

FRAM[®]混載 多目的ICカード向け ソフトウェアソリューション HIPERSIM[™]

当社は次世代の不揮発性メモリといわれているFRAM[®]市場に1999年に参入して以来、リーディングカンパニーとして市場を牽引してきました。本稿では、FRAM[®]を搭載した多目的ICカード向けのソフトウェアソリューションであるHIPERSIM[™]について解説します。

はじめに

ICカード市場は、2001年度には全世界で約4000億円、2004年度まで年率30%以上の成長が見込まれます(当社調べ)。そうしたなか、社会インフラに対してICカードが持つ役割も、より高度なものへ推移すると予測されます。当社では、この社会的要求に対応すべく2001年8月、世界に先駆けて0.35μmFRAM技術を採用した32ビットCPUを持つFRAM混載多目的ICカード「HIFERRON[®]*1」の発売を開始しました。本稿では、HIFERRONを最大限に活用するためのソフトウェアソリューション「HIPERSIM」をご紹介します。

特長

HIPERSIMには次の特長があります。

- **世界初のFRAM混載32ビットCPUの多目的ICカード向けOSを提供**
FRAMの特性^{*2}を最大限に活かすOSとアプリケーションを提供します。

- **次世代携帯端末向けの本人認証機能であるSIMとUSIMをサポート**
GSMおよび3GPPで携帯端末利用の際に必須となる、本人認証機能のSIMとUSIMを提供します。
- **携帯端末へインターネットブラウザ機能を提供**
インターネットブラウザを持たないGSM向け携帯端末に、HIPERSIMを搭載したSIMとUSIMを付加することでインターネットが利用できるようになります。
- **多目的ICカードの短期間での開発をサポート**
利用目的に応じたOS構成と洗練された開発環境を提供することで、多目的ICカードの効率的な開発をサポートします。
- **複数アプリケーションの同時実行で多目的ICカードの効果的な利用が可能**
- **ICカードの国際標準規約に準拠**

構成

HIPERSIMは、ICカード向けOSと標準アプリケーションの2つで構成されています。これらは、表1に示す国際標準に準拠しています。

表1 HIPERSIMを構成するICカード向けOS / 標準アプリケーションが準拠する国際標準規約

コンポーネント	規約No.	備考
ICカード向けOS	ISO7816-4	Interindustry commands for interchange
	ISO7816-8	Security related interindustry commands
	ISO7816-9	Security attributes and additional interindustry commands
	ISO7816-15	Cryptographic Information Application
	WAP-260-WIM-20010712-a	Wireless Identity Module
標準アプリケーション	GSM 11.11	Subscriber Identity Module - Mobile Equipment (SIM-ME) interface specification
	3GPP TS 31.102	Characteristics of the USIM application
	3GPP TS 31.111	USIM Application Toolkit(USAT)
	ETSI TS 102.221	UICC-Terminal interface
	ETSI TS 102.222	Administrative commands for telecommunications applications

ICカード向けOS機能

HIPERSIMのICカード向けOSには次の機能があります。

● マルチタスク

マルチタスクのサポートは、携帯端末/ICカードリーダーからの処理命令を、複数のアプリケーションに分散・並列実行させることを可能にします。例えば、アプリケーション群の共通部分を1つのライブラリアプリケーションとして共通化することで、開発の効率化が図れます。

● PKI向けフレームワーク

PKI(Public Key Infrastructure)の業界標準仕様PKCS#11*3をサポートすることで、ICカードを既存インフラのセキュリティデバイスとして容易に組み込むことができます。

● マルチタスクに対応したファイルシステム

アプリケーションのファイルシステム(以降FS)は、FRAMの特性を活かす最適設計となっており、アプリケーションの高速処理に寄与します。FSはアプリケーションごとに保持することが可能で、ISO7816のセキュリティアーキテクチャをサポートしています。

図1にマルチタスク対応ファイルシステムを示します。

● 利用目的に応じたモジュール構成

ICカードの利用目的に応じて、次の3パターンの開発形態を採ることができます。

マニファクチャラーズ・セット

独自仕様で多目的ICカードを開発されるお客様向けです。HAL*4、ファイルシステム、メモリマネージャ、タスクマネージャ、暗号・復号制御、およびHIPERSIM・API(Application Program Interface)などの基本OSの機能を利用してアプリケーションを開発することができます。

ディベロッパーズ・セット

標準規格に準拠した多目的ICカードを開発されるお客様向けです。マニファクチャラーズ・セットと併せて使用することで、アプリケーションマネージャおよびISO7816準拠のファイルシステム・インタフェースを利用してアプリケーションを開発することができます。

テレコミュニケーションズ・セット

標準規格に対応したネットワーク接続機能を持つ、多目的ICカードを開発されるお客様向けです。ディベロッパーズ・セットに加え、USIMなどのアプリケーションやマイクロブラウザを含みます。

図2にHIPERSIMのモジュール構成を示します。

標準アプリケーション機能

HIPERSIMが標準で提供するアプリケーション機能は次のものです。

● UICC

普遍的な、次のICカード用インタフェースを提供します。

- ・ファイルへのリード/ライト
- ・セキュリティ制御(PIN, AUTHENTICATION)など

● USIM

GSMあるいは3GPPネットワークと携帯端末との間に、セキュアな通信を確立するアプリケーションです。このアプリケーションは、IC

カードの所有者とネットワークオペレータ間の契約者情報を保持し、グローバルローミングを可能にします。

図3にHIPERSIMの情報保持の概念を示します。

● Microbrowser

SIMを装着可能な携帯端末から、WAP*5によるインターネットアクセスを可能にします。Microbrowserは、サーバサイドで構文解析処理済みのバイトコード化された情報を携帯端末で表示するため、低速な回線でも快適なインターネットサーフィンを実現します。

図4にインターネットアクセスにおけるHIPERSIMの役割を示します。

また、次に説明するWIMと連携すれば m- コマースも実現できます。

● WIM(WAP Identity Module)

PKIで必須となる電子署名/証明検証を実現します。

図5にインターネットにおけるPKIの位置付けを示します。

● USAT(USIM Application Toolkit)ライブラリ

ICカード から携帯電話に対して、次のようなアクションを実現することができます。このUSATの機能を利用すれば、SIM装着可能な携帯端末に対して付加価値を付けたサービスが提供できます。

図1 マルチタスク対応ファイルシステム

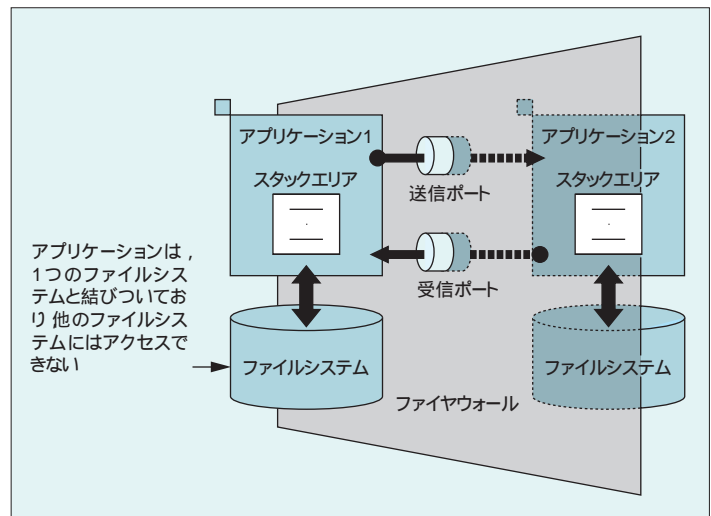
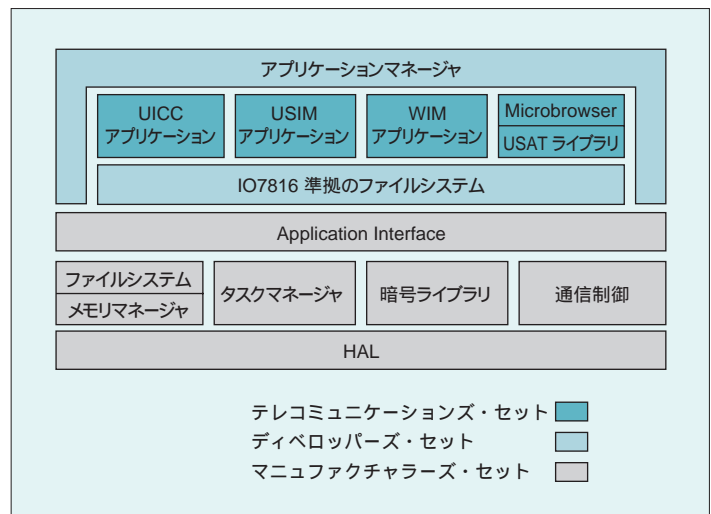


図2 HIPERSIMのモジュール構成



- ・ディスプレイへの文字出力
- ・ショートメッセージの送信
- ・トーン発音
- ・キーのスキヤニング

開発キット

表2に、HIPERSIMの開発キット構成とその他の所要開発環境を示します。

今後の展開

HIPERSIMは、本稿で説明した第一弾の機能のご提供のあと、

次の機能群を順次ご提供していく予定です。

- JVM(Java Virtual Machine): Sun Microsystems社が規定するJavaカードに準拠したJVM
- 非接触通信プロトコル: ISO 14443 TypeBに準拠した非接触通信プロトコル
- GPRS(General Packet Radio Service): GSMネットワークにおける高速データ通信規格
- オープンプラットフォーム: Global Platform社が推進するマルチアプリケーション管理の規格

* 1: HIFERRONの主な仕様については次のURLをご参照ください。

<http://pr.fujitsu.com/jp/news/2001/08/2.html>

* 2: FRAMは、現在のICカード向けメモリの主流であるEEPROMと比較して、書き込み速度が約1万倍、書き込み消費電力が約1/400倍、書換え回数が105倍のハイスペックを実現しています。

http://edevic.fujitsu.com/fj/CATALOG/AD05/05-00025/index_2e.html

* 3: PKCSは、米国RSA研究所が提案するPKI構成要素技術の規定した仕様群です。PKCS#11は、暗号トークンに関するインタフェース標準を規定します。

<http://www.rsa.com/rsalabs/pkcs/pkcs-11/>

* 4: HAL(Hardware Abstraction Layer): ハードウェアの機能をAPI化し、上位層であるOSにその機能を提供するレイヤです。

* 5: WAP(Wireless Application Protocol): 500以上の賛同企業で構成されたWAP Forum™において、携帯端末に関するワイヤレス仕様を規定しています。

<http://www.wapforum.org>

* HIPERSIM、HIFERRONは、富士通株式会社の商標です。

* FRAMはラムロン社の登録商標です。

* その他文中に記載の会社名および商品名は、各社の登録商標です。

図3 HIPERSIMの情報保持の概念

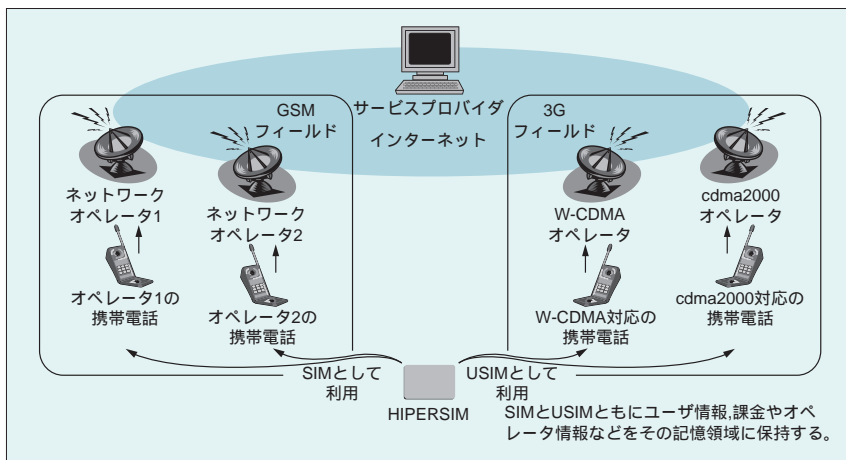


図4 インターネットアクセスにおけるHIPERSIMの役割

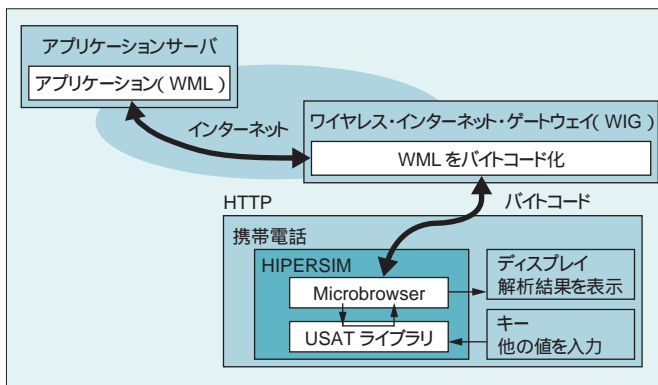


図5 インターネットにおけるPKIの位置付け

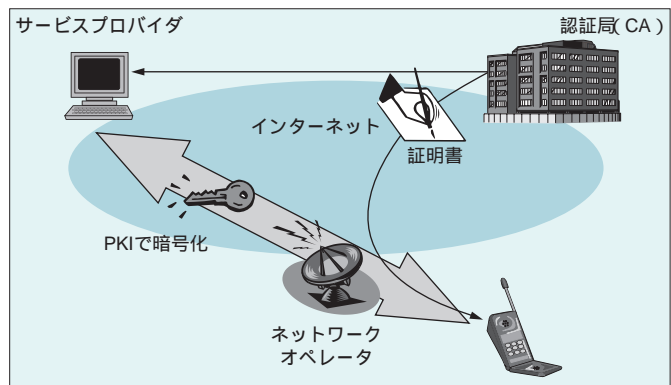


表2 HIPERSIM開発キットと所要開発環境

区分	名称	概要
開発キット	HIPERSIMソフト	HIPERSIMのOSとアプリケーション群をライブラリオブジェクト形式で提供します。
	Evaluationチップ (HIFERRON MB94RV2xxシリーズ)	多目的ICカード用チップHIFERRONのハードウェアおよびソフトウェアの開発・評価を行うためのEvaluation機能を搭載したLSIです。
	Evaluationボード	Evaluationチップを装着し、SOFTUNE・インサーキットエミュレータと併せて使用することで、ユーザシステムの開発評価を行うことができます。Evaluationボード上のフラッシュROMに開発したアプリケーションをダウンロードし、マスクROMのエミュレーションを実現します。
	ダウンロードツール (for Windows)	SOFTUNEで開発したHIPERSIMのアプリケーションを、EvaluationボードのフラッシュROM上へダウンロードするGUIツールです。
その他の所要開発環境	SOFTUNE V5.0	プログラム開発者のさまざまな要求に応えるべく設計された、使いやすさを追求した統合開発環境です。
	FR用インサーキットエミュレータ	SOFTUNEと連携して、HIPERSIM用アプリケーションの評価・デバッグが実行できます。

技術に関するお問い合わせ先: 電子デバイス事業本部 FRAM事業部

TEL(042)532-1422 FAX(042)532-2448

営業に関するお問い合わせ先: 最寄りの営業部門(裏表紙をご参照ください)