使用する。そうでなければ、ユーザーはユーザー認証機能を利用するか、または利用しないかを決めることができる。ユーザー認証機能を禁止した場合、ユーザーがその認証機能を再び使用可能にするまで、禁止されたままである。

正しい暗証番号を使用することによって、ME は、適切なアクセス条件によって保護されている USIM データに対して機能とアクションを実行できる。

誤った暗証番号が入力された場合、ユーザーには指示が与えられる。3 回連続して誤って入力すれば、その暗証番号は阻止(ブロック)されてしまう。つまり、その試みの間に UICC が取り外され、USIM が公認を取り消され、または ME のスイッチがオフになったとしても、アクセス条件によって保護されるデータに対する機能やアクションは不可能になる。暗証番号が阻止されてしまうと、それ以上の暗証番号の確認は拒否される。

USIM は、阻止された暗証番号の阻止を解く(アンブロック)ための機構をサポートしている。暗証番号の阻止を解くには、その暗証番号の阻止を解く鍵（Unblocking Key）を使用して行う。

暗証番号は､ユーザーが現在の暗証番号または阻止を解かれた暗証番号のどちらかを正しく入力すれば、変更できる。阻止を解かれた暗証番号は、ユーザーには変更できない。

阻止を解かれた暗証番号は、8 桁で構成されるが、ユーザーが変更することはできない。阻止を解かれた誤った暗証番号が存在する場合、ある指示がユーザーに示される。10 回連続して誤って入力をすると、その試みの間に UICC が取り外され、USIM が公認を取り消され、ME のスイッチがオフになったとしても、阻止を解かれた暗証番号は阻止される。阻止された暗証番号の阻止を解くことは不可能である。

暗証番号または阻止を解かれた暗証番号を読み取ることは不可能である。

5.3 ME に格納されるユーザー・データ

後述の例外はあるが、ネットワーク操作中に ME に転送されたすべてのユーザー関連情報は、UICC の取り外し、USIM の取り消し、ME の非活動化、または UICC の電気的なリセットが行われた場合、ME から削除される。[これには、USIM Application Toolkit のコマンドによって ME に転送されたデータが含まれる。FFS]

暗証番号や阻止を解かれた暗証番号などのユーザー関連のセキュリティ・コードは、そのようなコードを含む手順の間だけは ME に格納できるが、その手順の完了後直ちに ME から処分される。

任意選択で、UICC の取り外し、USIM の取り消し、または ME のスイッチ・オフの場合でも、ME はセキュリティに関係のないデータを保持できる。そのデータとは、SMS、ADN/SSC、FDN/SSC、LND である。これらのデータは、ME に格納されていても、(IMSI によって決められたのと)同じ USIM が再活動化されれば、読み取り可能／検索可能になる。IMSI がこの目的のために ME に保持される場合、IMSI は安全に格納されるが出力することはできない。

5.4 認証

USIM とユーザーの家庭環境の間のみで共有され利用可能な秘密鍵 K の情報を示すことによって、USIM とネットワークを相互に認証できる。この方法は、ネットワーク認証用の連続した番号ベースの１工程のプロトコルを組み合わせた challenge(挑戦)/response(応答)と鍵の確立プロトコルで構成される。

5.5 信号方式の要素のデータの完全性

いくつかの信号方式の情報要素は、デリケートであり、データの完全性を確保しなければならない。データの完全性の機能は、ME とネットワーク間で伝送される特定の信号方式の情報要素に適用される。

3GPP の完全性のアルゴリズム(UIA)は、完全性鍵(IK)と共に使用すれば、指定されたメッセージのメッセージ認証コードを算出することができる。IK の設定は、認証手順によってトリガされる。IK は、USIM に格納できる。

5.6 ユーザーの身元の機密保持

仮の身元を使用することによって、ユーザーの身元の機密保持を提供できる。仮の身元がそのネットワークで使用できない場合、グループ鍵を用いて本当のユーザーの身元(IMSI)を

暗号化する方法が使用できる。

5.7　セキュリティ・パラメータの長さ

3G でのセキュリティ・レベルの拡張を許可するためには、以下の要件を満たす必要がある。

- 3G 用のすべてのセキュリティ関連のパラメータが長さのインジケータを伴う。
- USIM が可変長のセキュリティ・パラメータをサポートする。

USIM が 3G のセキュリティに加えて GSM のセキュリティ機構をサポートしている場合、さらに GSM 11.11 [8]に従って固定長のセキュリティ・パラメータをサポートできる。

6　論理的な課題

6.1　アプリケーションの選択

複数のアプリケーション環境下では、柔軟なアプリケーションの選択方法が必要である。ISO/IEC 7816-5 [13] および 3G TS 31.110 [5]で定義されているアプリケーション識別子は、アプリケーションの選択に使用できる。部分的な DF 名の選択を含む直接のアプリケーション選択および ISO/IEC 7816-4 [12]の EFDIR 概念がこれに従う。特に ME がアイドル・モードのとき、ME が保持して使用可能な UICC のうちの１つをユーザが選んで起動することができるように ME と UICC 間の機構が指定されなければならない（これによりユーザは、例えば２つの異なった USIM アプリケーションのうちの１つを選ぶことが可能になる）。スイッチがオンにされると、最後に起動された USIM が自動選択される。最後に起動された USIM は UICC に格納される。もし最後に起動された USIM が UICC の中で定義されていなければ、ユーザはデフォルトにより、UICC 中の使用可能な USIM の中から起動された USIM を選ぶことができる。

6.2　同時アクセス

複数のファイルまたはアプリケーションへの同時アクセスができる。

7　サービス要件

7.1　ユーザーのプロフィール

各 USIM には、少なくとも１つのユーザー・プロフィールが含まれている。[FFS]

7.2　データ転送

アプリケーションや関連データを UICC/USIM から、または UICC/USIM への高度に安全な転送を可能にする機構は、3G TS 22.101 [2]での要件に沿って指定できる。これには、安全な転送機構が必須である。GSM 02.48 [20] および GSM 03.48 [21]がここでは考えられるが、これでは既存の加入契約の状況でダウンロード済みのアプリケーションを実行する場

合に限定されてしまう。例えば新しい USIM または他のアプリケーションをダウンロードしなければならない場合のセキュリティ要件については、さらに検討を要する。

初期の USIM 仕様では、加入契約関連のアプリケーション(例えば SIM Application Toolkit)の転送が指定できると考えられている。一般的なアプリケーションのダウンロード(例えば新しい USIM のダウンロード)は、この初期の仕様には含まれていない。

アプリケーションの作成は、コード・タイプや言語の取り決めだけでなく、ファイルの作成と他の管理的な操作でも構成されている。

7.3 アプリケーションの実行環境

アプリケーションの実行環境は、3G TS 31.111 [6]で定義されている機能性を含む UICC/USIM 上に存在できる。

7.4 プロフィールの交換

ME、USIM とネットワークがサービス機能を交換する機構を指定する。以下のサービス機能の交換ができる。

- ME のサービス機能が USIM/UICC に提供できる。
- USIM/UICC のサービス機能が ME に(および場合によってはネットワークにも)提供できる。
-ネットワークのサービス機能が ME 経由で USIM/UICC に提供できる。

7.5 バージョンの確認

USIM のバージョンを確認する方法が提供されている。

8 物理的な特性

8.1 寸法

GSM SIM に使用される ID-1 とプラグ・イン形式を採用する。第三の形式は、プラグ・イン形式より小さいが、さらに検討を要する。新しい形式が定義された場合には、不正なカードの ME への挿入を防ぐために特定の方法を指定する。

8.2 接点

UICC は、VPP 接点への接続は提供しない。その接点は、UICC 上に提供される。ME は、リーダーでの VPP 接点をサポートする。ME は、この接点を地面にも UICC 供給の電圧にも接続させることはない。

注意：ISO/IEC 7816-3 [11]によれば、VPP 接点は ICC の RFU が 3V で稼動している。

9　電気的特性と伝送プロトコル

電子信号と伝送プロトコルは、他に指定されていなければ、ISO/IEC 7816-3 [11]に従う。

電気に関する仕様は、GSM 11.12 [9] と GSM 11.18 [10]で指定されているように少なくとも 1.8V と 3V の電圧範囲に及ぶ。低電圧については将来追加されるだろう。3G 端末は、ME-UICC インタフェースにおいて 5V をサポートできない。ME と UICC は両方とも、ISO/IEC 7816-3 [11]で定義されているように操作クラス表示をサポートする。ME と UICC は両方とも、少なくとも 2 つの電圧クラスをサポートする。

ME と UICC は両方とも、少なくとも GSM 11.11 [8]で定義されている値で ISO/IEC 7816-3 [11]で定義されている PPS をサポートする。

ME には、ISO/IEC 7816-3 [11] で定義されているウォーム･リセットを開始する機能がある。UICC は、ISO/IEC 7816-3 [11] で定義されているウォーム･リセットをサポートする。

注意：ウォーム･リセットは、ユーザーのアクションまたはネットワーク･データのダウンロードによってデータの内部修正が引き起こされたために、USIM を再起動する必要がある場合のセッション中に使用される。

UICC は、ATR においてそのウォーム･リセットに対し、ウォーム･リセットの前に使用されていたパラメータを使用して、特定のモードに自動的に入ることを指示できる。コールド･リセットの場合、UICC は通行可能なモードに入る。

UICC と ME に必須の T=0 プロトコルに加えて、ME には T=1 プロトコルが必須である。T=1 プロトコルは、UICC にとっては任意である。

GSM 11.11 [8]で指定されている速度の向上は、ME と UICC の両方でサポートされる。GSM 11.11 [8]で指定されているビット速度よりも高速のインターフェースのビット速度が考えられる。

9.1　電力消費の表示

電力消費量は、暗号のコプロセッサを利用して、より安全な認証アルゴリズムの必要性に基づいて変更される。GSM 仕様と互換性を保つために、UICC は ATR の間、GSM 11.12 [9] と GSM 11.18 [10]で設定されている電力消費仕様に適合する。USIM の状況情報には、電力消費情報が含まれる。この情報は、ATR に表示される操作クラスと認証アルゴリズムを実行するために表示される操作頻度に関係がある。

注意：電力消費量は、UICC 上でのアプリケーションによって異なる。したがって、電力消費値によって、ME はカードでのアプリケーションをサポートする場合もあるが拒否する場合もある。

ME は、状況情報に表示される電流を供給できない場合と、その電流が USIM を稼動するため UICC の使用用に定義された最大値を超えた場合には、USIM を拒否できる。

１０　基本ファイルの内容

10.1　USIM 情報の格納要件

USIM には、3G ネットワーク操作のための情報要素が含まれる。USIM には、加入者、3G サービスと家庭環境に関連した情報要素、またはサービス・プロバイダ関連の情報が含まれる。

UICC は以下の格納機能を提供する。

- UICC 関連の情報
  - IC カードの身分証明: UICC とカード発行者を一意に識別する番号
  - 優先言語
  - アプリケーションのディレクトリ

- USIM 関連の情報
  - 管理情報: USIM の操作モードを表示する（例えば、正常、型式承認）
  - USIM のサービス表: USIM がどのオプションのサービスを提供するかを表示する
  - IMSI
  - 言語の表示
  - 所在地情報
  - 暗号鍵(Kc)と暗号鍵シーケンス番号
  - アクセス制御クラス
  - 禁止された PLMN
  - フェーズの識別
  - GPRS の暗号鍵
  - GPRS の所在情報
  - セル同報通信の関連情報
  - 緊急呼び出しコード
  - 電話番号(ADN、 FDN、 SDN)

- 短いメッセージと関連パラメータ
- 機能と構成のパラメータ
- HPLMN 検索期間 [FFS]
- BCCH 情報 :セル選択に使用する搬送周波数のリスト[FFS]

- USIM と他のアプリケーションにアクセス可能な情報
  - ADN

さらに、USIM は「5 セキュリティ要件」に従って以下の情報の格納を管理し提供する。

- 暗証番号
- 暗証番号の使用可能/使用禁止インジケータ
- 暗証番号のエラー・カウンタ
- 阻止を解かれた暗証番号
- 阻止を解かれた暗証番号のエラー・カウンタ
- データの完全性鍵
- 加入者認証鍵

10.2 電話帳

電話帳の機能は、GSM 11.11 [8]で定義される ADN 機能に基づく。追加の機能は、以下の従属節で説明する。電話帳登録は、1 つの ADN ファイル上の 1 件のレコード、および任意選択で異なる EF に置かれている追加レコードで構成される。後者の場合、同じ電話帳に登録上のすべてのレコードをリンクするための機構を定義する。これらの機能は ME ではサポートされるが、USIM ではオプションである。

10.2.1 1 登録毎に 2 つの名前フィールドをサポート

同じ名前の 2 つの異なる表現(例えば、日本語文字とラテン語文字で)を許可するために、1 登録毎に 2 つの名前フィールドをサポートする。

10.2.2 1 登録毎に複数の電話番号をサポート

1 登録毎に複数の電話番号をサポートする。例えば、オフィス、家庭、ファックス、移動電話またはポケットベルなど。さらに、これらの属性を識別するための情報が必要である。

10.2.3 e メールアドレスのサポート

電話帳登録にリンクされる e メールアドレスをサポートする。さらに、これらのアドレスを識別するための情報が必要である。

10.2.4　ユーザーが定義できるグループ化のサポート

電話帳の登録をユーザーが定義するグループ(例えば、ビジネスとプライベートなど)にグループ化することをサポートする。

10.2.5　隠し登録のサポート

電話帳の登録を「隠し」としてマークする方法をサポートする。

10.2.6　登録の数

少なくとも 500 個の登録の格納をサポートする。

10.2.7　警告のモード

[FFS]

10.3　通話明細の格納

通話明細情報を格納するための機能をサポートする。通話明細情報は、以下の属性で構成される。

- 移動端末の着信通話
  通話してきた相手の電話番号、日付と時間、通話してきた相手の名前と通話状況(つまり、応答したか応答しなかったか)、通話時間と通話料金[FFS]
- 移動端末の発信通話
  通話した相手の電話番号、日付と時間、通話した相手の名前、通話時間と通話料金[FFS]
- 移動端末の発信通話と移動端末の着信通話とは別に、以前の通話の累積通話時間
- 以前の通話の累積料金情報[FFS]

明細の属性は、任意選択である。それらの属性を「未定義」とマークする値が利用できる。

注意１：通話相手の名前は、電話帳から利用できる。

注意２：複数の相手の通話情報の格納については、FFS である。

１１　3G/GSM の相互作用

11.1　3G ネットワークでの GSM 加入者

3G 22.101 [2]：「UMTS は、プレ UMTS 加入者が簡単に UMTS にローミングしそのサービスにアクセスすることを許可する。」

3G 22.100 [1]：「UMTS の移動端末は、フェーズ 2 とフェーズ 2+ GSM SIM を UMTS ネットワークへのアクセス・モジュールとしてサポートする。こ の場合に提供できるサービスは、UMTS ネットワーク内に提供される GSM のようなサービスに限定されることがある。

GSM SIM の使用を UMTS ネットワークでのアクセス・モジュールとして受け入れるかどうかは UMTS ネットワークのオペレータ次第である。」

11.2 GSM ネットワークでの 3G 加入者

次の要件が 3G 22.101 [2]に記述されている。「UMTS は、UMTS 加入者が簡単にプレ UMTS システムにローミングしそのサービスにアクセスすることを許可する。」

このことは、UICC での GSM 11.11 [8] に定義されているすべての必須要素を提供することによって達成できる。

この仕様では、GSM サービスを受けるために UICC を(GSM/ 3G) ME と GSM ME のデュアル・モードで使用することを許可する。

注意：このことは、例えば、UICC 上の PDC アプリケーションのサポートをしない、ということではない。

2 ローカルワイヤレスインタフェースに関わる動向

2.1 Bluetooth

2.1.1 方式概略

2.4GHz 帯を使った DFS の無線通信方式で低価格・低消費電力・互換性の高いことが特徴で、数年内に大半の携帯電話、ノート PC に搭載されると予測されている。

2.1.2 基本技術仕様

1）周波数帯

2.402～2.480GHz の 1MHz を 625μ秒毎に切り替えて使用する周波数ホッピング方式を採用

2）通信速度

1Mbps　音声 56Kpbs　データ 432.6Kpbs（対称）または 723/56Kbps（非対称）

3）同時接続性

全体で 8 台までの双方向同時通信が可能

（ただし 1 台はマスターで残り最大 7 台までのスレーブ間通信を中継する）

4）伝送範囲

Class 1　最大 100mW（20dBm）　通常 N/A　最小 1mW（0dBm）

Class 2　最大 2.5mW（4dBm）　通常 1mW（0dBm）　最小 0.25mW（-6dBm）

Class 3　最大 1mW（0dBm）　通常 N/A　最小 N/A

一般に 1mW（0dBm）で 10m、100mW（0dBm）で 100mが到達範囲と言われている。

5）ノイズ・干渉

周波数ホッピング方式のため妨害電波には強いと言われている。

6）消費電力

待機時が 1mW であり携帯電話にも搭載可能と言われている。

2.1.3 セキュリティ

セッション確立時に前もって知っているリンクキーによる相互認証を行うことが可能。またリンクキーから暗号化キーを生成し通信データの基本的な暗号化は実施。

2.1.4 標準化動向

Bluetooth コンソーシアムの SIG 活動で使用を作成。SIG 活動の特徴は利用場面を想定した標準化の作成と機器の互換性ホ確保するロゴ認証制度である。

SIG 活動では現在 V1.0 として Generic Access（機器の接続・認証）、Serial Port、FAX 、File Transfer（ファイル転送）等 13 個のプロファイルを制定済み。V2.0 として Automotive（自動車内のサービス）、Printing（プリンタ機器）、Human Input Device（マウス・キーボードなど）のプロファイルを検討中。決済については Financial Transaction として SIG 活動の前段階である Study Group で検討中。

2.1.5 特徴

1）グローバルな標準ワイヤレス技術

PC、携帯電話、ヘッドセット、プリンタ等の機器を無線で接続する標準ワイヤレス技術。世界 2000 社以上が賛同。

2）低消費・低価格・小型・軽量

待機時の消費電力 1mW で携帯電話にも搭載可能、目標価格は 5 ドル、切手並みのサイズ

3）ネットワーク構成が容易

アドレスの設定等不要で自動接続が可能

4）利用場面までを想定した仕様作成

利用場面から検討してプロファイルを設定しているため、利用度が高い。

2.1.6 利用に適した場面

1）Bluetooth の一般的使い方

・PC と携帯電話のワイヤレス接続、ワイヤレスヘッドセット、コードレス電話、LAN、小人数の会議での PC 情報交換、ワイヤレスプロジェクター、など

・LAN（無線 LAN）に比べてアドレス設定が不要なこと、通信のためのルータの準備が要らないことが長所

・IrDA に比べて最大 7 台までの同時接続が可能なこと、距離・方向の自由度があることがメリット

2）Bluetooth の決済応用案

・ドライブスルー等で予め注文が出せる

・有料駐車場の支払いである程度離れた距離からの支払いが可能

・非接触 IC カード、IrDA と比べて距離と方向の自由度が高い

・最大 7 台までの接続が可能なので、同時処理が可能

2.1.7 モバイルコマース適用への問題点

1）取引をする相手を特定するまでの手続きが必要なこと（セッション確立の手続きが必要）

Bluetooth は複数相手との同じ通信が可能であるが、取引では通常 1 対 1 取引と

なるため相手を特定する必要がある。IrDA や非接触 IC カードではこの操作は複数の相手とは通信が出来ないため、物理的に近づけることが相手を選択することになる。

2）相手を特定するために時間を要すること（セッション確立の時間がかかること）

Bluetooth で通信をするためには相手を特定する必要があるが、このためにはインクワイアリ（周りにいる BT 機器を発見しその固有 ID を得る操作）とページング（接続したい相手に呼びかけセッション確立の手続き）が必要である。インクワイヤリの推奨値として約 10 秒のウエイト時間が決められているため、高速化等の対策が必要と思われる。

3）相手の物理的特定

1）、2）で相手が無線通信上特定出来たとしも、それが本当に取り引きする相手かどうかの識別が出来ていない場合がある。例として POS レジで支払う場合、接続しているのは目の前の人ではなく後ろに並んでいる人かもしれない。

2.1.8 モバイルコマースへの適応事例

2000-12-19、Ericsson と ICA（ノルウェーの販売グループ）が小売店での Bluetooth での支払い実験をおこなったのが最初で唯一の例。

詳細は不明だが POS レジと WAP 対応電話機の間での支払いで、現金やクレジットカードよりも速くてたやすいとの評価をしている。

2.2 IrDA

2.2.1 はじめに

昨今のインターネットサービスの急速な普及は，パソコンや携帯情報端末，あるいは携帯電話によるモバイル環境におけるデータ通信の需要を一気に押し上げた。このようなデジタル化の流れの中，赤外線通信技術は Bluetooth などに代表される高周波通信技術とならんで，「いつでも，どこでも，誰とでも」通信が可能なコードレスのモバイルコンピューティング環境を実現する技術として新聞や雑誌紙上を賑わしている。

その一方で，IrDA というキーワードは知られているものの，IrDA の規格にはどう言った仕様があるのか，それぞれの仕様が何を規定しているのか，またその違い・関係についてはあまり知られていない。ここでは，それぞれの規格誕生の背景にも触れながら各規格の位置づけとその概要，そして応用について解説する。

2.2.2 IrDA 規格の概要

IrDA の規格は，大きく 2 つのプラットフォームに分類することが出来る。データ通信用プラットフォーム（図 2-1）と，機器制御用プラットフォーム（図 2-3）である。IrDA では，データ通信用プラットフォームを総称して IrDA-Data 規格と呼び，機器制御用プラットフォームを IrDA-Control 規格と呼んでいる。

2.2.2.1 機器を向かい合わせてデータ交換をする規格 ～ IrDA-Data

IrDA-Data 規格は，「機器を向かい合せるだけでデータ交換ができる」使い勝手の良い赤外線通信機能を実現し，異なるメーカ／異なる機器を相互に接続することを目的として策定された規格である。IrDA-Data 規格は，これら機器間のシリアルケーブル，あるいはパラレルケーブルを双方向の赤外線通信に置きかえることで，1m 程度の短い通信距離での簡単なワイヤレス接続を可能にする。

IrDA-Data 規格は，赤外線送受信部の物理的な仕様や変復調方式など通信の基本部分を規定した物理層規格(SIR)と，機器間で透過的かつ信頼性のある通信路を提供するために通信の制御を行うデータリンク層規格(IrLAP, IrLMP)，そして様々な応用を実現する上位層規格(Tiny-TP, IrCOMM, IrOBEX など)から構成される。

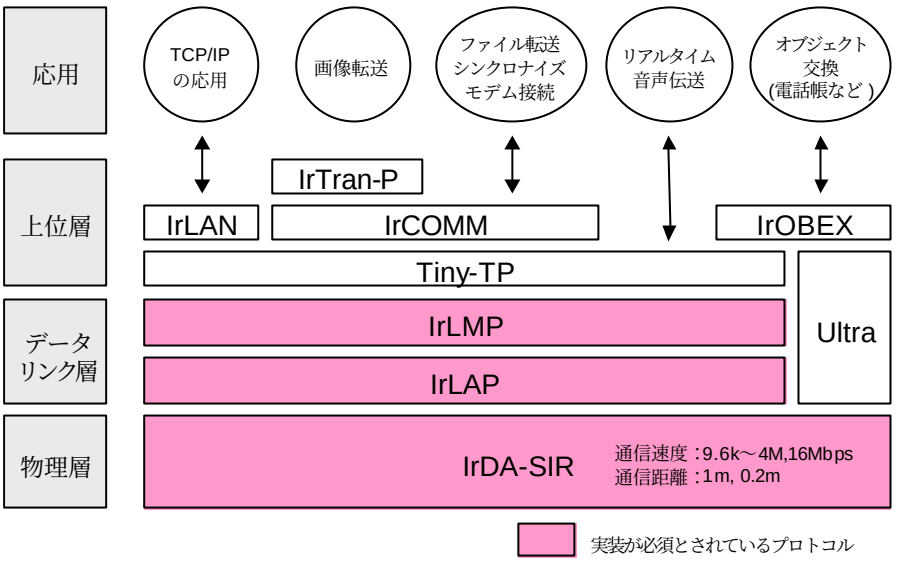


図 2-1 IrDA-Data 規格のプロトコルスタック

2.2.2.2 物理層規格（SIR）

IrDA-Data 規格の物理層（SIR）は，通信距離 1m，±15 度の範囲において 1 対 1 の無線通信を実現する赤外線通信方式を規定している。当初 SIR に対しては，次のような要求仕様が挙げられた。

- シリアル／パラレル通信ケーブルを赤外線で置き換えられること。
- 最低でも RS232C 通信と同じ 115.2kbps 程度の伝送速度ができること。
- UART が通信コントローラに使用できること。
- 通信範囲は 0～1m（オプションで 3m）を満足すること。
- 通信形態は指向型の 1 対 1 通信でよい。
- 数ドル程度のコストでハードウェアが実現できること。

この要求を満足する解として最初に制定されたのが，SIR1.0 規格（9.6 kbps ～ 115.2 kbps の方式）である。SIR1.0 規格では，ハードウェアのコストを低減するために，UART に簡単なパルス圧縮・伸長回路を加えるだけで実現できる RZI(Return to Zero Inverted) 方式を変調方式に採用した。SIR 規格では，変調方式のほかに，通信方式，データ速度，赤外線の放射強度，通信距離や角度などを規定している。[1]

SIR 規格は，通信の高速化や低消費電力の要望増大に伴い，これまでに幾度かバージョン改訂が行われている。現在ノート PC を中心に最も普及しているのが 1995 年の 10 月に規格化された SIR1.1 規格（SIR1.0 規格に 576kbps/1.152Mbps/4Mbps を追加したもの）である。SIR1.1 規格では，4Mbps の高速通信を実現するために，4 値 PPM(Pulse Position Modulation)方式と呼ばれる変調方式を採用した。4PPM 方式では，シンボル時間を 4 つの

スロットに分割し,赤外線パルスの位置によって2ビットの情報を表現できる。また,SIR1.1規格では，同期方式が調歩同期方式からフレーム同期方式に変更されている。

SIR 規格は，その後も消費電力の低減を目的として短距離通信モード（省電力オプション）が追加され（SIR1.2/1.3 規格），1999 年 10 月には通信速度が 16Mbps の方式が新たに追加された[2]。以下に各 SIR 仕様の概要を示す。（下表）

表 2-1 SIR 規格一覧

項目	仕様			
	SIR1.0	SIR1.1		SIR1.4 (仮称)
通信速度	9.6kbps~115.2kbps	576kbps, 1.152Mbps	4Mbps	16Mbps
通信距離	0~1m 標準) 0~20cm (SIR1.2 省電力オプション)	0~1m 標準) 0~20cm (SIR1.3 省電力オプション)		0~1m 標準)
通信方式	調歩同期式	フレーム同期式		フレーム同期式
変調方式	RZI方式	RZI方式	4値PPM方式	HHH(1,13)方式
最小放射強度	40mW/sr 標準) 3.6mW/sr (SIR1.2 省電力オプション)	100mW/sr 標準) 9.0mW/sr (SIR1.3 省電力オプション)		100mW/sr
通信角度	±15°以上	±15°以上		±15°以上

2.2.2.3 データリンク層・上位層

データ通信を行うために必要となる通信規約は，データリンク層以上で規定されている。データリンク層以上の各プロトコルの働きを図 2.2 に示す。IrDA-Data 規格のデータリンク層のプロトコルには，IrLAP(Infrared Link Access Protocol)と IrLMP(Infrared Link Management Protocol)があり，これらのプロトコルを実装することが必須となっている。

IrLAP は，HDLC (High level Data Link Control) をベースにした通信プロトコルであり，物理層の上で信頼性のある Point to Point の通信路を提供する。以下に IrLAP の規定概要を示す[3]。

- 4 バイト長のアドレス（局アドレス）を使用して局を識別する。
- 両局間の最適通信速度を決定する。IrDA-Data では，これまでに複数回のバージョン改訂が行われているため，通信開始時に両局間の最適通信速度を決定しておく必要がある。通信速度のネゴシエーションは，9.6kbps で行う。

・半 2 重不平衡モード（一方が親局、他方は子局となり、親局が送信権を制御する動作モード）を使用する。赤外線通信では，2 つの局が同時に送信すると混信して正しく通信ができないため（半 2 重の通信路であるため），本モードを用いてメディアアクセス制御を行う。
・エラー訂正とフロー制御機能を有する通信路（データリンクコネクション）を上位層に対して提供する。
・最大パケット長は、64／128／256／512／1024／2048 バイトから選択できる。
・エラー検出には 16 bit（4Mbps 時は 32 bit）CRC を使用する。

一方 IrLMP は，確立した 1 本の伝送路で上位層に対して複数のデータコネクションを提供する多重機能や，両局のサービス機能の問い合せ方法について規定している[4]。

IrDA-Data 規格の上位層のプロトコルには，Tiny-TP，IrCOMM，IrOBEX，IrTran-P などの規格がある。これらはいずれもオプション規格という扱いになっている。しかしながら，OSI のトランスポート層に相当する Tiny-TP は，現在ほとんどの IrDA-Data 規格準拠製品に実装されており，事実上の必須規格になっている。Tiny-TP は，データリンクコネクションのフロー制御を行う。IrLAP がおおもとの 1 本のデータリンクのフロー制御を行うのに対して，Tiny-TP は IrLMP によって多重化された個々のデータリンクのフロー制御を担当する[5]。

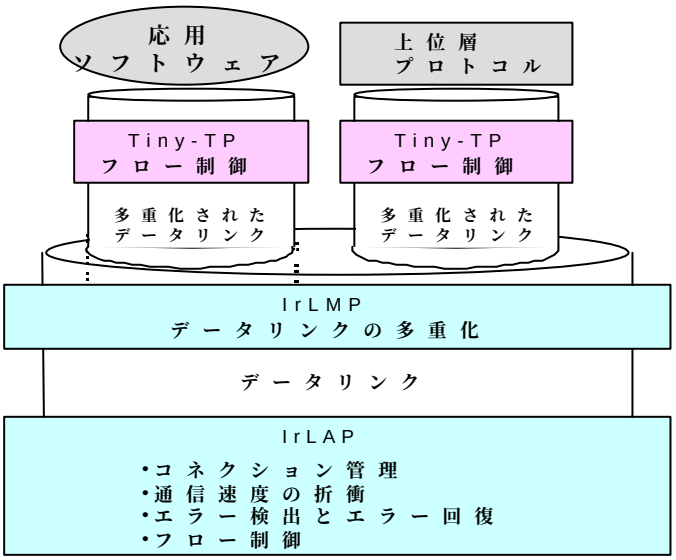


図 2-2 各プロトコルの働き

その他の上位層プロトコルの規定概要を以下に示す。（表 2-2）

表 2-2 IrDA-Data 規格の上位層プロトコル

プロトコル	プロトコル概要
IrCOMM	パソコンのパラレル／シリアルポートをエミュレーションするための規格[6]。この規格を利用することで、パラレル／シリアル通信ポートを使った既存のパソコン用アプリケーションソフトウエアを変更することなく、接続ケーブルを赤外線に置き換えて使用することができるようになる。
IrOBEX	インターネットの HTTP (HyperText Transfer Protocol) に類似した機能を持つ。この規格を利用することで、両局間でアドレス帳などオブジェクトデータを送受信することができる [7]。
IrTran-P	SCEP (Simple Command Execute Protocol), bFTP (Binary File Transfer Protocol), UPF (Uni Picture Format) のプロトコル群の総称。 静止画像を確実に送信するためのコマンドや画像フォーマット、圧縮方法、色コーディングなどを規定している[8]。

2 年ほど前まで IrDA は，SIR，IrLAP，IrLMP，Tiny-TP，IrCOMM の物理層から上位層までのプロトコルを標準規格として策定し IR 通信の普及活動を推進してきた。複数のベンダーから高性能な赤外線トランシーバが安価で販売されるようになり，PC 用のチップセット（Super I/O）に SIR を実現するためのデジタル回路が内蔵され，PC の最も普及している OS である Windows95 に IrLAP，IrLMP，Tiny-TP，IrCOMM のプロトコルが実装された事で 1996 年には，ほとんどのノート PC に IrDA-Data 用のハードウェア（赤外線トランシーバと通信コントローラ）が標準搭載されるまでに至った。

しかしながら，ノート PC に標準搭載された IR 通信もその他の機器にはなかなか浸透しなかった。またノート PC についても，搭載されている IR 通信機能がユーザに十分活用されていない状況が明らかになった。いくら優れたテクノロジーでも，「ユーザが好む利便性の高い応用がなければ，誰も IR 通信を利用しない」という市場の実態を如実に反映していたのである。この頃から IrDA は，キラーアプリケーション（IR 通信を最も有効に活かす応用）を求めるようになり，特定の応用を睨んだ標準規格化を進めるようになった。このようにして誕生した規格が IrTran-P や IrMC である。

2.2.3 キラーアプリケーションとしての期待 ～ IrMC

IrDA-Data 規格のうち，IrDA が最近最も期待しているものに IrMC がある。IrMC は IrDA 赤外線通信を携帯電話に利用する際の応用規格である。携帯電話という市場規模そのものに IrDA が期待している部分も少なくないが, 携帯電話経由のパケット通信網の利用や, 携帯電話そのものによる電子メールやインターネットの利用などにより, 携帯電話とその他機器間でのデータのやり取りそのものの需要が高まっているからである。

IrMC 規格を策定するにあたって，IrDA がまとめた要求仕様は以下の通りである。

・携帯電話小型化・薄型化を妨げないよう，デバイス（赤外線トランシーバ）自体が十分小型で実現できること。

・携帯電話の待受け時間・通話時間を圧迫することのないよう，IR 通信機能を実現するハードウェア（主に赤外線トランシーバ）は，十分な低消費電力化を図れること。

・これまでに IrDA-Data が実装されている PC/PDA などとの相互通信が確保できること。

・ページャなど処理能力の低いハードウェアを持つ端末との通信も可能であること。

上記要求を受けて, Ericsson, Nokia, Motorola, NTT DoCoMo などが中心になって IrMC 規格をまとめあげた。IrMC では，携帯電話における赤外線通信の応用として，電話帳やスケジュール, メッセージやノートなどのオブジェクト交換, データ通信（モデムアクセス），音声通信の 3 つを想定して関連する事項を定義している。IrMC は，既にアメリカ・ヨーロッパを中心に Nokia，Motorola，Ericsson の携帯電話に実装されており，国内では Nokia の DoCoMo 向け携帯電話（NM502i）にも実装されている。これらの携帯電話機では，携帯電話にいちいち電話帳やスケジュールを入力しなくても，PC 上の PIM ソフトウェア（Microsoft Outlook）から，電話帳・スケジュールをそのまま転送できてしまう。また特殊なソフトウェアを PC にインストールしなくても, PC の IR 通信"窓"の横に携帯電話を置くだけで，ネットワークにダイヤルアップ接続できてしまう。

IrMC は，下位層から上位層まで実に様々なことを定義しており，新たに策定されたプロトコルも含め，携帯電話向けの実装ガイドラインとなっている。以下に IrMC 規格の概要を示す[9]。

(1) SIR，Low Power Option として短距離通信モードを追加。

これまでの SIR（Version 1.1）規格では，全ての機器は 1m 以上の距離で通信できなければならなかった。1m 以上の通信距離を達成するためには，LED（赤外線発光素子）に数 100mA の電流をながす必要があり，消費電力を可能な限り低減したい携帯電話にとっては非常に厳しい仕様であった。その一方で，携帯電話での応用を想定した場合，通信距離は 20cm 程度あれば実用上問題ないという意見が多かった。この理由から，通信距離は 20 cm 以上あれば良いという新しい条件（Low Power Option）が SIR 規格に追加され，Version 1.2(〜115.2kbps)/1.3(576kbps/1.152Mbps/4Mbps)に更新された。（表 2.1）

(2) 下位層プロトコルに SIR，IrLAP，IrLMP，Tiny-TP を用いる。

ただし，簡易手順として IrLAP，IrLMP，Tiny-TP の代わりに Ultra を用いても良い。IrMC では上記 3 つの応用（オブジェクト交換, モデムアクセス, 音声通信）全てにおいて，SIR から Tiny-TP までのプロトコルを用いることを原則としている。しかしながら，ページャのようにハードウェア上の制約が大きい機器では, これら全てのプロトコルを実装することは困難である。そこで IrMC では，ハードウェアの制約が大きい小型機器向けにコネクションレス型の簡易プロトコルである Ultra プロトコルを定義した。Ultra はオブジェクト交換にのみ使用できる。

(3) データ通信用上位層プロトコルとしては，IrCOMM を用いる。

パソコンなどを携帯電話と赤外線で接続し，公衆回線を使ってデータ通信を行う場合には IrCOMM プロトコルを用いる。Windows95 以降は，OS に標準的に IrCOMM までのプロトコルが搭載されているため,特にパソコン側にソフトウェアを追加する必要もなくデータ通信ができる。

(4) オブジェクト交換用上位層プロトコルとしては，IrOBEX を用いる。

(5) オブジェクト交換フォーマットとして次を用いる。

オブジェクト交換の応用では IrOBEX を使用する。IrOBEX は，IrDA-Data 規格のセッション層の統一的なプロトコルとして利用することが，IrDA によって推奨されている。但し，セッション層を同じにしても，肝心のオブジェクトフォーマットが異なっていると機器間で交換することができないため，IrMC では以下のように，交換するオブジェクトの各種のフォーマットを定めている。

- 電話帳：vCard 2.1（Internet Mail Consortium が定めている vCard フォーマット）
- カレンダ：vCalender 1.0（Internet Mail Consortium が定めている vCalender フォーマット）
- メッセージ：vMessage（IrMC が新たに定義したフォーマット）
- ノート：vNote（IrMC が新たに定義したフォーマット）

(6) 音声伝送方式を新たに定義する。

従来通りの IrLAP から Tiny-TP までのプロトコルを使ってリアルタイム音声伝送する方式が規格として採択された。従来通りのプロトコルによるリアルタイム通信は，NTT，松下電器，NEC が実証して見せた。

2.2.4 家電製品への普及に向けて ～ IrDA-Control 規格

IrDA-Data 規格は，PC，プリンタやデジタルカメラなどの周辺機器，あるいは PDA や携帯電話などの携帯機器まで幅広い製品に普及してきた。先述の通り，IrDA-Data 規格は PC や PDA などで使用していたケーブル通信（PC 同士をクロスシリアルケーブルあるいはパラレルケーブルで接続して通信するもの）の無線化を狙ったものである。この応用においてはメガバイトオーダーのファイルを交換する場合も多々あり，高速性が要求された。このため，IrDA-Data では通信範囲を短い距離にしぼり，16 Mbps までの高速通信を実現している。

しかしながら，IrDA の悩みはこれら情報端末よりも格段に市場規模の大きい家電製品市場に赤外線通信を普及させられないことにあった。そこで策定された規格が，IrDA-Control 規格である。

2.2.5 IrDA-Control 規格の概要

IrDA では，1996 年末頃から IrDA-Data とは全く異なる IR 通信についての議論を開始

した。この IR 通信は IrDA-Control と呼ばれており，マウスやキーボード，ジョイスティックといったパソコン入力機器の無線化や，セットトップボックスなどのデジタル家電用リモコンの高機能化など，機器の制御や少量の情報交換を目的とした規格を標準化しようというものである。要求仕様の策定から様々な議論を経て，1998 年 2 月にシャープ，マイクロソフト，インテル，HP の４社が共同提案した"IrBus"が，IrDA-Control 規格として採用された。

IrDA-Control 規格は，Data 同様，双方向の赤外線通信であることに変わりはない。しかしながら，家電製品の制御という目的から，リモコンなみの長距離・広範囲の通信領域で，1 台のパソコンあるいはデジタル家電に複数台の入力装置を接続する規格となっている[10]。

IrDA Control 規格も，赤外線送受信部の物理的な仕様や変復調方式など通信の基本部分を規定した物理層規格と，1 対 n の通信の制御を行うデータリンク層規格から構成される。（下図）なお，IrDA-Data 規格と IrDA-Control 規格の通信方式は全く互換性が無く，互いに通信はできない。

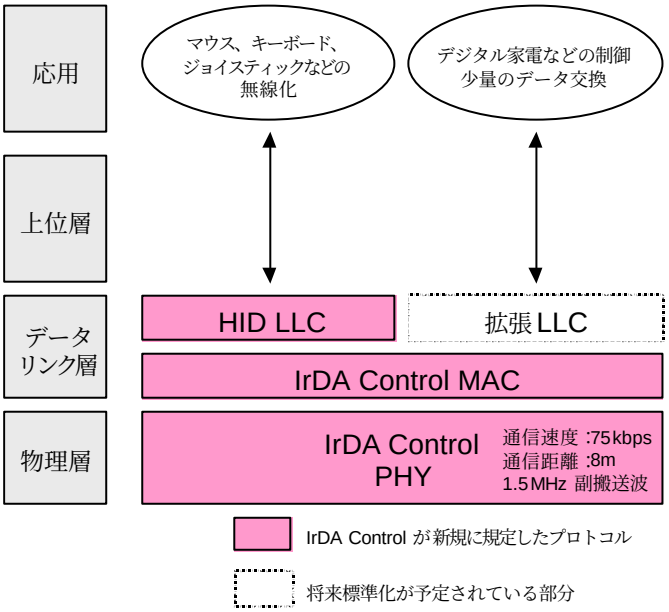


図 2-3 IrDA-Control 規格のプロトコルスタック

IrDA-Control の物理層規格では，通信距離が最低 5m と IrDA-Data 規格に比べて長距離化されている。長距離通信実現のために，蛍光灯から悪影響を受けにくい 1.5MHz の副搬送波を用いた ASK(Amplitude Shift Keying)方式を変調方式に採用した。通信速度は 75kbps と低速であるが，従来のリモコンの通信速度と比較しておよそ 70 倍の容量があるため，少量の情報転送の応用も可能である。

IrDA-Control システムは，1 台のホストと複数台のペリフェラル（最大 8 台まで）から構成される（下図）。例えば，パソコンはホストとして，マウスやキーボードなどの入力周

辺機器はペリフェラルとして動作する。

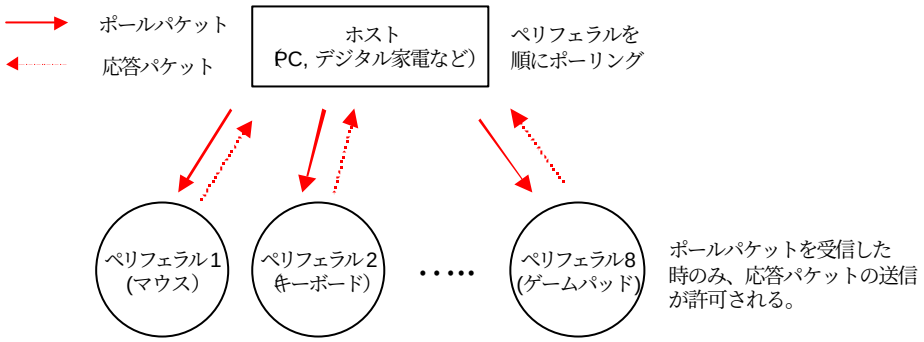


図 2-4 IrDA-Control システム

IrDA-Control 規格のデータリンク層は，ホストが複数台のペリフェラルと同時に赤外線データ通信できるよう設計されている。ホストは各ペリフェラルに対してポーリングを行い，ペリフェラルの通信を制御する。各ペリフェラルは，ホストからポールパケットを受信したときにのみその応答としてパケットを送信することが許可される。ホストは 13.8 ミリ秒の周期の間に 4 つのタイムスロットを持ち，ペリフェラルのポーリングを行う。4 台以上のペリフェラルがシステムに登録されている場合は，次の周期にまたがってスロットを割り付ける。

2.2.6 デジタル家電の革命児となるか IrDA-Control の応用

IrDA-Control の有力な応用としては，双方向のデータ伝送性と 75kbps の通信速度を活かし，従来のリモコンの機能を拡張する新しいリモコンへの展開が検討されている。

例えば，デジタル放送で配信される電子番組表（EPG, Electronic Program Guide）を，セットトップボックスから手元のリモコンにダウンロードし，リモコン上の液晶画面上に表示させることで，番組内容を手元で確認しながら番組の選択をしたり，ビデオの録画予約をしたりするといったことができるようになる。また，家庭内の各機器からリモコンに操作メニューをダウンロードし，ユーザが操作メニューを組合せることで，部屋の照明を消すと同時に，テレビやエアコンの電源も切るといった家電の連携動作などが可能になる。近い将来，IrDA-Control を活用したこれまでにない新しい製品が期待される。

2.2.7 おわりに ～ IrDA における最近の標準化動向

現在の IrDA での標準化活動は，特定応用を目的とする新しいプロトコルの開発から，IrDA 規格のさらなる普及を目的とする IrDA 規格を実装するためのガイドラインの策定にシフトしつつある。

1993 年 6 月の発足以来，IrDA では IR 通信を使った応用および IR 通信の市場拡大を目指して，様々なプロトコルの標準化を非常に早いペースで行ってきた。その結果，様々な

製品・応用に IrDA が利用された反面，実装方法の相違による相互通信性の欠如が浮き彫りとなり，「使いにくい」という評価が紙面を賑わすようになってしまった。

そこで IrDA では，「機器を向かい合わせてさっとデータを渡す」という IrDA が最も得意とする応用，すなわち，近距離でのファイルや画像データの転送，印刷，モデムアクセス，データのシンクロナイズといった応用毎に，実装上の規約をガイドラインとして明確にして，相互通信性が保証されるようにしようということになった。 この実装ガイドラインは，プロファイルと呼ばれる。プロファイルは，実装したい応用について，下位層から上位層までどの通信プロトコルのどのサービスを実装しなければならないかを規定している。2000 年 4 月には，このプロファイルの第一段として，1 対 1 の機器間でのオブジェクトデータの交換を実現するための"Point and Shoot"プロファイルが策定された。今後もモデムアクセスなどのプロファイルが策定されていく見通しである。

【参考文献】

[1] Infrared Data Association, Serial Infrared Physical Layer Specification Version 1.3. October 15, 1998

[2] Infrared Data Association, Serial Infrared Physical Layer Specification for 16Mb/s Addition, Errata to IrPHY Version 1.3, January 8, 1999

[3] Infrared Data Association, Serial Infrared Link Access Protocol (IrLAP) Version 1.1, June 16, 1996

[4] Infrared Data Association, Link Management Protocol Version 1.1, January 23, 1996

[5] Infrared Data Association, 'Tiny TP': A Flow-Control Mechanism for use with IrLMP Version 1.1, October 20, 1996

[6] Infrared Data Association, 'IrCOMM': Serial and Parallel Port Emulation over IR Version 1.0, November 7, 1995

[7] Infrared Data Association, IrDA Object Exchange Protocol IrOBEX Version 1.2, March 18, 1999

[8] Infrared Data Association, IrTran-P (Infrared Transfer Picture) Specification Version 1.0, October, 1997

[9] Infrared Data Association, Specifications for Ir Mobile Communications (IrMC) Version 1.1, March 1, 1999

[10] Infrared Data Association, IrDA Control Specification (Formerly IrBus), IrDA CIR (Control IR) Standard, Final Specification, Final Revision1.0, June 30, 1998

2.3　非接触 IC カード（近接型）

2.3.1　方式概略

非接触 IC カードインタフェースは，電磁誘導結合によってカードへの電力伝送を行うとともに，変調してデータの伝送も行う。IC カードとリーダ間の非接触インタフェースは，交通機関や，公衆電話機の決済カードとしての実績がある。

携帯電話機への実装形態としては，①非接触 IC チップを内蔵し，外観は，携帯電話機であるが，IC カードとして機能し，移動体通信網の利用や外部機器のリーダとの通信を行う形態と，②非接触 IC チップおよび非接触リーダライタも内蔵し，①と同様に外部機器との通信に加えて，外部非接触 IC カードとの通信も可能とする２形態が考えられる。

IC カードは，耐タンパー性の高い IC チップを内蔵するため，高セキュリティであり，決済処理に適している。また，通信可能距離が（磁界強度によるが）数 cm と短いため，携帯電話機を外部機器に近づける必要があり，この行動自体が所有者の意志確認に利用できる。

非接触近接型 IC カードの規格は， ISO/IEC14443 に規定されているが，変調方式の違いにより２種類の Type A および Type B があり，さらにオプションとして日本より Type C が提案され，審議中である。

Type A，Type B および Type C ともに搬送波周波数は，13.56MHz とし，電磁誘導結合によってカードへの電力伝送を行うとともに，変調してデータの伝送も行う。

(1) リーダからカードへの伝送：

Type A は，ASK100%変調を用い，変形ミラー符号化方式で，通信速度 106kbps ある。

Type B は，リーダからカードへの伝送において ASK10%変調を用い，NRZ-L 符号化方式で，通信速度は，106kbps である。通信速度は，あとで 212kbps，424kbps に変更できる。

Type C は，リーダからカードへの伝送において ASK10%変調を用い，マンチェスタ符号化方式で，通信速度は，212kbps，424kbps，848kbps の選択で使用可能である。

(2) カードからリーダへの伝送：

Type A および Type B は，カード側で負荷変調することにより，847kHz（＝13.56MHz/16）の副搬送波を発生しする。さらに，

Type A は，この副搬送波をマンチェスタ符号化方式で OOK(ON/OFF キーイング)する。

Type B は，この副搬送波を NRZ 符号化方式で BPSK（２値位相偏移キーイング）する。

Type C は，副搬送波を使用せず，リーダとカードの双方向ともにマンチェスタ符号化方式である。

2.3.2　基本技術仕様

－ 搬送波周波数：13.56MHz

－ 通信速度：106kbps（衝突防止処理中）その後，プロトコル変更により変更可。

Type C：212kbps，424kbps，848kbps の選択で使用可

- 同時接続性：原理的には無制限であるが，重ねた場合など実質 3 枚が限度。
- 伝送距離：具体的に距離の規定はなく，動作磁界強度で 1.5A/m～7.5A/m と規定される。携帯電話機に搭載する場合は，消費電力の面から通信可能距離に制約を受ける。カードの消費電力にもよるが，磁界強度 1.5A/m で 10cm くらいを考慮している。
- セッション確立時間：約 5ms 以下
- 雑音・干渉：干渉を避けるためには，携帯電話機内にシールドが必要であるが，その場合通信可能距離が犠牲になることがある。カードからの微小信号を確実に復調するために，副搬送波を同期検波することにより，強力な送信磁界の中でランダム雑音を排除し，S/N 比が向上する。一方，マンチェスター符号を用いた方式では，転送速度を基準にした同期検波で S/N 比を向上させられる。
- 消費電力：カードは，5～10mW (マイクロプロセッサをもたないロジック回路で構成し，少容量，単機能ならば，0.1～0.2mW の IC チップもある)。リーダは，アンテナ出力で，1W 以下としなければならない。実際，携帯端末にリーダライタを内蔵する場合，電池消耗を考えると，カードとリーダを密着させた状態で運用することになるであろう。

2.3.3 セキュリティ

セキュリティ機能が１チップ内に組込まれているため，耐タンパー性が高い。

Type A, Type B ：上位アプリケーションレベルで考慮されなければならない項目である。

TypeC（FeliCa 技術方式）では，OS の機能により，Triple DES 等の暗号化通信を実現している。

2.3.4 標準化動向

現在，これらの標準化の状況は，下記の通りである。

Type A および Type B については，ISO/IEC 14443-1,-2,-3,-4 および試験方法の ISO/IEC10373-6 が完了している。それに追従して，JIS 化(JIS X 6322-1～3，6305-6)の作業も平成 12 年度に行われ，平成 13 年度に残りの JIS X 6322-４の作業を進める。

Type C については，日本提案として，電気的インタフェース規格を ISO/IEC 14443-2AMD1 に搭載することが決まり，2002 年 2 月の ISO 登録を目途として現在審議中である。

2.3.5 特徴

- 即時性が有る。

端末捕捉からセッション開始までの時間は，約 5ms と短い

- 位置決め精度は，荒くて良い。
  通信範囲は，基地局リーダのアンテナを中心とし半径 10cm 以内の半球状に非接触 IC カードまたは非接触 IC チップを搭載した携帯端末を移動させても通信が可能になる。
- リーダ１に対してカードまたは端末を最大 3（枚，台）まで通信が可能である。
- 高い耐環境性
  汚れ等の劣悪環境でも使用可能
- 端末の消費電力，アンテナ形状，アンテナ出力により通信可能距離が大幅に変化する。
- Type A は，日本の電波法の下で使用する場合に出力に制限を受け，通信可能距離が短く，リーダにカードまたは端末を密着させて運用する必要がある。
- Type C は，リーダとカードの双方向で，変調方式および符号化が同じであるため，携帯電話機内蔵のリーダは，外部非接触 IC カードの読み書きする（例えば，ビューアとして）こと，および外部機器のリーダとリーダ間通信することが可能となる。

2.3.6　利用に適した場面

【利用場面】

- 高速処理が必要とされる状況
- 決済処理等のセキュリティが必要とされる状況
  （TypeC の FeliCa 技術方式は，セキュリティを上位層で規定）

【用途】

- ユーザー認証
  改札ゲート，入退室カード
- 決済系データ通信
  電子マネー，プリペイド
- オブジェクト交換
  ポイントサービス

2.3.7　モバイルコマース適用への問題点

- 移動機実装の検討が必要
  電磁誘導により電力搬送を行っているために，周辺に金属が存在すると通信距離に制限が生じる場合がある。
- 店舗側への非接触インタフェース対応機器の配備が重要課題である。

2.4 非接触 IC インターフェース(FeliCa 技術方式)のモバイルコマースへの適用

2.4.1 方式概略

非接触IC カード機能とリーダライタと呼ばれるカード通信機能を耐タンパー性を施したIC チップ内に実装し、以下の 3 通りの使用方式を実現する。

・携帯電話と内蔵 IC カードとの通信
携帯電話にセキュアなメモリ部分（内蔵 IC カード）を備えることができ、サービスを格納した電子財布として使用する際に、バリューダウンロード及び携帯電話通信網を経由した決済が可能になる。

・内蔵 IC カードと外部リーダライタとの通信
携帯電話内のセキュアなメモリに保持されたバリューを用いて、リアルの端末でのサービス実行（例えば、物品購入決済やチケット利用など）を行う。

・外部 IC カードの読み取り
携帯電話ビューワとしての利用や、携帯電話通信網を利用した外部 IC カード内に保持されたサービス利用を行う。

2.4.2 基本技術仕様

FeliCa 技術方式は、ISO14443-2 Type C として審議中であり、特徴的な仕様は以下のとおり。

・通信速度：212kbps、424kbps、848kbps の中から選択可能

・通信方式：同期通信で対称型の通信であり、ローカルインターフェースとして 1 対 1 の携帯電話/携帯電話間（リーダライタ間どうし）での通信を容易に行うことができる。

2.4.3 消費電流

・待機時： 2μW 以下

・リモートアクセスモード（リーダライタ動作時）： 約 160mW

・カード互換モード（カード動作時）： 5mW 以下

2.4.4 セッション確立時間

リーダライタからの呼びかけに対し、5m sec 程度で携帯電話内蔵 IC カードの固有番号を返答し、リーダライタとのセッションを高速に確立できる。

2.4.5 セキュリティ

IC カードとしての耐タンパー性を備え、かつ OS に組み込まれた Triple DES 相互認証機能と、トランスポート層に組み込まれたセキュリティ機能の融合により、セッション中の

通信データを暗号化し盗聴・改ざん等のセキュリティ脅威への対抗を実現している。

2.4.6　特徴

2.4.6.1　非接触 IC カード機能

・駅の改札等混雑が予想される場所においてスムーズに料金徴収が行えることを目的として設計されたものであり、モバイル EC で要請される高速処理が実現できる。

・通信距離の制限として 10cm 以下となっていることから、不慮のサービス実行防止および利用者の意志によるサービス実行が容易にコントロールできる。

・非接触 IC カード/リーダライタ間での通信時に、不用意な通信切断等による障害に対し、サービス実行の中間状態をもたず、実行前の状態もしくは実行後の状態を保証する。

・複数ファイルの同時書き込みにより、複数サービス（例えば、チケットダウンロード/決済など）の一括処理が行えるため、通信安定性がない状態でも適正な利用が可能になる。

・携帯電話の表示機能を利用して、オンライン/オフラインビューワが実現できる。
携帯電話から電力供給を受けることにより、携帯電話組み込み小型アンテナにおいても充分な通信距離が実現できる。

2.4.6.2　リーダライタ機能

・外部 IC カードを表示する手段として、オンライン/オフラインビューワが実現できる。

・携帯電話をリーダライタ端末として機能させ、外部 IC カードでのサービス実行ができる。

2.4.7　利用に適した場面

・人の動きを停止させない高速処理が必要とされるモバイル EC 特有の利用環境
改札ゲート、入退室

・セキュアなサービス実行を必要とされる場面
決済系サービス

・サイバー上での物品購入
非接触 IC カード機能による携帯電話通信網を介した物品購入/決済

2.4.8　モバイルコマース適用の問題点

・携帯電話への実装用の工夫が必要であり、また実使用上の検証が必要。

2.4.9　モバイルコマースへの適用事例

非接触 IC カードを用いた、バスや鉄道の交通機関でのゲートコントロールや、プリペイド型電子マネー、入退室用 ID 管理、またこれら複数のサービスを一枚のカードで提供する

技術が、既に実用化されている。

モバイルコマースへの適用は、前記項目を含め以下のような特徴を利用した開発が進んでいる。

・同時書き込み 8 ブロックでの複数サービス書き込み保証処理

・複数ファイル同時処理によるサービス提供/同時決済処理の用途に適合

・リーダライタとカードの組み合わせでのメンテナンスが容易

・複数事業者による利用の場合に階層別に管理可能

・フィールドによるサービスの追加が容易

3　Bluetooth“技術動向とその応用

Bluetooth“技術動向とその応用”

次世代モバイル端末用
近距離無線インターフェース

2001年1月11日

お話しする内容

1. Bluetoothの特徴
2. Bluetoothの仕様概要
3. Bluetooth搭載製品の商品化手順
4. Bluetoothを用いたシステムイメージ

1．Bluetooth の特徴

1）グローバルな標準ワイヤレス技術

2）低消費・低価格・小型・軽量

3）ネットワーク構成が容易

4）利用場面までを想定した仕様作成

5）SIG（Special Interest Group）活動

ハラルド・ブルートゥース II世
（デンマークの王 940-981）

1）グローバルな標準ワイヤレス技術

◆PC、携帯電話、ヘッドセット、プリンタ、デジカメなどの機器を無線で接続する標準ワイヤレス技術

◆無免許で利用できる周波数を利用（2.4GHz）

◆グローバルな規格

“プロモータ”9社が中心に仕様作成作業を推進。

全世界の2000社以上が賛同。

2）低消費・低価格・小型・軽量

◆モバイルに適した、低消費電力、低価格、小型化

・不使用時には低消費電力モードで省エネ可能

・待機時の消費電力：1mw
　携帯電話にも搭載可能
・5ドル目標（現在：20～30ドル）
・切手なみサイズ
　携帯電話にも搭載可能

3cmX1.5cm
厚さ3.5mm

待機時：3ヶ月
データ通信：120時間
音声通信：75時間

エリクソン社製送受信モジュール

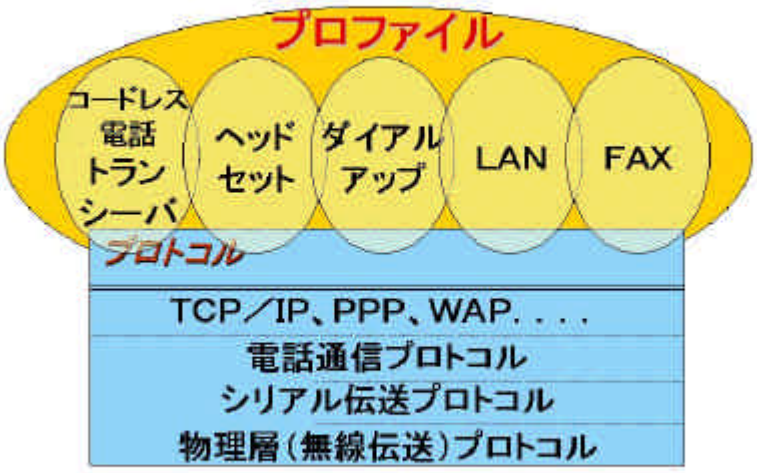
3）ネットワーク構成が容易

◆複雑な設定は不要で、自動接続が可能

◆常時接続ではなくAd-Hoc 接続

Buetoothの
ネットワークが
できる

4）利用場面までを想定した仕様作成



13個のプロファイルを定義（さらに、11種類を策定中）

7

13個のプロファイル：V1．0

♦Generic Access	機器の接続・認証
♦Service Discovery	サービスクラスの認識手順
♦Serial port	シリアルポート
♦Cordless Telephony	コードレス電話
♦Intercom	トランシーバ
♦Headset	ヘッドセット
♦Dial-up Networking	ダイアルアップ接続
♦FAX	FAX
♦LAN Access	LANアクセス
♦Generic Object Exchange	オブジェクト交換
♦Generic Object Push	オブジェクトプッシュ
♦File Transfer	ファイル転送
♦Synchronisation	ファイル同期

8

現在検討中のプロファイル：V2．0

- Automotive ：自動車内サービス
- Personal Area Networking ：個人エリアのネットワーク用途
- Human Input Device ：マウス・キーボード向け
- Audio/Video ：AVデータ転送処理
- Printing ：プリンター機器
- Still Imaging ：イメージデータ処理
- Extended SDP ：拡張SDP
- Local Positioning ：位置情報認識サービス
- Unrestricted Digital Use ：次世代携帯電話

◆その他
Radio 2 ：高速化
WLAN ：無線方式の共存

4つのStudy Group
- ISDN
- HCI：ホストとのインターフェース
- Industrial Automation
- Financial Transaction

SDP:Service Discovery Profile

5）SIG（Special Interest Group）活動

◆98年5月 プロモータ5社（Ericsson、Nokia、Intel、IBM、東芝）で規格作成
◆99年7月 仕様一般公開
◆99年12月 プロモータに4社（Microsoft、Lucent、3Com、Motorola）加入
◆アダプター（2000社以上）
Bluetoothの規格を利用できる資格。参加無料
◆アソシエータ企業（約130社）
SIGへの参画するための必要資格

★*仕様認証の仕組みを構築*

Bluetoothの名前の由来

名前の由来

・Bluetoothは携帯電話とPCの接続を目的とした無線方式

・Harald Blaatand "Bluetooth" II (940-981)
デンマークとノルウェーを無血統合した王様

・Bluetoothが通信業界とPC業界を統合することと、Harald Blaatand王が2つの国を統合したことをかけて銘々した。

2. Bluetooth 仕様概要

1) Bluetooth 周波数帯と転送速度

2) ネットワークの基本単位:
ピコネットとスキャタネット

3) 周波数ホッピング方式
<スペクトラム拡散通信方式>

Magic number

1）Bluetooth 周波数帯と転送速度

- ◆ 使用する周波数帯域
  - 2.4GHzのISM*バンド、出力1mW（半径10m）
  - 79MHz幅を使用(2.402～2.480GHz)
- ◆ データ転送速度： 1Mbps （Ver2.0で2Mbps）
  - 音声: 64 kbps
  - データ: 432.6 kbps（full duplex）
    723 / 56 kbps (非対称)
- ◆ ネットワーク 1:1／1:n（7台まで）

*ISM: Industry Science Medical

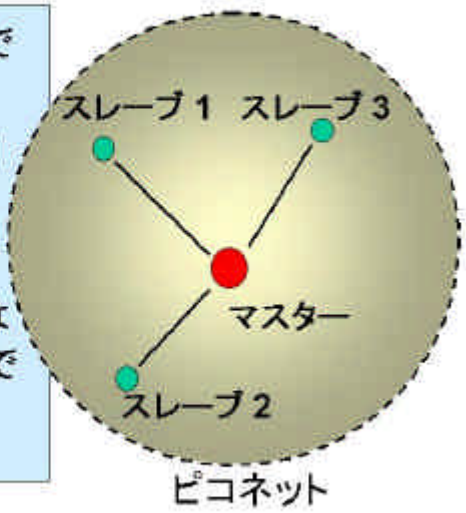
Bluetoothの出力クラス

Class	最大	通常	最小
Class 1	100mW (20dBm)	N/A	1mW (0dB)
Class 2	2.5mW (4dBm)	1mW (0dBm)	0.25mW(-6dBm)
Class 3	1mW (0dBm)	N/A	N/A

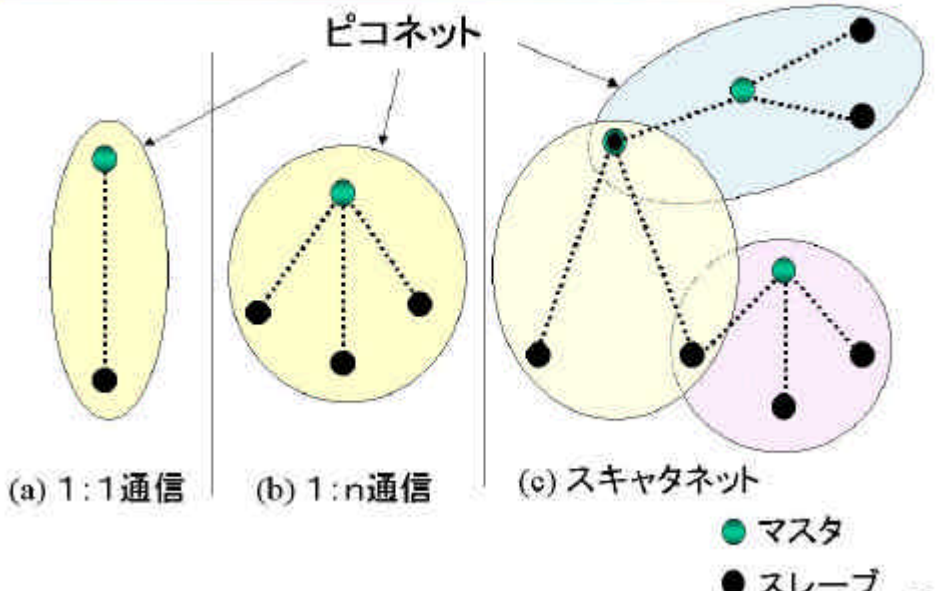
注） Class 1では4dBmから20dBmの電力制御が必須
各クラスとも - 30dBmから0dBmの電力制御がオプション

2）ネットワークの基本単位：ピコネット

- マスタと最大 7スレーブ で 1 個のピコネットを構成
- マスタが ピコネットを統制
- スレーブ は マスタとのみ 交信可能
- 255台までの スレーブ は 待機モード(Park Mode)で マスタの管理下



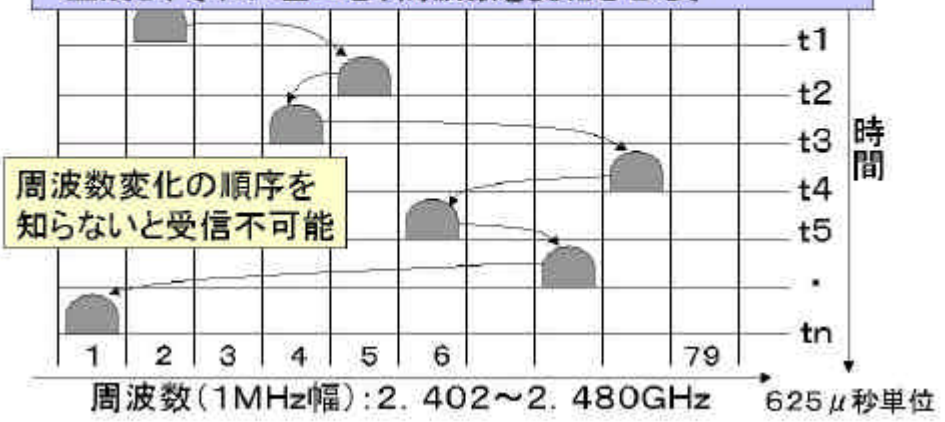
ピコネットとスキャタネット



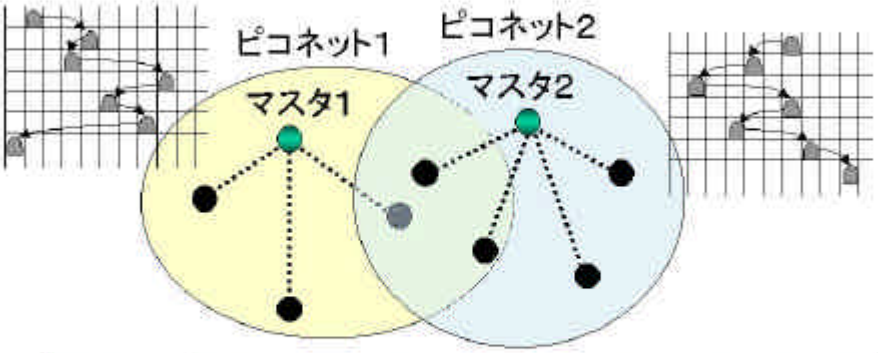
3）周波数ホッピング方式（スペクトラム拡散通信の一つ）

◆周波数を**毎秒1600回（625μ秒ごと）**に変化させ通信

◆**マスタの物理アドレス**をもとに乱数（周期はほぼ1日）を生成し、それに基づき、周波数を変化させる。



複数のピコネットの同時存在



・2つのピコネットの周波数の変化順序は異なっている。
・あるタイミングで同じ周波数帯域がぶつかっても、エラーを検出しデータを再送すれば良い。

★複数のピコネットが同時に通信できる。

3. Bluetooth搭載製品の商品化手順

◆Bluetooth アダプタ契約
- 会費無料
- 技術普及のためBluetoothに関する知的財産権の放棄

◆Bluetoothロゴ認証取得
- 機器間の互換性を確保するためのBluetooth独自の制度
- シール表示が義務づけられる見込み

◆各国型式認証取得
- 日本ではTELEC(電波法／無線設備規則)
  およびJATE(電気通信事業法／端末等規則)

Bluetoothロゴ認証制度

→ BQTF (認定テストラボ) → テスト結果

Bluetooth Qualification Test Facility

→ BQB (認証者) OK判定 → Bluetooth Brand Book → ロゴ認証合格

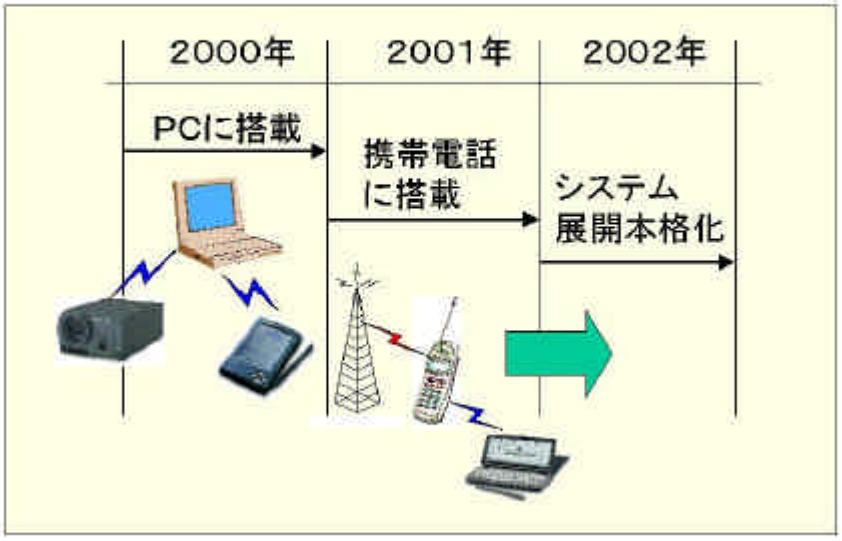
Bluetooth Qualification Body：世界で25人、日本人：1人(当社)

4. Bluetoothを用いたシステム像

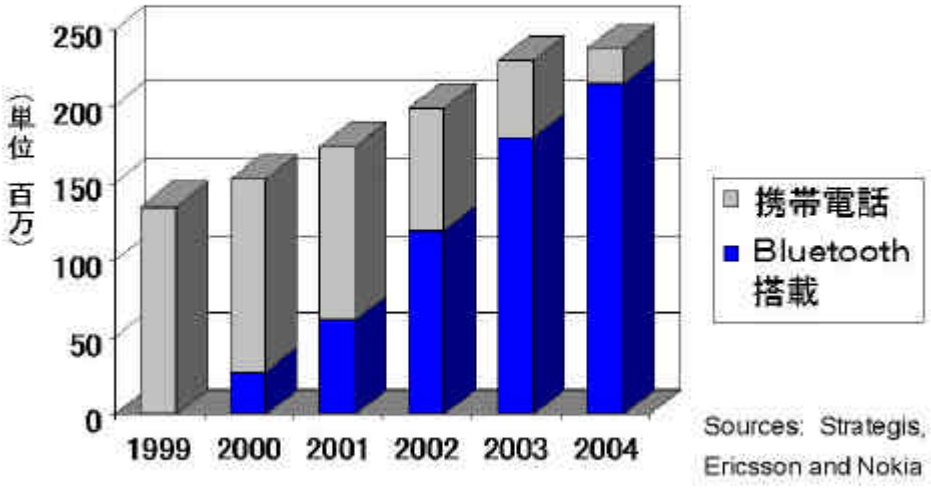
1）Bluetoothのビジネス展開
- ビジネス展開時期
- Bluetoothの搭載機器の広がり

2）Bluetooth応用イメージ
- PAN(Personal Area Networking)分野
- ホームネットワーク
- 情報提供サービス
- “電子財布”
-

1）Bluetoothのビジネス展開



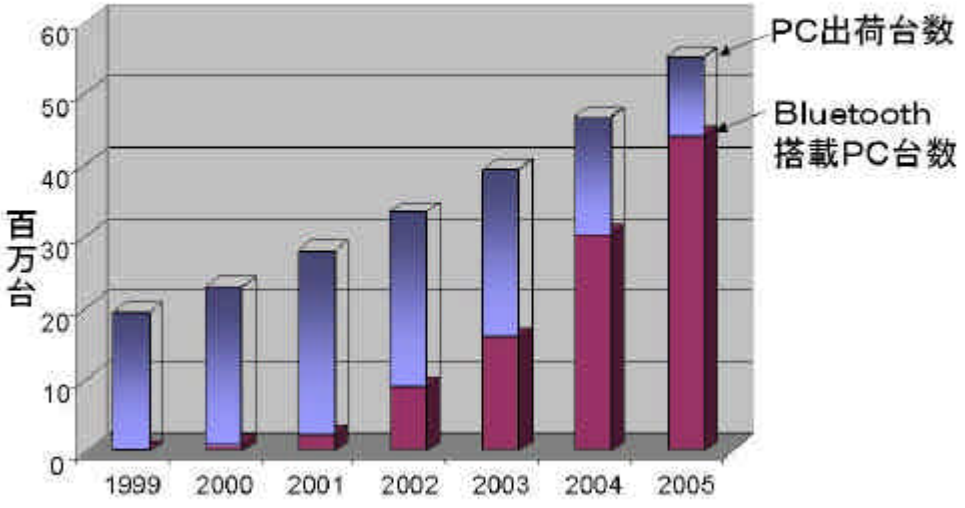
携帯電話のBluetooth搭載比率



Sources: Strategis, Ericsson and Nokia

23

ノートブックPCとBluetooth搭載比率



Source: Cahners, In-Stat Group

24

Bluetooth Cellular Phone (Ericsson)

2001 © TOSHIBA

25

Bluetooth Hotel

2001 © TOSHIBA

26

Whitetooth Refrigerator ? (Ericsson)

Bluetoothでお買い物

NE ONLINE INTERFACE Bluetooth

「Bluetoothでお買い物」，北欧デパート・チェーンが実践

北欧のデパート・チェーンであるIDA Ahold社は，2000年12月19日，Bluetoothを利用した電子支払いシステムの利用実験を行なったことを明らかにした（発表資料）。

デパートの利用者が，料金の支払いや，試着のチェック，販売品の積み忘れ防止などを，Bluetooth対応携帯電話機を使って行なうというもの。通常のように，キャッシュ・レジスタを使う場合や，クレジット・カードを使った処理よりも，早く簡単にできるとしている。

デパートのような環境において，Bluetoothによる無線データ通信がどの程度実現可能なのかを試験するのが目的。実験にはスウェーデンEricsson社が協力している。

ストックホルム郊外にあるIDA Ahold社の店舗内に，複数のBluetooth用アクセス・ポイントと，Bluetooth対応サーバ機を設置した。実験にさま，Ericsson社のWAP対応携帯電話機「R320」に，Bluetooth用アダプタを装着して利用した。実験の結果は「デパートのような環境で，Bluetoothを使った無線による電子支払システムが良好に稼動することが実証された」（IDA社）という。

IDA Ahold社は，スカンジナビア半島およびバルト海沿岸8箇国に，4600店まりの店舗を保有している。

Bluetooth対応腕時計

■移動体通信:

Bluetooth対応の腕時計，セイコーインスツルメンツが初公開(2001/1/9)

2001年1月6日～1月9日に米国Las Vegasで開かれた民生機器関連の展示会CES(Consumer Electronic Show)で，セイコーインスツルメンツは近距離無線データ通信技術「Bluetooth」に対応した腕時計を展示した。試作機はBluetoothの「Version 1.0b」に対応していたが，実際の製品では「Version 1.1」に対応する見込み。

スウェーデンEricsson社のブースにも腕時計が置かれていた

Bluetoothに対応した携帯電話機と組み合わせて使うことを想定している。携帯電話機に着信があると，腕時計を鳴らすことで消費者に知らせる。リストバンドの裏側にマイクとスピーカが内蔵されており，腕時計を外してリストバンドの部分を伸ばせば通話も可能になる。さらに，携帯電話機などの無線通信規格向けに開発されたプロトコルであるWAP(wireless application protocol)に対応している。インターネット上の情報サイトから，各種情報を携帯電話網経由で腕時計の画面に表示させることができる。

携帯電話機以外では，パソコンと通信してプログラムの起動や操作が可能。「PowerPoint」を起動して操作したり，CD-ROM装置に入った音楽CDを聴くことができる。パソコンのセキュリティ技術と組み合わせれば，腕時計を身につけた人がパソコンから離れた場合に，パソコンが腕時計からの電波が届かなくなったことを感知してパソコンを使えなくすることも可能だ。腕時計単体では，ゲームやスケジュール管理などの機能を使うことができる。

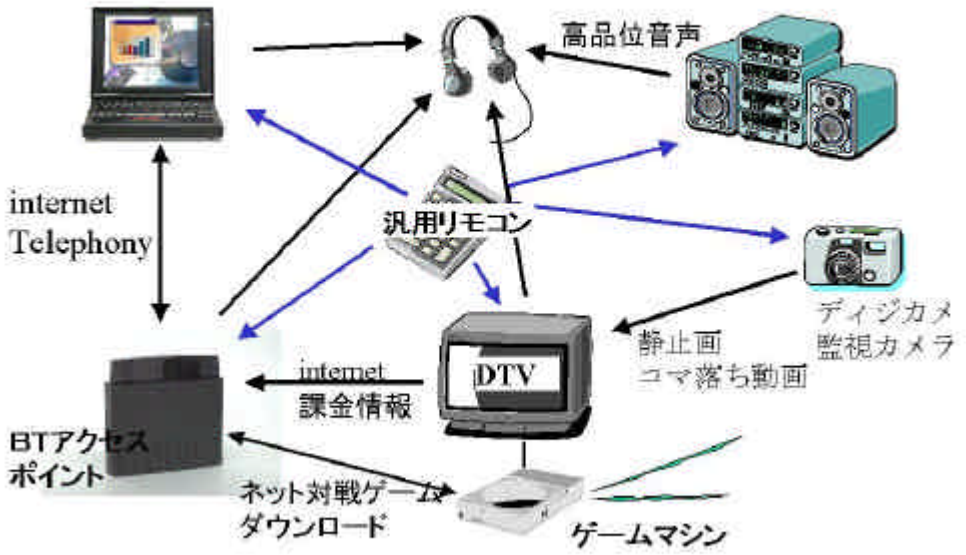
試作機では，上述したすべての機能が使用可能になっている。電池駆動時間は標準的な使い方で1日間程度。電池充電用の端子などはなく，電磁誘導方式などで使用している技術を利用して非接触で充電が可能にした。ハードウエアはほとんど完成しており，現在はこの製品に適したサービスなどを検討しているという。今回の展示会への出展は，市場の反応を確かめるねらいもある。発売は2001年中，価格は3万円以下を目指している。(河合基伸)

2）応用イメージ：PAN環境の実現

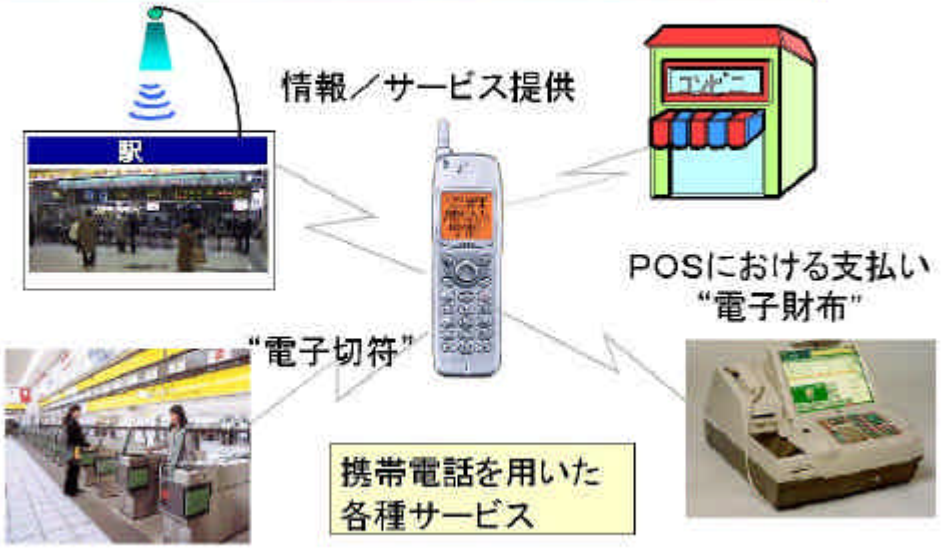
- ワイヤレス環境でデータを交換
- 名刺を電子的に交換
- プリンタやプロジェクタをケーブルなしで共有

PAN：Personal Area Network

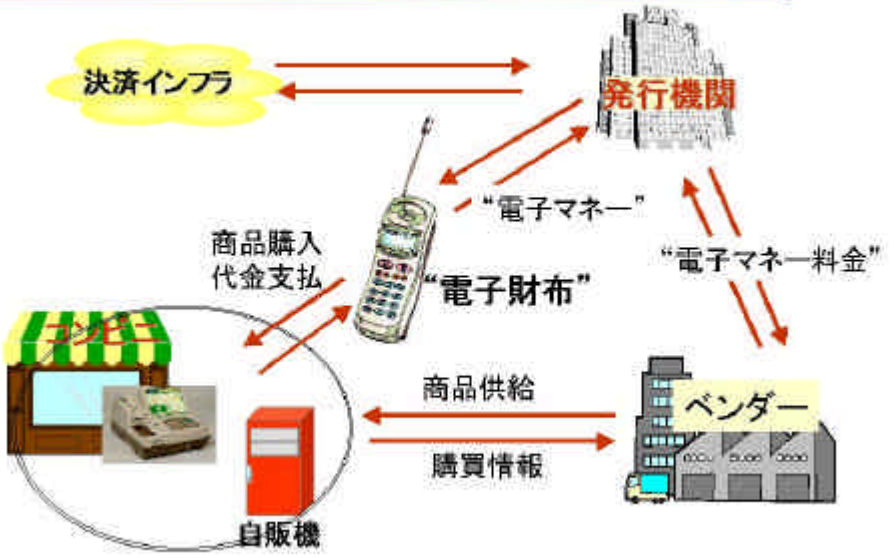
応用イメージ：ホームネットワーク分野



応用イメージ：情報／サービス提供



応用イメージ:“電子財布”



最新情報入手先

- ♦ WWW.Bluetooth.com
  - Bluetooth仕様V1.0 (ダウンロード可能)
  - 報道発表一覧
  - 最新アダプタリスト
  - 機関紙SIG ‘nal (ダウンロード可能)
  - Bluetooth Conference 案内等のニュース
  - メンバー加入申請方法　等

◆「ワイヤレス通信の新技術 Bluetoothガイドブック」 ISBN4-526-04594-2
日本エリクソン株式会社 宮津和弘著 日刊工業新聞社 3200円

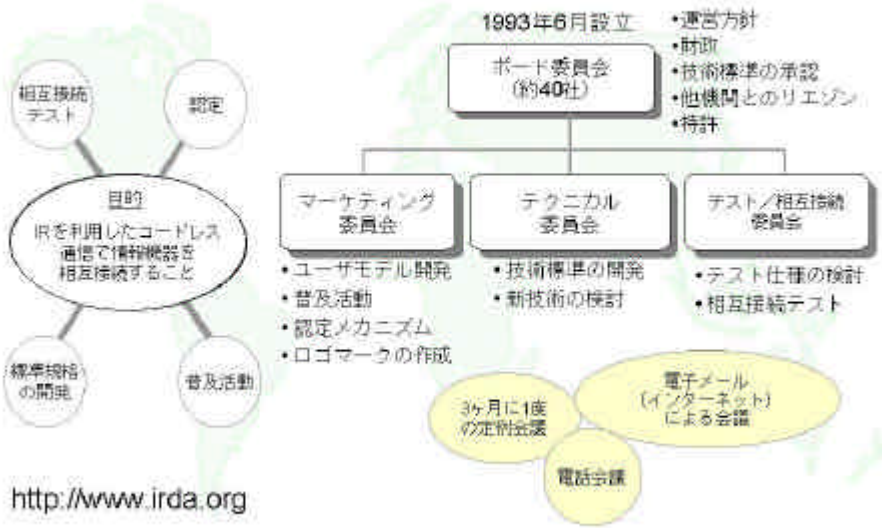
◆「明解 Bluetooth」 ISBN4-89797-450-x
モバイルコンピューティング推進コンソーシアム編著 リックテレコム1600円

4　携帯電話における赤外線通信技術の現状

携帯電話における
赤外線通信技術の現状

2001 © SHARP　1

IrDA(Infrared Data Association)とは



2001 © SHARP　2

IrDAの目的の変化

- 設立当初の目的:
  - 赤外線を利用したコードレス通信で，情報機器を相互に接続する
    - ➡ 相互に接続するための規格を標準化する

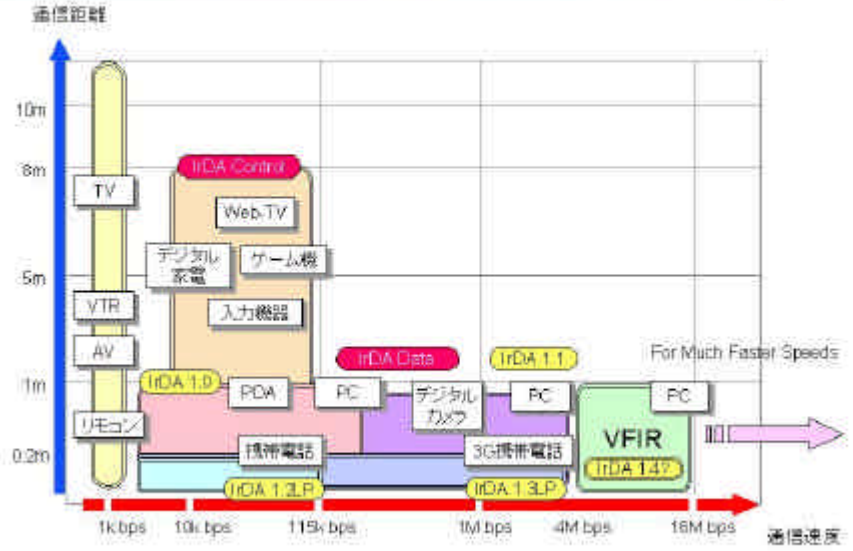
➡「情報機器」のスコープは時代を経て変化
➡Bluetoothなど，競合(補完?)する技術規格の登場

- 最近の目的
  - 赤外線に最も適した応用を実現／提案する.
    - ➡「相互に接続する」から具体的な応用の実現に変化
    - ➡ 携帯電話向け規格 = IrMC (IrDA Mobile Communication)

IrDA規格のスコープの変遷 (1)

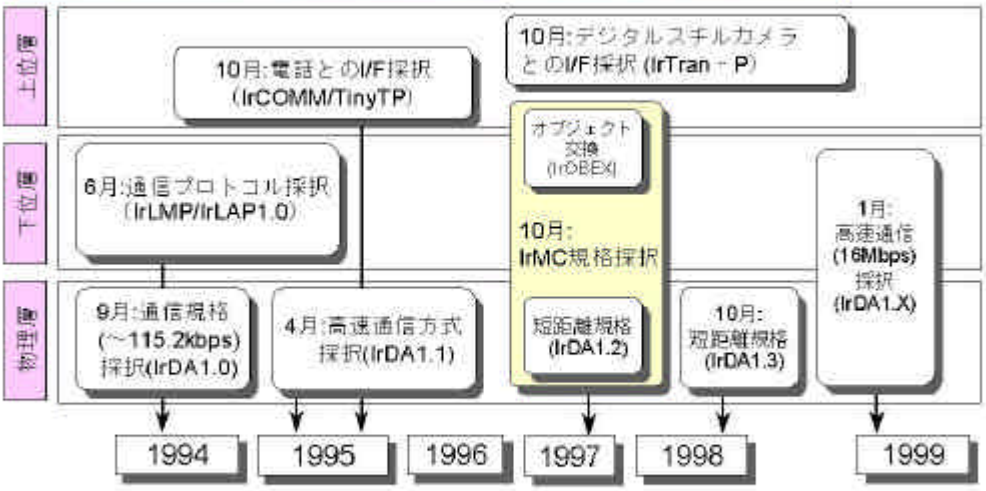
- 草創期 (～ 1996)
  - PCとPDAが「情報機器」（短距離，高速化）
    - シリアルケーブルを無線に
- 興隆期 (～ 2000)
  - PCとの親和性を特徴とする携帯機器 （低消費電力化）
    - デジタルカメラ，携帯電話，ページャ
  - 「ボタンひとつで写真を送信」「アドレス帳を携帯電話に送信」
- 発展期 (2000 ～)
  - デジタル情報を扱う機器(家電製品への展開)
    - 制御，デジタル家電間のデータグラムの送信

IrDA規格のスコープの変遷 (2)



5

IrDA: 標準化のあゆみ



IrLMP: Infrared Link Management Protocol IrLAP: Infrared Link Access Protocol TinyTP: Tiny Transport Protocol
IrOBEX: Infrared Object Exchange IrTran-P: Infrared Transfer Picture

6

データ通信用プラットフォーム: IrDA-Data

印刷

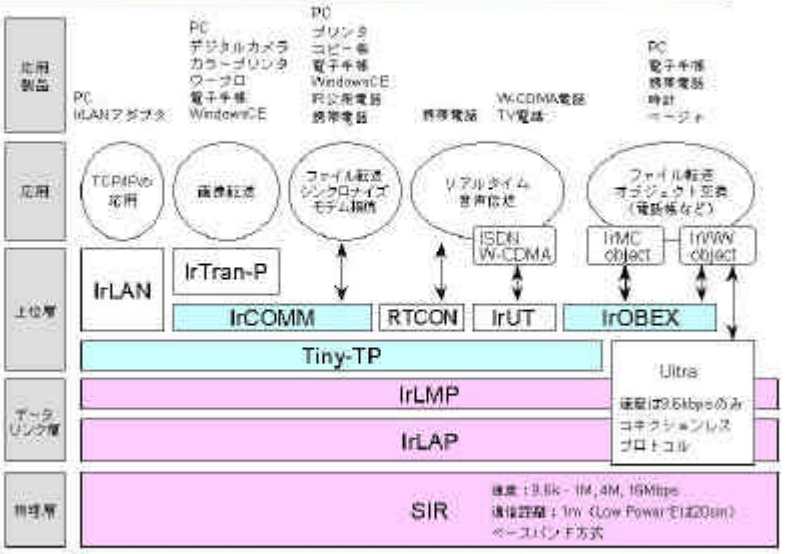
データ交換

公衆網に接続

- 目指した世界
  - 機器を向かい合せるだけでデータ交換ができる
- 要求仕様
  - 無線による器機間の簡単な接続
  - シリアル／パラレルケーブルの赤外線への置き換え
  - 通信速度は115kbps程度は必要
  - 通信範囲は1m程度
  - 低消費電力で携帯機器に使える
  - ハードウエアは低コストで実現

IrDA-Dataを搭載した商品例

IrDA-Data プロトコルスタック



IrDA-Data 物理層規格の仕様概要

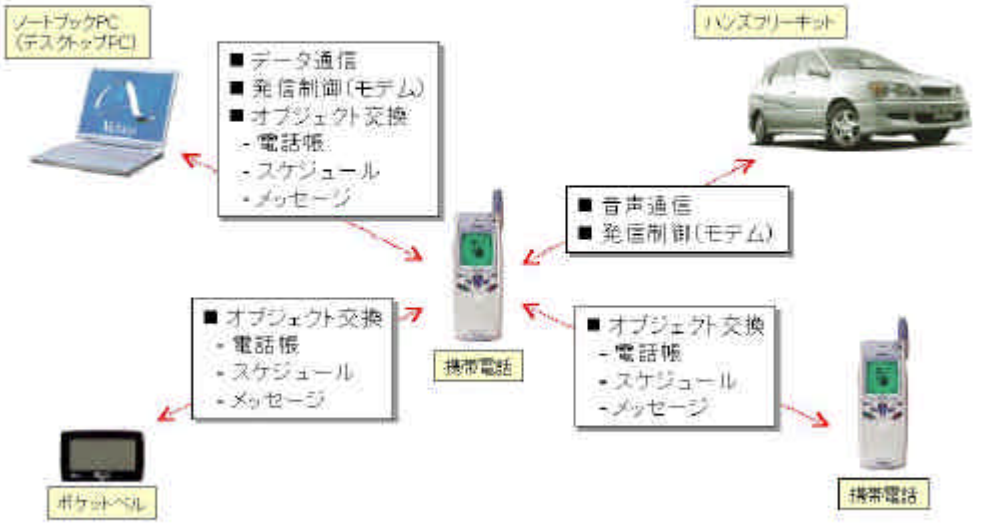
項目	仕様			
	SIR1.0	SIR1.1		SIR1.4 (仮称)
通信速度	9.6k ~115.2kb/s	576kb/s, 1.152Mb/s	4Mb/s	16Mb/s
通信距離	0 ~ 1 m (標準)	0 ~ 1 m (標準)		0 ~ 1 m (標準)
通信方式	調歩同期式	フレーム同期式		フレーム同期式
変調方式	RZI方式	RZI方式	4値PPM方式	HHH(1,13)方式
最小放射強度	40mW/sr (標準)	100mW/sr (標準)		100mW/sr
通信角度	±15° 以上	±15° 以上		±15° 以上

IrDA-Data: データリンク層 仕様概要

- IrLAP (Infrared Link Access Protocol)
  - コネクション管理
    - 局の発見
    - 半二重不均衡モード
  - 通信速度の折衝
    - 9.6kbpsで折衝
  - エラー検出とエラー回復
  - フロー制御
- IrLMP (Infrared Link Management Protocol)
  - データリンクの多重化
  - サービス問い合せ
- Tiny-TP (Tiny Transport Protocol)
  - フロー制御 (分割再構成)

携帯電話における
赤外線通信アプリケーション

想定するアプリケーション



3つのアプリケーションクラス

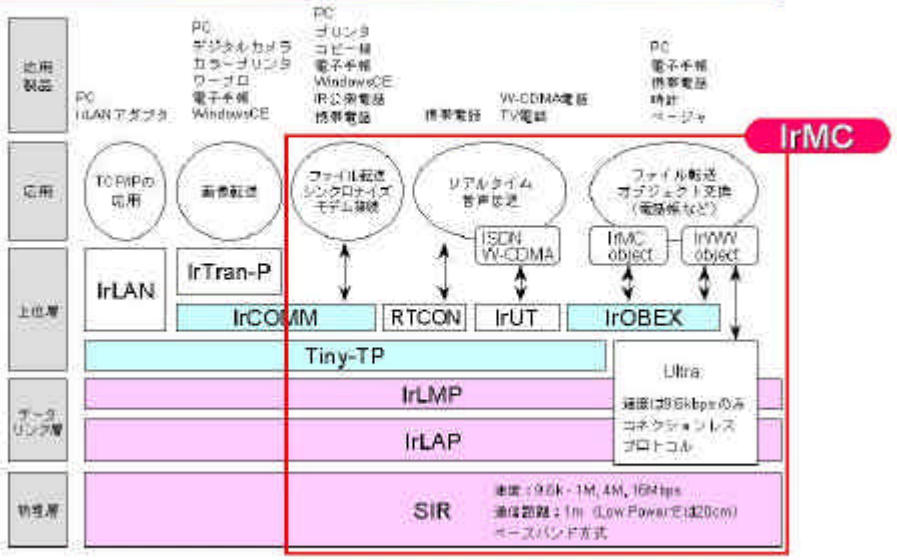
- Atomic Information Exchange
  - 2局間でのオブジェクト交換 - 機能ごとにレベルを規定
    - 電話帳，スケジュール帳，メッセージ
- Stream-oriented Information Exchange
  - テレコム機器を双方向のストリーム情報の送信機として利用
    - 携帯電話をモデムとして利用
- Real-time Information Exchange
  - 赤外線上での音声のリアルタイム伝送
    - 携帯電話とハンズフリーキット

携帯電話向け
赤外線通信標準規格 IrMC

IrMCの概要

- 機能
  - Atomic Information Exchange（オブジェクト交換）
    - IrOBEXを利用
    - シンプルなオブジェクト転送から，シンクロナイズまでレベルを規定
  - Stream-oriented Information Exchange（モデム接続）
    - IrCOMMを利用
  - Real-time Information Exchange（音声伝送）
    - RTCONを利用
- 規格が規定する内容
  - IrDA-Data規格の実装ガイドライン
    - 物理層規格を拡張 (IrDA-SIR version 1.3)
    - コネクションレス型プロトコル: Ultraの実装ガイドライン
  - 交換するオブジェクト形式
    - 電話帳 (vCard), スケジュール (vCalendar), メモ (vNote), メッセージ (vMessage)

IrMC プロトコルスタック



17

オブジェクトフォーマット

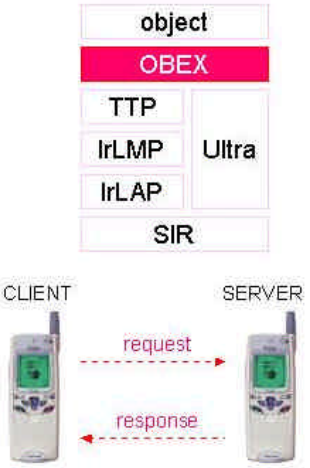
オブジェクト名	内容
Phonebook	アドレス帳. "vCard - The Electronic Business Card Exchange Format - version 2.1", Internet Mail Consortium (IMC)で規定されたものを一部拡張
Calendar	スケジュール帳. IMCが規定した"vCalender - The Electronic Calendaring and Scheduling Format - version 1.1"
Message	送受信したメッセージ(電子メールなど). アプリケーション依存. 但し, "vMessage version 1.1"(IMCで規定)のサポートが必須.
Note	送受信したショートメッセージなどのメモ. アプリケーション依存. 但し, "vNote version 1.1"(IMCで規定)のサポートが必須
Realtime Voice	音声のリアルタイム伝送. RTCONプロトコルを利用する.

object	
OBEX	
TTP	Ultra
IrLMP	
IrLAP	
SIR	

18

オブジェクト交換プロトコル: IrOBEX

- "IrDA-DataのHTTP"
  - クライアントとサーバーの対話形式
    - DISCONNECTにも応答を返す
  - 主なサービス
    - PUT: オブジェクトの送信
      - Ultra上ではPUTだけ実装可能
    - GET: オブジェクトの受信
    - SetPath: 受信側のカレントディレクトリを変更
  - Inbox connection
    - Simple OBEX file transfer
      - 送信側はobjectをinboxに送るだけ
    - Capability Service
      - サーバーがサポートするフォーマット形式が分かる



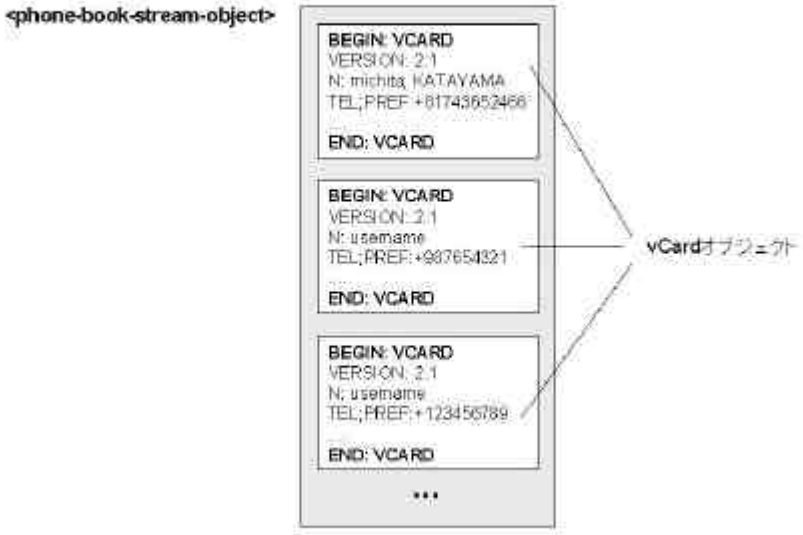
IrMC: 4つのサポートレベル

- オブジェクト交換における機能に基づく
- 単純なオブジェクト転送からシンクロナイズまで
  - Level 1 support
    - ひとつのオブジェクトを，一方の局から他方の局にPush (PUT)することができる．
      - 自分の携帯電話番号を友人の携帯電話へ送信
  - Level 2 support
    - 全てのオブジェクトエントリについて，一方の局が他方の局に対して，read/writeすることができる．
      - 機種変更に伴い，電話帳全てを新しい機種に送信
  - Level 3 support
    - ターゲットとなる機器のオブジェクトのindexを再現できる．(階層構造を表現できる)
      - データベースの転送
  - Level 4 support
    - 2局間で，シンクロナイズすることができる．

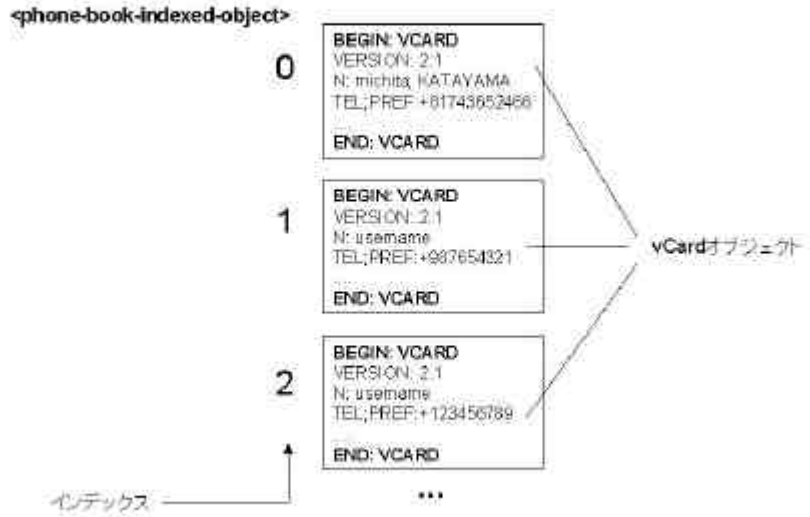
Level 1 support (vCard: michita.vcf)

```
BEGIN:VCARD
VERSION:2.1
N:michita;KATAYAMA
FN:KATAYAMA michita
ORG:SHARP;R & D Group
TITLE:ASSISTANT SUPERVISOR
NOTE:KATAYAMA in SHARP
TEL;WORK;VOICE:+81 743 12 3456
TEL;WORK;FAX:+81 743 12 3457
ADR;WORK:;;2613-1 ICHINOMOTO;TENRI;NARA;632-8567;Japan
LABEL;WORK;ENCODING=QUOTED-PRINTABLE:2613-1
   ICHINOMOTO=0D=0ATENRI, NARA 632-8567=0D=0AJapan
ADR;HOME:;;;;;;Japan
LABEL;HOME:Japan
EMAIL;PREF;INTERNET:michita@slab.tnr.sharp.co.jp
REV:19990817T024453Z
END:VCARD
```


Level 2 support



Level 3 support



コネクションレス型プロトコル: Ultra

- 「投げ捨て」型
  - 信頼性のない通信路を提供
    - 上位層で信頼性を保証する必要がある
    - ユーザーへの「送信成功」提示が必要である
- 必須の機能
  - IrLAPのフレーミング，メディア制御に従う
    - 局の発見(device discovery)は行わない
    - 通信速度の折衝も行わない
  - 全ての通信は9.6kb/sで行う
- オプション機能
  - 2.4kb/sによる通信
    - IrDA-SIR1.0が2.4k～115.2kb/sだったため
  - 分割再構成機能

モデム接続と音声伝送

- モデム接続
- IrCOMMを実装する.
  - PCのシリアル・パラレルポートをエミュレーション
  - ケーブルを赤外線に置きかえることが可能
    - 9-wire
    - 3-wire
    - 3-wire raw (IrLPT)
    - セントロニクス
- 音声伝送
  - RTCONを実装する.
    - ITU-T G.726の32kb/s ADPCM音声CODECを共通のCODECとして使用
    - 20ms毎に80byteの音声データを含むパケットを生成
    - 潤沢なバッファが必要
    - 0.5msのターンアラウンドタイムが必要

IrMC: 物理層規格の拡張

（背景その1）

- 携帯電話は電池寿命の要求が厳しい
  - 低消費電力化が必須
  - ➡ LED（送信側）の出力を従来の1/10に
  - ➡ 出力を抑えた結果，通信距離が20cmに

（背景その2）

- 携帯電話は小型化・軽量化が必要だった
  - 従来規格用の赤外線トランシーバでは実装できない
  - ➡ デバイスサイズを小型化
  - ➡ レンズ設計上の問題などから，1mの通信距離が困難に

IrMC: 物理層規格の仕様概要

項目	仕様			
	SIR1.0	SIR1.1		SIR1.4 (仮称)
通信速度	9.6k ~115.2kb/s	576kb/s, 1.152Mb/s	4Mb/s	16Mb/s
通信距離	0 ~ 1 m (標準) 0 ~ 20cm (SIR1.2 省電力オプション)	0 ~ 1 m (標準) 0 ~ 30cm (SIR1.3 省電力オプション)		0 ~ 1 m (標準)
通信方式	調歩同期式	フレーム同期式		フレーム同期式
変調方式	RZI方式	RZI方式	4値PPM方式	HHH(1,13)方式
最小放射強度	40mW/sr (標準) 3.6mW/sr (SIR1.2 省電力オプション)	100mW/sr (標準) 9.0mW/sr (SIR1.3 省電力オプション)		100mW/sr
通信角度	±15° 以上	±15° 以上		±15° 以上

IrDA対応携帯電話の現状

IrDA対応携帯電話の現状

- 欧米
  - TOP3社では，積極的に実装が進められている
    - ビジネス用途中心に提案
      - （例）Palmと携帯電話で名刺交換
  - TOP3社では，戦略モデルへの実装が進められている
    - TOP3社によるシェア争奪戦
      - 仕様競争に陥っている見方もある
  - 中堅メーカでの実装もようやく始まる
    - 状況は厳しい - シェア獲得の為のコストダウン
- 国内
  - 独自仕様によるIR通信機能搭載モデルが続々登場
    - IR通信のメリットがどこまで享受できるか?

世界の主要メーカおよび製品(1)

NOKIA

- 全市場向けにIrDA対応機種を投入
- NM502iでは，以下の機能に対応
  - シンクロナイズ
  - vCard
  - vCalender
  - vMessage
- 8210 GSMは，IrDAのみが外部I/F
  - シンクロナイズ
  - vCard
  - vCalender
  - vMessage

世界の主要メーカおよび製品(2)

エリクソン
R320s GSM

モトローラ
Timeport L7082 GSM

エリクソン

- R320sでは以下の機能をサポート
  - シンクロナイズ
  - vCard
  - vCalender
  - 着信メロディ転送

モトローラ

- L7082では以下の機能をサポート
  - シンクロナイズ
  - vCard
  - vCalender
  - vMessage

日本の市場

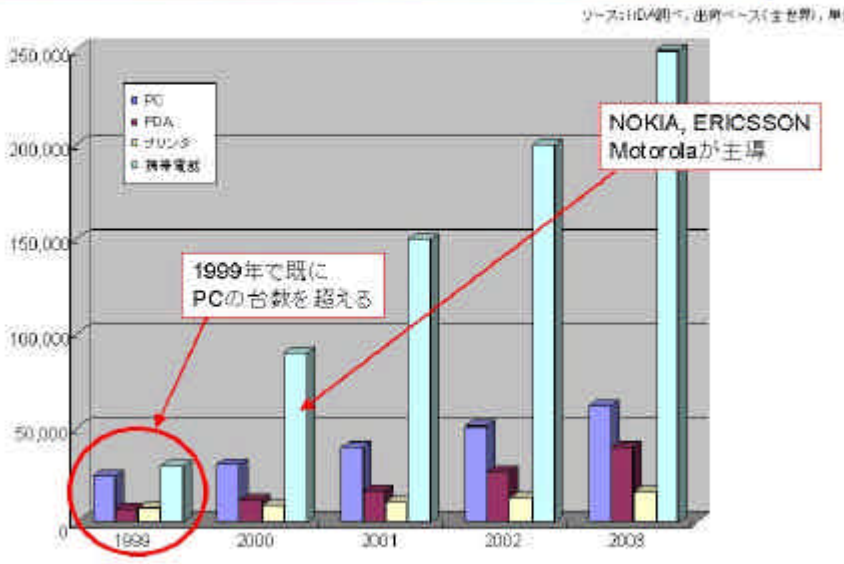
IrDA規格準拠

- NOKIA
  - NM207 for DoCoMo
  - NM502i for DoCoMo

赤外線通信機能(非IrDA)

- いずれも電話帳，メモ，ブックマークを交換
- Panasonic
  - P502i
- 三菱電器
  - D208
  - D502i
  - D209i

IrDA実装製品の出荷台数実績 / 見込



Why IrDA?

- 欧米メーカの眼から見たIrDA
  - 他の無線技術に比べて，安価で実装が可能
    - 「データ量に対する実装コスト」
  - 他の無線技術に比べて，小型の実装が可能
  - 他の無線技術に比べて，高速通信（～16Mb/s）が可能
  - ユーザーモデルが分かりやすい
    - 「通信したい機器に向けて，ボタンを押すだけ」
  - 相互通信性が改善された
    - IrDAは現在PC/PDAに最も普及している技術
    - （全ての無線技術に共通）通信相手がいて初めて意味がある

今後の動向

- 着信メロディの転送
  - 日本での普及は「エンターテイメント」が重要 ???
- 対戦ゲーム
  - 卓球やブロック崩しなどのIRを利用した簡易対戦ゲーム
- 腕時計との連携
  - IrWWによる時刻合わせ，アラーム情報の交換
- Bookmarkの転送
  - 時期バージョンのIrMCには組込まれる見込み
- WAP over IrDA
  - WAP Forumでの提案

IrDAとBluetooth（応用からみた比較1）

- IrDAが強みを発揮する利用シーン

IrDAがその強みを最も発揮するのは

- 通信したい相手が特定できて
- 通信したい相手が近くに存在する場合で
- 通信結果をその場で見るような場合 もしくは 高速通信が要求される場合

これに合致するシーンは

- PDAどうしで、お互いの名刺交換
- 携帯電話どうしで、お互いの電話番号交換
- デジタルカメラどうしで、お互いに撮影した写真／動画データを交換
- PCのスケジュール帳データで、PDAのスケジュール帳をアップデート

などが挙げられる。

面と向き合って、「さっ」とデータを渡す。 渡したデータをその場で活用する。
そんな利用シーンでは、IrDAが便利

IrDAとBluetooth（応用からみた比較2）

- Bluetoothが強みを発揮する利用シーン

  Bluetoothがその強みを最も発揮するのは；
  - 通信したい相手が比較的遠隔地に存在する あるいは
  - 通信したい相手と自局の間に遮蔽物があるような場合で
  - 通信結果をその場で見る必要がない場合

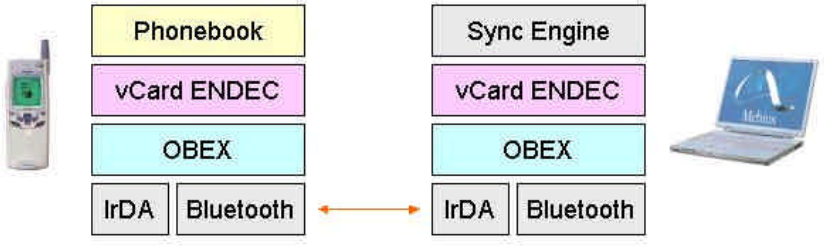
  これに合致するシーンは
  - 自分のデスクのPCから、居室内のプリンタへドキュメントを印字
  - 商談に利用したプレゼンを、商談に出席者のPC（複数）へ送信
  - 新幹線で移動中に、PCだけ取り出してダイヤルアップ

  などが挙げられる。

ちょっと離れた機器にデータと投げておいて、後からそのデータを利用する。
そんな利用シーンでは、**Bluetooth**が便利

IrDAとBluetoothによる補完関係

- IrMC規定のシンクロナイズ機能
- vCard, vCalender
- 下位層のメディアにとらわれずにシンクロナイズすることが重要



IrDAとBluetoothの共存

- 双方の短所
  - IrDA：物理的制限を受ける（遮蔽物に弱い）
  - Bluetooth：強力な認証、セキュリティが必要（回路が複雑）
    他の電波発生体からの影響（ISM帯は多くの機器で利用）
- 用途別の利用
  - 安価、小型、高速通信、一時的利用、（直感的） → IrDA
  - ネットワーク、場所の制限を受けない、複数機器通信 → Bluetooth
- 無線通信共通の課題
  - どのようなシーンで、どのようなことを行うのか？
    - IrDAにてIrReadyとして利用シーンを想定して規格化を推進
- アプリケーションの共通化
  - 無線通信アプリケーションに対してはIrDAに一日の長がある
    → 上位プロトコルはIrDAの規格も採用（OBEXの利用）

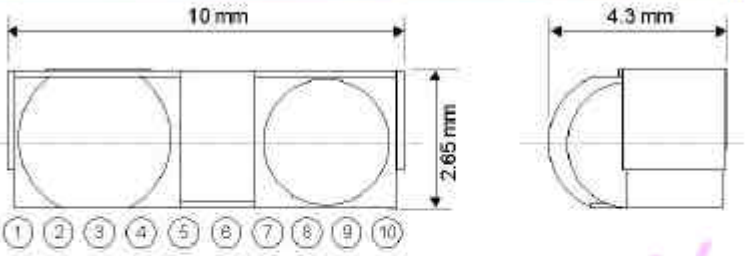
携帯電話向けIrDAトランシーバ

IrDA1.3対応トランシーバ

GP2W1301YP

- IrDA1.3 省電力モード(4Mbps)に対応
  動作時電流(LED電流を除く) : 1.2mA
- IrDA1.3規格対応の超小型パッケージ
  <size: 9.95 (W) x 3.8 (D) x 2.65 (H) mm> with Shield Case
- 低電圧駆動:
  Vcc = 2.7 ~ 5.5V
- スタンバイモード内蔵
  スタンバイ時の最大消費電流: 1 uA
- 外付け部品点数を最少化
- トライステート出力機能内臓
  入出力レベル制御端子により, 低電圧駆動LSIとのI/Fが可能

IrDA1.3LP対応トランシーバ 外観図



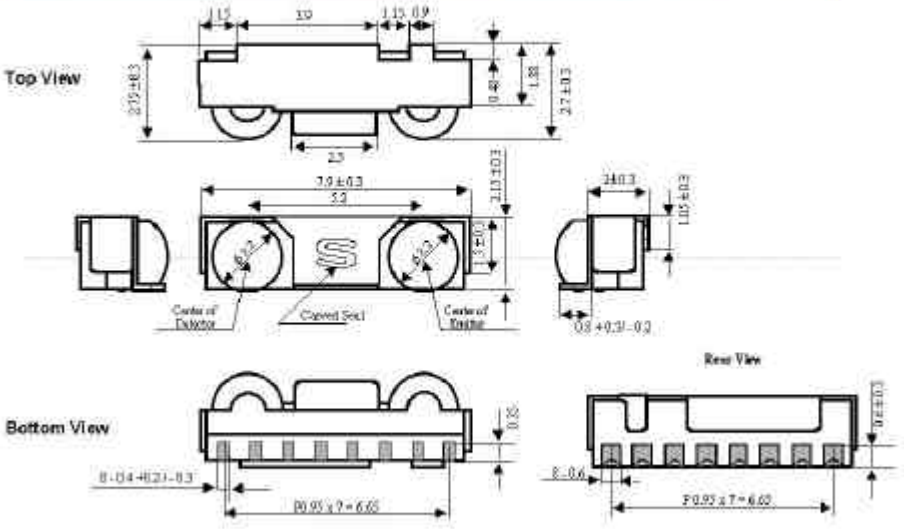
1	AVcc	6	DVcc
2	AGND	7	GND
3	FSEL	8	RXD
4	SD	9	TXD
5	VREF	10	VLED

IrDA1.2対応トランシーバ

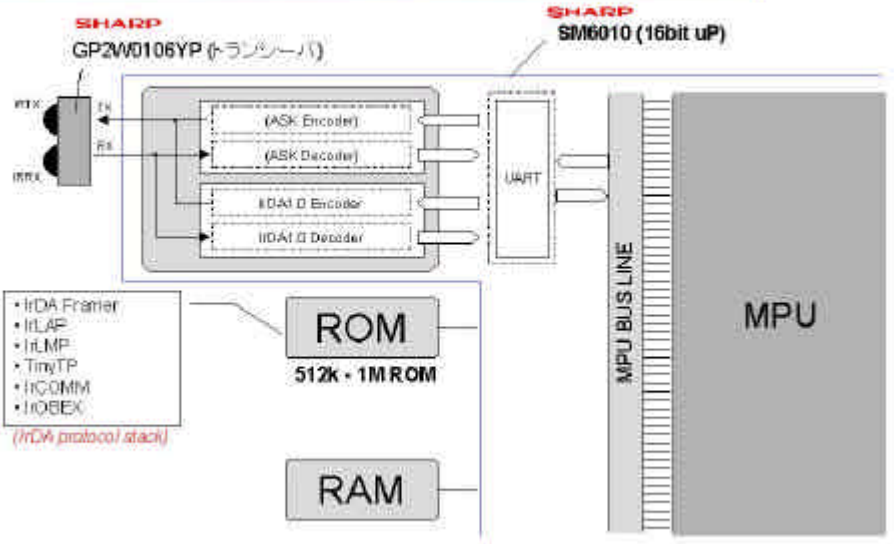
P/N: GP2W0103YP
P/N: GP2W0104YP
P/N: GP2W0106YP
P/N: GP2W0112YP

- IrDA1.2 省電力モード(115.2kbps)に対応
  動作時電流(LED電流を除く) : 1.2mA @ Link Distance 20cm
- IrDA1.2規格対応の業界最小パッケージ
  <size: 7.9 (W) x 2.8 (D) x 2.15 (H) mm> with Shield Case
- 低電圧駆動:
  Vcc = 2.4 ~ 5.5V (GP2W0103YP/0104YP)
  Vcc = 2.0 ~ 3.6V (GP2W0106YP)
  Vcc = 1.7 ~ 2.5V (GP2W0112YP)
- スタンバイモード内蔵
  スタンバイ時の消費電流 typ. 10nA, max 200nA
- 外付け部品点数を最少化
- トライステート出力機能内臓 (GP2W0106YP)

IrDA1.2対応トランシーバ 外観図



赤外線通信の実装例



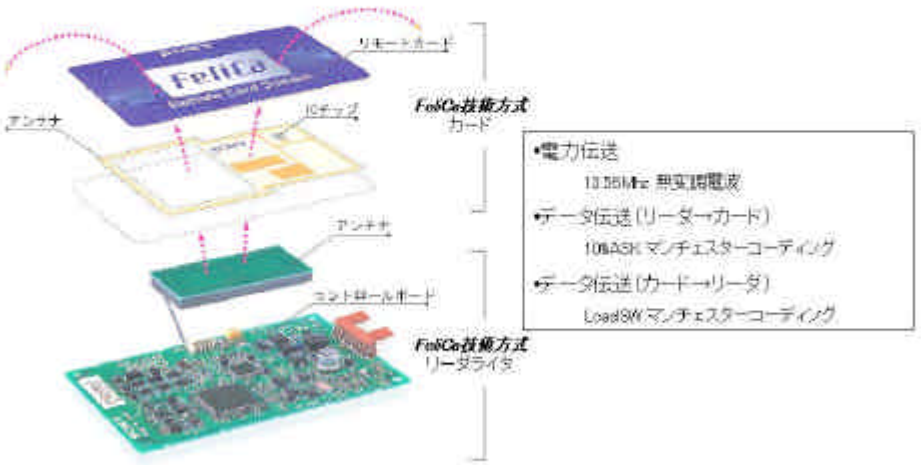
45

46

5　FeliCa 技術方式の特徴とセキュリティ

FeliCa技術方式の
特徴とセキュリティ

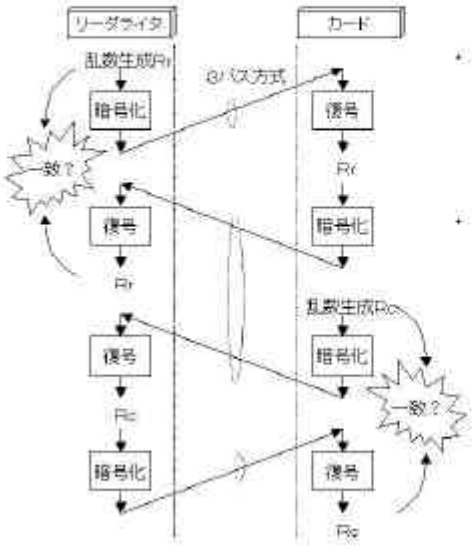
FeliCa技術方式の動作原理



FeliCa技術方式の特徴

- 速いトランザクション処理
  （通信、暗号処理、ファイル管理、メモリ保護）
- 高いセキュリティ
  （相互認証、秘密通信、改ざん防止、タンパレジスト）
- 多彩なアクセスコントロールを備えたファイル管理
  - 階層ファイル構造
  - 従属アクセスコントロール
  - サービス現場でのファイル登録
- 複数ファイルに対して同時オペレーション可能
  - 一括相互認証
  - 完全な同時書き込みみを保証
- 銀行オペレーション型アプリケーション
  - FeliCaは金庫、R/Wは店内サービス、
    金庫の中に他人は入れない
    （FeliCaにアプリケーションソフトのダウンロードを行わない）
  - R／Wの機能アップのみで素早く多彩なサービス運用が可能

FeliCa技術方式の相互認証



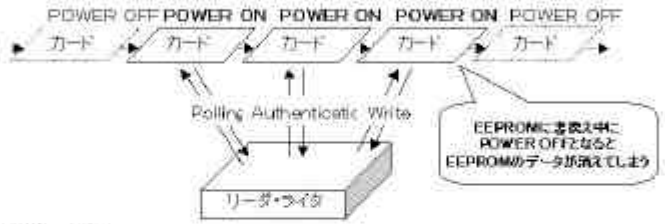
- **相互認証方式**

  ISO9798の3パス方式を強化した
  FeliCa技術方式オリジナル
  （特徴）
  主文の秘密通信方式を踏まえた相互認証で
  主文通信の高速性とランダム性を高めた。

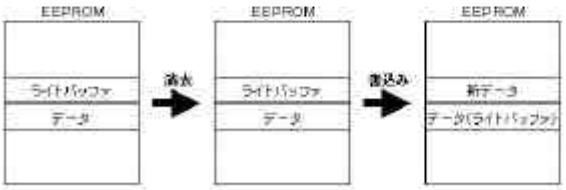
- **暗号化・復号方式**

  トリプルDES（世界標準方式）
  （特徴）
  公開されているため、全世界で強度評価が
  されている。
  シングルDESよりも強度が高い。

FeliCa技術方式のメモリ保護機能
(Anti Broken Transaction)

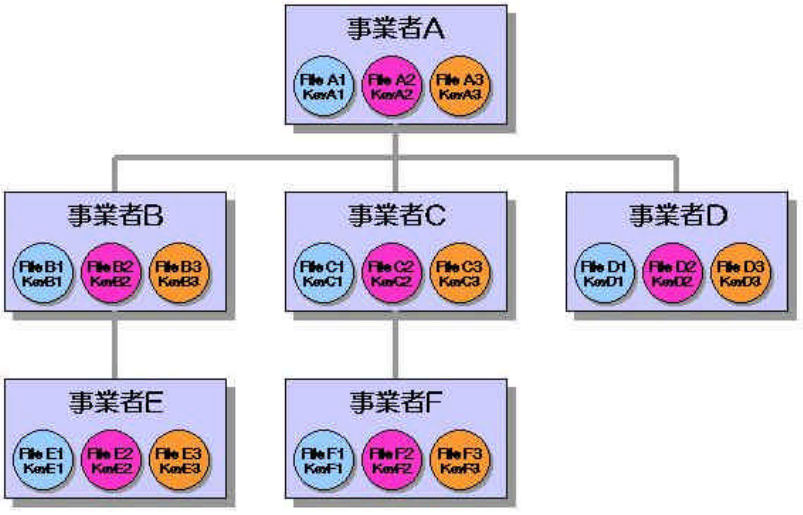


EEPROMの書換え手順



異なるファイル間で
8ブロックまで
同時書込みが可能

FeliCa技術方式のファイル構造例



FeliCa技術方式のアクセスコントロール

事業者DがA1、B2、C3をアクセスする場合

・一般的なカードの場合

KeyA1 で相互認証、 KeyB2 で相互認証、 KeyC3 で相互認証

A1、B2、C3ファイルに対して相互認証完了

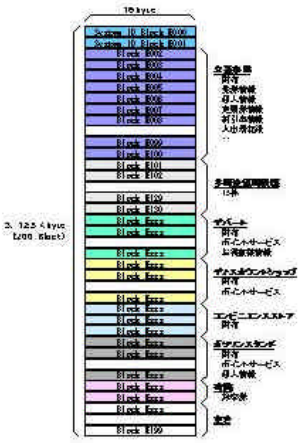
・*FeliCa技術方式*の場合

KeyA1 + KeyB2 + KeyC3 → KeyTemp

KeyTemp で相互認証

A1、B2、C3ファイルに対して相互認証完了

メモリの運用イメージ



メモリ運用機構の行うこと

- カードの発行
- 顧客管理
- 事業者へのメモリレンタル業
- 事業者－メモリ運用機構間の決済
- 事業者－事業者間決済の代行
- 端末販売レンタル

サービスの内容（例）

- 事業者に対して1blockを10円程度のレンタル料で貸す。
- 事業者は使用者のカードに登録した時点でカード発行者にレンタル料を支払う
- 使用者にとって、各事業者の財布は全て相互使用ができる。（1つの財布のように見える）
- 事業者は独自のサービスをカードに組み込むことができる。（ポイントサービス等）
- 使用者に対しては、盗難・紛失時に全額保証を行う。
- 各事業者のトランザクションは、スピーディに低価格の手数料で決済できる。
- 各事業者間で、財布を使った場合は、事業者間で手数料を支払う。
- メモリのレンタル期間は1~3年程度とする。

FeliCa技術方式の信頼性

ISO 10536 - 1	コンタクトレスICカード
ISO 7816-1,-2,-3 / JIS6303	接点付きICカード
ISO 10373	プラスチックカード
ISO 7810 / JIS6301	磁気ストライプカード

◆機械強度

① 静的曲げ強度
② 動的曲げ強度
③ 動的ねじり強度
④ 動的角こすり
⑤ IC chipピンポイント強度
- IC局部曲げ強度
- ピンポイント静荷重
- ピンポイント衝撃強度

◆特殊環境

① 耐紫外線
② 耐X線
③ 耐フラッシュ試験
④ 耐外部磁界
⑤ 耐候性
⑥ 自動洗濯機洗い
⑦ 毒性
⑧ 剥離試験

◆熱的環境

① 低温動作・低温保存
② 高温動作・高温保存
③ 高湿動作
④ 低湿動作
⑤ 冷熱衝撃試験
⑥ 結露試験
⑦ プレッシャークッカー試験

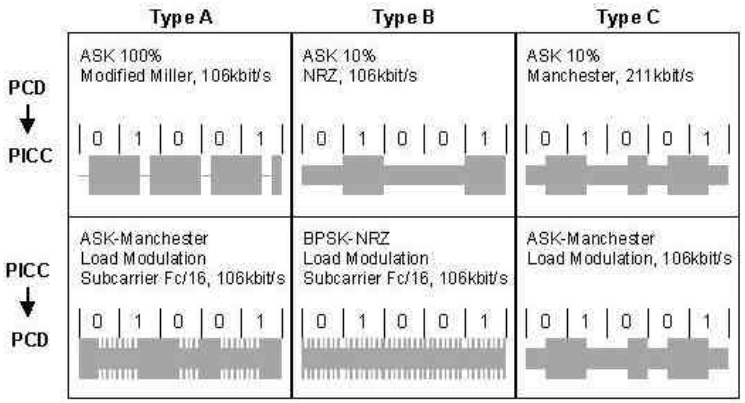
◆電気的環境

① 静電耐力試験

◆耐化学特性

① 食塩水・酢酸水・砂糖水・炭酸ソーダ水・他
② 塩水噴霧・人工汗（アルカリ性 / 酸性）

ISO-14443 Type A/B/C



Type-Cの技術的優位性

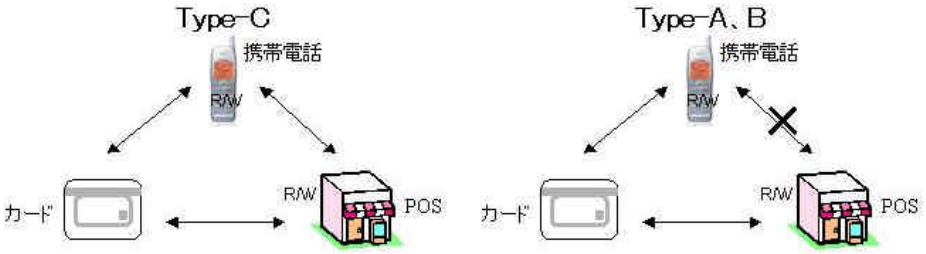
カード → リーダ

- サブキャリアを使わない変調方式
- リーダに対して同じ変調を返す方式

⇓

同デバイスの通信が可能

(カード-カード間、リーダ-リーダ間)



*FeliCa*の導入実績/計画

実績

香港（900万枚）	地下鉄、高速道路料金徴収、駐車場、コンビニ等
TRAMET 、東急、瀬の川スカイレール	定期券、交通チケット
コンサートチケット	チケット予約、購入
MEGA WEB（お台場）	電子マネーによる飲食、物販、乗物チケット
ゲートシティー大崎（２０００年２月）	電子マネーによる飲食、物販 入退出鍵、社員証、キャッシュカード
メディアージュ（２０００年４月）	電子マネーによる飲食、物販、チケット

計画

JR東日本(650万枚)（２００１年後半）	定期券、イオカード（リーダライタ　9,100台）
郵政省ミレニアムプロジェクト	携帯電話、携帯端末と組合せた標準化、実証実験
コンビニKIOSK端末	電子マネーへの入金、利用、会員カード
So-net（インターネット・プロバイダ）	インターネット経由での電子マネー、チケット
シンガポール(500万枚)（２００１年後半）	全土の地下鉄４路線、バス4,000台
中国（深セン）(100万枚)	バス5,500台、タクシー8,500台、地下鉄

非接触ICカードを活用したプリペイド型電子マネーの展開

プリペイド型電子マネー “Edy!”

電子マネー ＋入館カード

電子マネー ＋ 銀行キャッシュカード

- リアルとインターネットの双方で安全、便利に使える
- グローバルな電子マネーを目指す

*FeliCa技術方式*による電子マネーの特徴

1. 処理スピードが速い
   決済のスピードが要求されるコンビニ、KIOSK、
   スーパー、自動販売機などのマイクロ・ペイメントに向く

2. 信頼性が高い
   接点磨耗・異物（砂、汗、煙）等による信頼性低下がない
   振動の多い自動車内、列車内等でも高信頼性を維持

3. 複数のアプリが1枚のICカードに
   定期券、社員証、入退出鍵などの普段所有している
   社会インフラカードに電子マネーをいれられる

4. リアル・バーチャルの両方で共通利用可能
   接点がないため、家庭での利用時にも安心して使える
   様々な機器へのR/W内蔵がしやすい

*FeliCa*技術方式のサイバーでの展開

リアル・サイバー
共通のICカード

- ネットワーク
  サービスへのID
  (個人ごとの画面に
  即座にアクセス)
- 安全、便利な
  電子決済手段
  (電子マネー等)
- 電子チケット
  (購入とダウンロード)

*FeliCa*内蔵の携帯電話

FeliCa内蔵の携帯電話は、“電子財布”になる

- 電子マネー *Edy*
  - -入金
  - -利用
  - -残高確認
- チケット
  - -チケットの購入
  - -チケットのダウンロード
- キャッシュ
  - -モバイルバンキング
- クレジット
  - -クレジットでの支払い
- 会員証
  - -会員証
  - -ポイント
  - -クーポン
- ・・・その他各種サービス

FeliCa技術方式の情報公開

下記のWebサイトよりご参照ください。

http://www.sony.co.jp/Products/felica/index.html

17

メンバリスト

決済モデル検討SWGメンバリスト

No.	氏名	会社名	所属
	前川　徹 委員長	早稲田大学	国際情報通信研究センター

1	木下　眞希 リーダ	(株)ＮＴＴドコモ	MM事業本部MM企画部
2	長岡　二郎 サブリーダ	(株)シーメディア	
3	前田　正法 サブリーダ	(株)ジェーシービー	情報ネットワーク部
4	青木　一人	ノキアジャパン(株)	サービス&アプリケーション・プロダクトマーケティング部
5	飯塚　昭夫	(株)住友銀行	ネットビジネス企画部
6	石丸　直裕	国内信販(株)	ネット事業推進部
7	井本　明	東京通信ネットワーク(株)	技術部アステルサービス開発G
8	大山　芳明	(株)ダイエーオーエムシー	カード営業本部 企画管理部
9	岡崎　正一	三菱電機(株)	インフォメーション・ネットワーク事業推進本部
10	金子　稔	アコム(株)	経営戦略部
11	北村　正 (西尾　学)	ＮＴＴソフトウェア(株)	技術開発部エレクトロニックコマース技術センター
12	工藤　真男	日本エリクソン(株)	モバイル インターネット ソリューション、ソリューション部
13	倉井　智也	シャープ(株)	情報システム推進本部 営業システム企画部
14	酒井　清一郎 (小野瀬　研次)	(株)ディーディーアイ	移動体技術本部モバイル IT 部ゲートウェイビジネスG
15	佐久間　優	モルガン・スタンレー・ディーン・ウィッター	情報技術部
16	佐藤　順一	ソニー(株)	i-カードサービスソリューション事業部 サービス事業企画課

17	新谷　敦	(株)セントラルファイナンス	カード部
18	鈴木　輝美 (森田　栄二)	大日本印刷(株)	C&I 企画開発センター、ネットワークソリューション企画開発室
19	高橋　浩 (白土　由美子)	富士通(株)	システム本部
20	高山　久	松下電器産業(株)	マルチメディアシステム研究所メディア・オペレーション・グループMO第二チーム
21	田代　繁盛	(株)ディーシーカード	ディジタル事業推進部 EC企画G
22	津田　彰一 (谷　貴之)	富士電機(株)	情報システム事業部 SI ソリューション第二部
23	仲　望	(株)アクセス	事業開発室
24	永塚　郁也	ユーシーカード(株)	EC事業部
25	日置　敏昭 (太田　晴也)	三洋電機(株)	ハイパーメディア研究所KdMプロジェクト
26	藤原　希仁	(株)ミリオン・カード・サービス	IT ネットワーク事業部
27	堀　伸彦	共同印刷(株)	IC カード事業推進部
28	宮澤　徹 (松澤　尚樹)	ニフティ(株)	サービス企画部
29	牟田　敏保	アンリツ(株)	インフォソリューションズ 開発本部
30	森岡　照善	日本認証サービス(株)	営業担当
31	柳　健一郎	(株)東芝	流通・放送・金融システム事業部マーケティング事業推進担当
32	米井　博敏	ビザ･インターナショナル	メンバーリレーションズ

モバイル事務局

S1	成瀬　一明	電子商取引推進協議会	モバイルEC･WG
S2	太細　孝	電子商取引推進協議会	モバイルEC･WG

オブザーバ

	青島　幹郎	電子商取引推進協議会	

ICチップアドホック・メンバリスト

No.	氏名	会社名	所属
1	酒井　清一郎 リーダ	(株)ディーディーアイ	移動体技術本部モバイル IT 部ゲートウェイビジネスG
2	柳澤　孝浩	(株)ＮＴＴドコモ	MM事業本部MM企画部モバイルEC推進室
3	保谷　卓磨	Ｊ-フォン東日本(株)	サービス企画室コンテンツ企画・編集G
4	小峰　正裕	Ｊ-フォン東日本(株)	サービス企画室コンテンツ企画・編集G
5	日置　敏昭	三洋電機(株)	ハイパーメディア研究所KdMプロジェクト
6	高山　久	松下電器産業(株)	マルチメディアシステム研究所メディア・オペレーション・グループMO第二チーム
7	柳　健一郎	(株)東芝	流通・放送・金融システム事業部マーケティング事業推進担当
8	鈴木　輝美	大日本印刷(株)	C&I 企画開発センター ネットワークソリューション企画開発室
9	佐野　勝大	マイクロソフト(株)	マーケティングモバイル＆エンディットG
10	高橋　浩	富士通(株)	システム本部
11	白土　由美子	富士通(株)	システム本部
12	片山　透	日本電気(株)	ネットワークス開発研究所 第６研究部
13	長岡　二郎	(株)シーメディア	
14	前田　正法	(株)ジェーシービー	情報ネットワーク部
15	青木　直人	(株)ジェーシービー	情報ネットワーク部
16	米井　博敏	ビザ･インターナショナル	メンバーリレーションズ
17	山本　泰三	(株)三和銀行	ダイレクトバンキング部

モバイル事務局

S1	成瀬　一明	電子商取引推進協議会	モバイルEC･WG
S2	太細　孝	電子商取引推進協議会	モバイルEC･WG

ローカルワイヤレスインタフェース・アドホック・メンバリスト

No.	氏名	会社名	所属
1	辻　　秀一 リーダ	東海大	工学部電子工学科
2	牟田　敏保	アンリツ(株)	インフォソリューションズ 開発本部
3	桑田　大介	(株)ＮＴＴドコモ	MM 事業本部 MM 企画部モバイル EC 推進室
4	柳　健一郎	(株)東芝	流通・放送・金融システム事業部マーケティング事業推進担当
5	倉井　智也	シャープ(株)	情報システム推進本部 営業システム企画部
6	佐藤　順一	ソニー(株)	i-カードサービスソリューション事業部 サービス事業企画課
7	市川　琢也	ソニー(株)	i-カードサービスソリューション事業部 カード開発部 テクニカルフロント課
8	苅部　浩	TDK テクノ(株)	
9	高山　久	松下電器産業(株)	マルチメディアシステム研究所メディア・オペレーション・グループ MO 第二チーム
10	長岡　二郎	(株)シーメディア	
11	片山　透	日本電気(株)	ネットワークス開発研究所 第６研究部
12	安井　憲郎	(株)住友クレジットサービス	e ビジネス推進部
13	山本　泰三	(株)三和銀行	ダイレクトバンキング部
14	黒澤　聡	早稲田大学大学院	国際情報通信研究科

モバイル事務局

S1	成瀬　一明	電子商取引推進協議会	モバイル EC･WG
S2	太細　孝	電子商取引推進協議会	モバイル EC･WG

平成１３年３月発行
発行：電子商取引推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5500-3600
E-mail　info@ecom.or.jp