高いセキュリティのモバイル コンタクトレス サービスを実現するUIMカード

UIM Realizing Highly-Secure Mobile Contactless Services

石橋　孝信　　栗山　量一

■ ISHIBASHI Takanobu　■ KURIYAMA Ryouichi

UIM (User Identity Module) は，ネットワーク接続するための情報が書き込まれる小型のICカードで，現在国内外で広く普及している第3世代携帯電話で使用されている。

東芝は，携帯電話とUIM間の通信として従来から使用されているT=0プロトコル通信に加え，新たに電話関連規格団体European Telecommunication Standards Institute (ETSI) で規格化されたSingle Wire Protocol (SWP) / Host Controller Interface (HCI) を装備したUIMを開発した。このUIMは高セキュリティ機能を装備し，今後拡大が期待される，携帯電話を使用した決済の一つであるモバイル コンタクトレス ペイメントなどに応用できる製品である。

The user identity module (UIM), containing personalized user data for network connection, is a compact integrated circuit (IC) card that is widely used for third-generation (3G) cellular phones in the global market.　The T=0 protocol is currently used as the data transmission protocol between UIMs and cellular phones.

Toshiba has developed a new UIM for near-field wireless communication that supports the Single Wire Protocol (SWP) and Host Controller Interface (HCI) standardized by the European Telecommunications Standards Institute (ETSI), as well as the conventional T=0 protocol.　Furthermore, we have developed a high-security function for the new UIM, which is applicable to mobile contactless payment using cellular phones.

1　まえがき

近年，携帯電話では近距離無線通信を使ったモバイル コンタクトレス サービスの実現に期待が高まりつつある。モバイル コンタクトレス サービスは，携帯電話を店舗のPOS（販売時点情報管理）端末や自動販売機にかざして支払いやコンテンツの交換などを可能にするサービスで，買物だけでなく日常生活の多くの場面に簡単で便利な機能を提供できるものである。このためETSIをはじめとする各種標準化団体で，グローバルに使用可能な技術とするために標準化が進んでいる。特に，第2世代携帯電話のGlobal System for Mobile Communications（GSM）を採用する通信事業者団体GSM Association（GSMA）は近距離無線通信を使用し，高いセキュリティ機能を装備したUIMにモバイル コンタクトレス サービス アプリケーションを格納して運用するPay-Buy-Mobile Programmeを強く推進している。

UIMは，携帯電話が通信ネットワークに接続する際に必要な鍵情報及び各種のネットワークパラメータを格納し，接続に必要な暗号・認証処理を行う。また，携帯電話が使用者の手に渡った以降でも通信ネットワークを通じてアプリケーションの追加を可能とするために，Java Card™ (注1) 及び Global-Platform仕様に準拠する機能を装備している。

図1. UIMを装備した携帯電話 ― UIMを携帯電話内に挿入し，近距離無線通信で各種のサービスを利用できる。

UIM inserted into cellular phone

モバイル コンタクトレス サービスは，携帯電話と外部のモバイル コンタクトレス サービス端末（以下，サービス端末と略記）との間で近距離無線通信を行うことで実現される。このため，携帯電話には近距離無線通信を行うCLF（Contactless Front End）チップとアンテナが装備される。CLFとUIMの間はSWP(1)/HCI(2)通信でつながれている。サービス端末が，CLFを介して携帯電話内部のUIMに搭載されたモバイル コ

(注1)，(注2)　Java Card及びJavaは，米国Sun Microsystems, Inc.の米国及びその他の国における商標又は登録商標。

ンタクトレス サービス プログラムにアクセスすることで，サービスが提供される。近距離無線通信規格としては，主にISO/IEC 14443（国際標準化機構／国際電気標準会議規格14443）又はISO/IEC 18092が使用される。

東芝は，GSMAが推進するPay-Buy-Mobile Programmeに準拠して，T=0プロトコル通信とSWP/HCI通信をサポートし，高いセキュリティ機能を装備したUIMを開発した（**図1**）。

ここでは，開発したUIMの特長とモバイル コンタクトレス技術について述べる。

2　開発したUIMの特長

2.1　ハードウェア

2.1.1　UIMの構造　UIMは，コンタクト基板にICチップを実装し，封止剤で封止したICモジュール（**図2**）と，印刷が施されたカード基材で構成され，物理仕様はETSI TS 102 221[3]の規格に準拠する。UIMは，クレジットカードと同じ大きさのID-1形状で商品化され，携帯電話取扱店で携帯電話で標準的に使用されているID-000形状に抜き取られ，携帯電話に挿入される（**図3**）。

2.1.2　接続端子　UIMはコンタクト基板上に8個の外部端子を持ち，C1～C8の端子名称が与えられている。各端子に接続される信号は**表1**のとおりである[4]。

表1．接続端子の仕様
Specifications of terminals in contact circuit board

端　子	用　途
C1	電源入力（直流電源電圧5 V，3 V，又は1.8 Vを印加）
C2	リセット信号
C3	クロック信号（動作周波数は1～5 MHz）
C4	未使用
C5	グランド
C6	SWP/HCI通信
C7	T=0プロトコル通信
C8	未使用

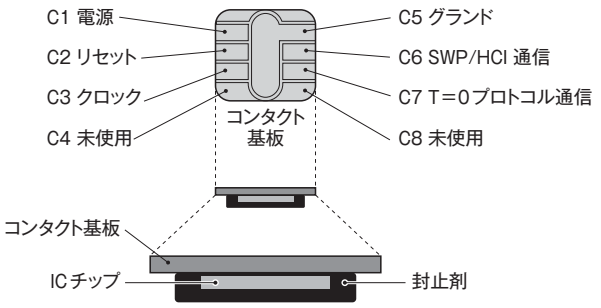

図2．ICモジュール — UMIのICモジュール部は，コンタクト基板にICチップを実装し，封止剤で封止して作製する。
IC module of UIM

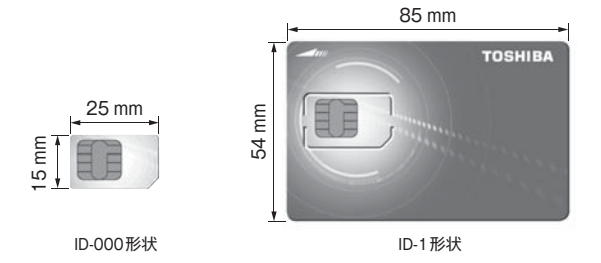

図3．UIMの形状 — 商品化時はID-1形状で，携帯電話に挿入するときは抜き取ってID-000形状にする。
Appearance of UIM

2.2　ソフトウェア

UIMのソフトウェアは，モバイル部，Java Card™及びGlobalPlatform部，Card Operating System（Card OS）部，及び携帯電話の使用者がモバイル コンタクトレス サービス アプリケーションの登録を行うアプリケーション部で構成される（**図4**）。

2.2.1　モバイル機能　通信事業者の通信ネットワークに接続するために必要な暗号・認証処理を行う。サポートする機能は，世界192か国で400以上の通信事業者のネットワークで使用されているGSM，第3世代携帯電話で採用されている3rd Generation Partnership Project（3GPP），及びそのほかの第3世代通信方式である。GSMは3GPP TS 51 011[5]，3GPPはETSI TS 102 221[3]の規格に準拠する。

2.2.2　Java Card™及びGlobalPlatform機能

Java Card™機能[6]-[8]は，Sun Microsystems, Inc.が開発したICカード向けのプラットフォーム仕様に準拠する機能で，

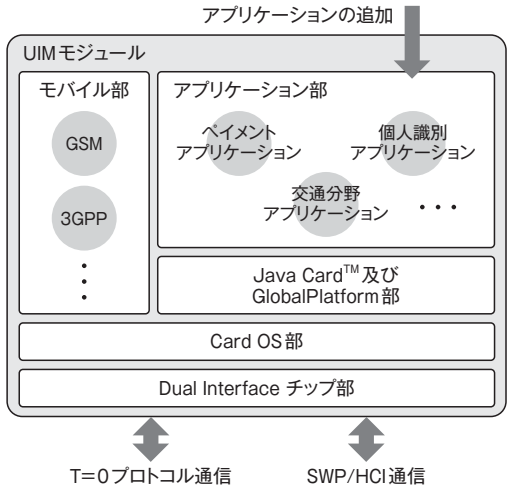

図4．UIMの機能構成 — 主に，モバイル部，Java Card™及びGlobalPlatform部，Card OS部，及びアプリケーション部で構成される。
Functional configuration of UIM

一般論文

Java™(注2)言語で記述されたICカード向けのアプリケーションをICカード上で動作させる環境を提供する。GlobalPlatform機能[9),10)]は，ICカード向けアプリケーションのICカードへの搭載機能とICカード内での状態管理機能を提供する。これらの機能を使って，モバイル コンタクトレス サービスに対応するアプリケーションをUIMへ搭載し，実行できるとともに，初期化や運用状態，一時機能停止状態などを管理できる。

Java Card™及び GlobalPlatform機能の主な特長を以下に示す。

(1) 携帯電話が利用者の手元にある場合でも，通信ネットワークを介して携帯電話内部のUIMに対し，アプリケーションの追加や削除が可能

(2) プログラム言語として広く利用されているJava™言語によるアプリケーションの開発と流用が可能

(3) Java Card™及びGlobalPlatform仕様で規定された高いセキュリティを備えたApplication Programming Interface（API）群を利用することでアプリケーション開発が容易

(4) UIM内に搭載されたアプリケーションの管理が容易

2.2.3 Card OS機能　カードの起動管理，通信制御，カード内部のメモリ管理，及びアプリケーション実行管理を行う。通信制御は，T=0プロトコル通信によるUIMとUIM Controller間の通信と，SWP/HCI通信によるUIMとCLF間の通信を同時に動作させることができる。アプリケーション実行管理は，外部からの指示に従って，外部の複数のサービス アプリケーションからそれぞれに対応するカード内のアプリケーションを並行して実行させることができる。

2.2.4 セキュリティ機能　UIMは，モバイル コンタクトレス ペイメント アプリケーションに対応するため，金融決済分野のICカードと同等の高度なセキュリティ機能が要求される。

セキュリティ機能の概念を**図5**に示す。UIMは，セキュリティ機能として，主に誤動作誘発，サイドチャネル攻撃，及び物理的攻撃の3種の脅威に対する防御機能を装備している。これらUIMの防御機能の代表的な動作を以下に示す。

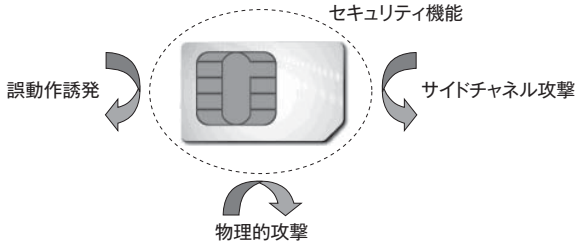

図5. セキュリティ機能の概念 — セキュリティ機能によって外部から受ける各種の攻撃を防御する。

Concept of security function

(1) 誤動作誘発　電源電圧や動作クロックを変動させるなどして誤動作を誘発し，UIM内部の格納データを破壊したり改ざんする攻撃が想定される。攻撃を防御する機能の一つとして，破壊や改ざんを検知するためにデータの正当性を確認する機能を装備している。

(2) サイドチャネル攻撃　UIMが動作しているときの消費電力や，処理時間，漏えい電磁波の変動パターンを測定して，外部から処理内容や処理データを解読する攻撃が想定される。攻撃を防御する機能の一つとして，実行処理中の消費電力，処理時間，及び漏えい電磁波の変動パターンをかく乱する機能を装備している。

(3) 物理的攻撃　UIMを分解してICチップを取り出し，解析を行う攻撃が想定される。この攻撃を防御する機能の一つとして，光検知回路をICチップ上に装備している。これにより，ICチップが外部にさらされた状態で動作すると，光検知回路によりICモジュールから取り出されたことを認識し，動作を停止する機能が働く。

3 モバイル コンタクトレス技術

3.1 通信技術

UIMでは，T=0プロトコル通信とSWP/HCI通信が同時に動作可能で，前者を使用する従来のモバイル機能に影響を及ぼすことなく，後者を使用するモバイル コンタクトレス サービスに対応できる。モバイル コンタクトレス サービスに関係する携帯電話内部の機能ブロックを**図6**に示す。UIMを制御するUIM Controllerと，携帯電話外部のサービス端末との近距離無線通信を行うアンテナ及びCLFが携帯電話に装備される。

UIMとUIM Controller間のT=0プロトコル通信は，電圧

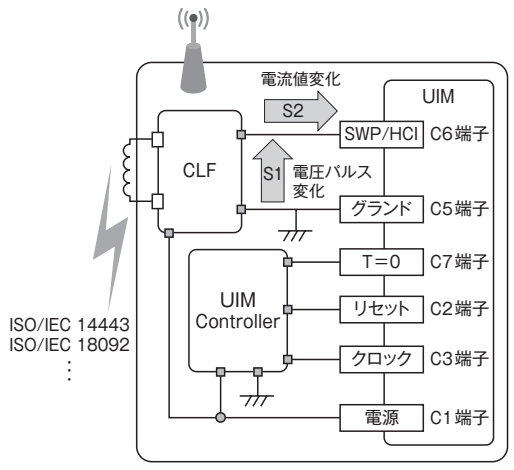

図6. 携帯電話とUIMの接続 — UIMは携帯電話内部でCLFとUIM Controllerと接続され，モバイル コンタクトレス サービスの機能を実現している。

Connection between cellular phone and UIM

レベル変化で通信データを認識し，二者間通信の一方が送信の場合に他方は受信となる，この関係を交互に切り替える半二重通信方式である。

UIMとCLF間のSWP/HCI通信は，同時に双方向に送信が可能な全二重通信方式である。CLFからUIMへの送信では電圧のパルス変化でデータが認識され（信号名称S1），UIMからCLFへの送信では，流れる電流の値でデータが認識される（信号名称S2）方式である。通信速度は，最大で1.6 Mビット/sまで実現可能である。

近距離無線通信の代表規格は，ISO/IEC 14443とISO/IEC 18092である。前者は，IC旅券やICカード運転免許証で使用され，後者は交通分野のICカードで広く使用されている。

3.2 モバイル コンタクトレス サービス

UIMは，携帯電話内のCLFとSWP/HCI通信によりモバイル コンタクトレス サービスを実現する。サービス端末，携帯電話内のCLF，及びUIMの動作フローの例を以下に示す。

(1) サービス端末は，無線信号を出して，利用者が携帯電話をかざすのを検出する状態にある。
(2) 利用者は，利用するサービスのサービス端末に，UIMが挿入されている携帯電話をかざす。
(3) CLFは，サービス端末からの近距離無線通信プロトコルを識別し，CLFがサポートしている通信規格と一致した場合，その近距離無線通信のプロトコルに従って，通信の初期処理をサービス端末との間で行う。
(4) サービス端末は，取引を実施するため，UIMへ処理命令としてコマンドを送る。
(5) CLFは，サービス端末から受信したコマンドをSWP/HCI通信で，UIMへ送る。
(6) UIMは，受信したコマンドを処理し，レスポンスとして処理結果をCLFに送信する。UIM内の処理手順は次のとおりである。
  (a) Card OS部によるコマンド受信
  (b) Java Card™及びGlobalPlatform部によるアプリケーションの選択とコマンド処理
  (c) Card OS部によるレスポンスの送信
(7) CLFは，UIMから受信したレスポンスを(3)で使用した近距離無線通信でサービス端末に送る。

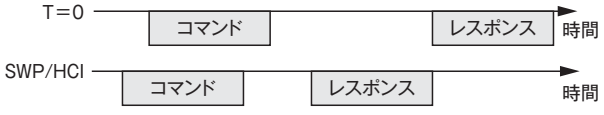

図7. T=0プロトコル通信とSWP/HCI通信の同時動作例 — T=0プロトコル通信とSWP/HCI通信は同時に動作可能で，それぞれのUIMへの入力（コマンド）に対してUIMからの出力（レスポンス）が返される。

Example of concurrent operation of T=0 protocol communication and SWP/HCI communication

(8) 取引内容により(4)～(7)を複数回繰り返す。この取引が実行中に，UIMとUIM Controller間にT=0プロトコル通信が発生しても，UIMとCLF間のSWP/HCI通信は独立して通信処理ができる（**図7**）。

4 あとがき

CLFを実装した携帯電話が，今後商品化されることが予想されるが，今回開発したUIMをこれに搭載することで，近距離無線通信による複数のモバイル コンタクトレス サービスを一つの携帯電話で実現することができる。また，高いセキュリティを実現したことで，今後の多様なモバイル ペイメント アプリケーションの搭載要求にも対応できると期待している。

文 献

(1) ETSI technical committee Smart Card Platform (SCP). ETSI TS 102 613 : 2008. Smart Cards; UICC - Contactless Front - end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7) v7.3.0. 57p.
(2) ETSI (SCP). ETSI TS 102 622 : 2008. Smart Cards; UICC - Contactless Front - end (CLF) interface; Host Controller Interface (HCI) (Release 7) v7.2.0. 52p.
(3) ETSI (SCP). ETSI TS 102 221 : 2008. Smart Cards; UIC-C - Terminal interface; Physical and logical characteristics (Release 7) V7.12.0. 174p.
(4) ISO/IEC 7816-3 : 2006. Identification cards - Integrated circuit cards - Part 3: Cards with contacts - Electrical interface and transmission protocols. 58p.
(5) 3GPP. 3GPP TS 51 011 : 2005. 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (Release 4) V4.15.0. 173p.
(6) Sun Microsystems, Inc. Java Card 2.2.2 Virtual Machine Specification. 2006, 276p.
(7) Sun Microsystems, Inc. Java Card 2.2.2 Runtime Environment (JCRE) Specification. 2006, 148p.
(8) Sun Microsystems, Inc. Java Card 2.2.2 Application Programming Interface. 2006, 409p.
(9) GlobalPlatform Inc. GlobalPlatform Card Specification Version 2.2. 2006, 375p.
(10) GlobalPlatform Inc. GlobalPlatform Card UICC Configuration Version 1.0. 2008, 46p.

石橋 孝信 ISHIBASHI Takanobu
社会システム社 セキュリティー・自動化システム事業部 ICカードシステム営業部主務。ICカードシステムの営業技術業務に従事。
Security & Automation Systems Div.

栗山 量一 KURIYAMA Ryouichi
社会システム社 小向工場 ICカードシステム部参事。
ICカードのソフトウェア開発に従事。
Komukai Operations