New Technical Report

ICカード（加入者情報モジュール）対応車載機

Car Phone for IC Card (Subscriber Identity Module)

NTT DoCoMoでは，セキュリティーアルゴリズムおよび加入者情報を内蔵するセキュリティー性の高いICカード（加入者情報モジュール）を使用し，一つのICカードで複数の車載機を利用できるという利便性の向上に向け，開発を進めてきた．

本稿では，ICカードインターフェースにおける標準規格の概要ならびに，その標準規格に基づいて開発したICカードおよびICカード対応車載機の技術概要および機能について述べる．

The IC Card (Subscriber Identity Module) and the Car Phone has been developed in NTT DoCoMo in order to improve the convenience that plural Car Phones can be used by one IC Card which stored the security algorithm and the subscriber identities.

In this article, we describe the standardization outline of the IC Card interface and also the technology outline and the functions of the IC Card and the Car Phone based on the standardization.

矢崎　英俊　Hidetoshi Yazaki
平児玉　功　Isao Hirakodama
越前谷　三夫　Mitsuo Echizenya

まえがき

1993年4月よりサービス開始しているデジタル移動通信方式であるPDCシステム[1]の移動機では，移動機内に書き込まれたセキュリティーアルゴリズムおよび加入者情報（加入者番号，ネットワーク情報，メモリダイヤル情報など）を用いて基地局と通信を行う．このセキュリティーアルゴリズムおよび加入者情報は移動機内に物理的に取り付けられているメモリ領域に書き込まれており，簡易に取り外すことは不可能となっている．近年になり，CPU（中央処理装置），ROM（プログラム領域），EEPROM（加入者情報領域）を備えたセキュリティー性の高いICカードが安価で普及し始め，PDCの標準規格においても，加入者情報モジュール化が採り入れられた．NTT DoCoMoでは，加入者情報を書き込んだICカードを車載機に装着して使用することで，1つの加入者情報で複数の車載機を使用できるという利便性の向上を図るため，ICカードおよびICカード対応車載機の開発を進めてきた．

本稿では，ICカードの物理的および電気的特性，セキュリティー機能，ICカードのインターフェースを「デジタル方式自動車電話システム，ARIB標準規格RCR STD-27Fの付録4」に基づいて説明し，その後，今回開発したICカードおよびICカード対応車載機のハードウェア構成，機能概要について述べる．

ICカードインターフェースにおける標準規格の概要[1]

■ICカードの物理的および電気的特性

ICカードは3Vまたは5Vの外部電圧と1～5 MHzの外部クロックの供給により動作する．標準化では，通信プロトコルとしてはISO規格であるT＝0プロトコル（キャラクタ転送プロトコル）を必須としており，本プロトコルは1バイトのデータ単位で送受信およびエラーチェックを行うものである．ICカードとのデータ送受信のための信号線は1本のため，半二重通信方式で行う．ICカードの形状としてはフルサイズICカード（クレジットカードと同等のサイズ）とプラグインICカード（ICチップと同等のサイズ）の2種類がある．本ICカード内部のブロック図を図1に示す．ICカード内のROM領域には，セキュリティーアルゴリズム，移動機からのコマンドに対する解析／実行／応答，データ管理，アクセス管理などのプログラムを格納し，またEEPROM領域には移動機が通信を行ううえで必要な情報として，加入者番号，移動局番号，ホーム網情報，ローミング情報，発信履歴情報，着信履歴情報，メモリダイヤル情報，通話時間情報，通話料金情報などの用途の異なる情報がファイル単位で書き込まれる．

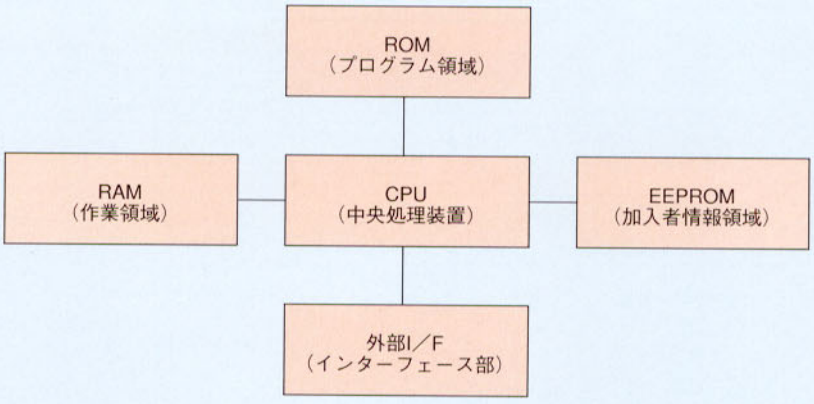

図1　ICカード内部のブロック図
Figure 1　Block Diagram of IC Card.

■ICカードのセキュリティー機能

ICカードのセキュリティーメカニズムを図2に示す．移動機とICカードとの通信はコマンド（命令）とレスポンス（応答）のやりとりで成り立っており，コマンドは移動機からICカードに命令として出力し，その命令に対する実施結果（正常，異常）をレスポンスとして，ICカードから移動機に報告する．すなわち，移動機が能動的装置で，ICカードは受動的装置という位置づけとなる．移動機からICカードに対するコマンドは複数用意されており，そのコマンドの中でアクセス条件を必要とするコマンドを命令重要度により，5つのレベル（データ読出／検索＜データ更新＜データ加算＜ファイル無効化＜ファイル有効化）にレベル分けされている．各ファイルにおける各5レベルのコマンドのアクセス条件には，「ALWAYS」，「PIN1」，「PIN2」，「発行者」，「NEVER」のいずれかが独立して設定されており，移動機はこの条件を満足しない限り，該当ファイルに対する該当レベルのコマンドがアクセスできない．「ALWAYS」は常にアクセス可能を意味し，「NEVER」は常にアクセス不可を意味する．「PIN1」および「PIN2」は4～8桁のパスワードで，本パスワードの照合成功により，アクセス権を取得できる．「発行者」のアクセス条件は発行者管理のため規定していない．PIN1およびPIN2はICカード内部に格納されており，外部からPIN1もしくはPIN2のパスワードを入力し，照合が成功した場合は全ファイルの中の全アクセス条件を対象として，本PIN種別が設定されているレベルのコマンドがアクセス可能となる．このアクセス条件の中で通信に必要な必須情報の「データ読出／検索」のアクセス条件はすべて「PIN1」に設定されているため，移動機は通信を行う前にPIN1の照合を行い，情報を読み出す必要がある．その他のアクセス条件に「PIN2」が設定されていれば，必要に応じてPIN2の照合を行い，アクセス権を取得する．

また，ICカードへアクセスを許可するためのPIN照合では照合許容回数が規定されており，3回連続して照合が失敗すると，ICカードはPIN照合を受け付けなくなる．この状態を解除するため，8桁のUNBLOCK PINと呼ばれる解除用パスワードで照合を行う．本UNBLOCK PINの照合が成功すると，本状態が解除され，再びPIN照合を受け付ける．しかし，本UNBLOCK PIN照合にも照合許容回数が規定されてお

＜ファイルに設定されているアクセス条件＞

アクセス条件／ファイル名	レベル1 データ読出／検索	レベル2 データ更新	レベル3 データ加算	レベル4 ファイル無効化	レベル5 ファイル有効化
ファイルA	PIN1	PIN1	PIN2	発行者	発行者
ファイルB	PIN1	PIN2	発行者	発行者	発行者
ファイルC	PIN1	PIN1	PIN1	PIN2	発行者
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

PIN1で照合成功

＜ファイルに設定されているアクセス条件＞

アクセス条件／ファイル名	レベル1 データ読出／検索	レベル2 データ更新	レベル3 データ加算	レベル4 ファイル無効化	レベル5 ファイル有効化
ファイルA	PIN1	PIN1	PIN2	発行者	発行者
ファイルB	PIN1	PIN2	発行者	発行者	発行者
ファイルC	PIN1	PIN1	PIN1	PIN2	発行者
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

：この部分のコマンドがアクセス可能

図2　セキュリティーメカニズム
Figure 2　Security Mechanism.

り，10回連続してUNBLOCK PINの照合が失敗すると，UNBLOCK PIN照合も受け付けなくなり，本状態を解除する手段を与えられていない．なお，PIN1に関してはUNBLOCK PIN1，PIN2に関してはUNBLOCK PIN2の解除用パスワードが各々のPINに対して割り当てられており，PIN1とPIN2およびUNBLOCK PIN1とUNBLOCK PIN2の照合許容回数は同一である．

■ICカードのインターフェース

ICカードを移動機に装着して，移動機を電源ONすると，まずICカードに対して活性化という処理が行われる．本処理は移動機からICカードに対して外部電圧および外部クロックを供給し，ICカードを起動させる．本処理が完了すると，通信に必要な情報を読み出すため，操作部からPIN1を入力し，ICカードに対してPIN1照合を行わせる．入力されたPIN1とICカード内に記憶されたPIN1の照合はICカード内部で行い，照合が成功しない限り，通信ができないこととなる．照合が成功した場合，移動機はICカードから通信に必要な情報を読み出し，基地局と通信を行う．その後の移動機と基地局との間で行う認証処理に関する認証アルゴリズムはICカード内に隠蔽されており，基地局から認証要求を受信した移動機はICカードに対して認証演算命令のコマンドを出力し，ICカードは認証アルゴリズムに従って演算する．演算結果はレスポンスとして移動機に出力し，移動機は受信した演算結果をそのまま基地局へ送信する．このような認証アルゴリズムをICカード内に閉じこめ，セキュリティーアルゴリズムの部分を移動機に依存させない構造となっている．

ICカード対応車載機とICカード

■ハードウェア構成

ICカード対応車載機であるデジタル・カーホンE401の主要諸元を表1，本車載機の装置構成を図3，本車載機の外観を図4，本移動機に装着して使用するDoCoMoアプリケーションカードの主要諸元を表2，本ICカードの外観を図5に示す．車載機は無線機本体，ICカードリーダー／ライター内蔵型電話機，電話機置台，DC12V電源端子[2]，RFアンテナ端子[2]から構成される．ICカードリーダー／ライター内蔵型電話機では，3Vまたは5Vの外部電圧と約3MHzの外部クロックをICカードに供給して9600bit/sのボーレートで通信を行う．基地局と通信するため，無線機本体で必要な情報[1]（加入者番号，移動局番号，ネットワーク情報など）は10芯ケーブル[2]を通じて電話機から転送される．本体内の無線部は，無線区間伝送レート[1]ではフルレートとハーフレートをサポートし，無線帯域[1]は800MHzのデジタル帯域はもちろんのこと，デジタル化された800MHzのアナログ帯域にも対応している．

表1　デジタル・カーホンE401の主要諸元
Table 1　Digital Car Phone E401 Major Specification.

項　目	諸　元
無線周波数帯	940.050～957.975MHz（デジタル800MHz帯）
	925.050～939.975MHz（アナログ800MHz帯）
送受周波数間隔	130MHz（デジタル）
	55MHz（アナログ）
最大送信電力	2.0W
キャリア周波数間隔	50kHz（25kHzインターリーブ）
キャリア数	718（デジタル）
	598（アナログ）
アクセス方式	3チャネル／キャリアおよび6チャネル／キャリア
変調方式	π／4シフトQPSK
音声符号化方式	V-SELP（11.2kbit/s）
	PSI-CELP（5.6kbit/s）

■ICカード対応車載機の機能概要

(1)　ICカード装着状態監視制御

本車載機は電源ON中にICカードの物理的な装着状態を常に監視しており，本ICカードが抜かれた場合は直ちに現在の処理を中止し，ICカード挿入を促すための警告表示を行う．また本状態でICカードが再び装着された場合は自動的にICカードを活性化処理し，電源ON時と同一の処理を開始する．

(2)　コマンド再送制御

本ICカードとの通信処理において，ICカードからのレスポンスが非受信もしくはレスポンスデータが異常の場合，前回出力したコマンドの再送を行う．再送した結果，再びレスポンスが非受信もしくはレスポンスデータが異常の場合は，ICカードが異常という旨の警告表示を行う．

(3)　加入者情報読出制御

本車載機は本ICカードとの組み合わせを装着ごとにチェックしており，車載機とICカードの各々において，今回の組み合わせが前回の組み合わせと異なる場合はICカードから全加入者情報を読み出し，通信を開始するが，同一の場合は前回読み出した情報と同一であると判定し，ICカードからあらためて全加入者情報の読み出し処理は行わず，前回読み出して記憶していた一部の加入者情報をそのまま使用することで，電源ON時から通信可能状態までの起動時間の短縮を図っている．

(4)　親子電話機

本車載機から電話機までの10芯ケ

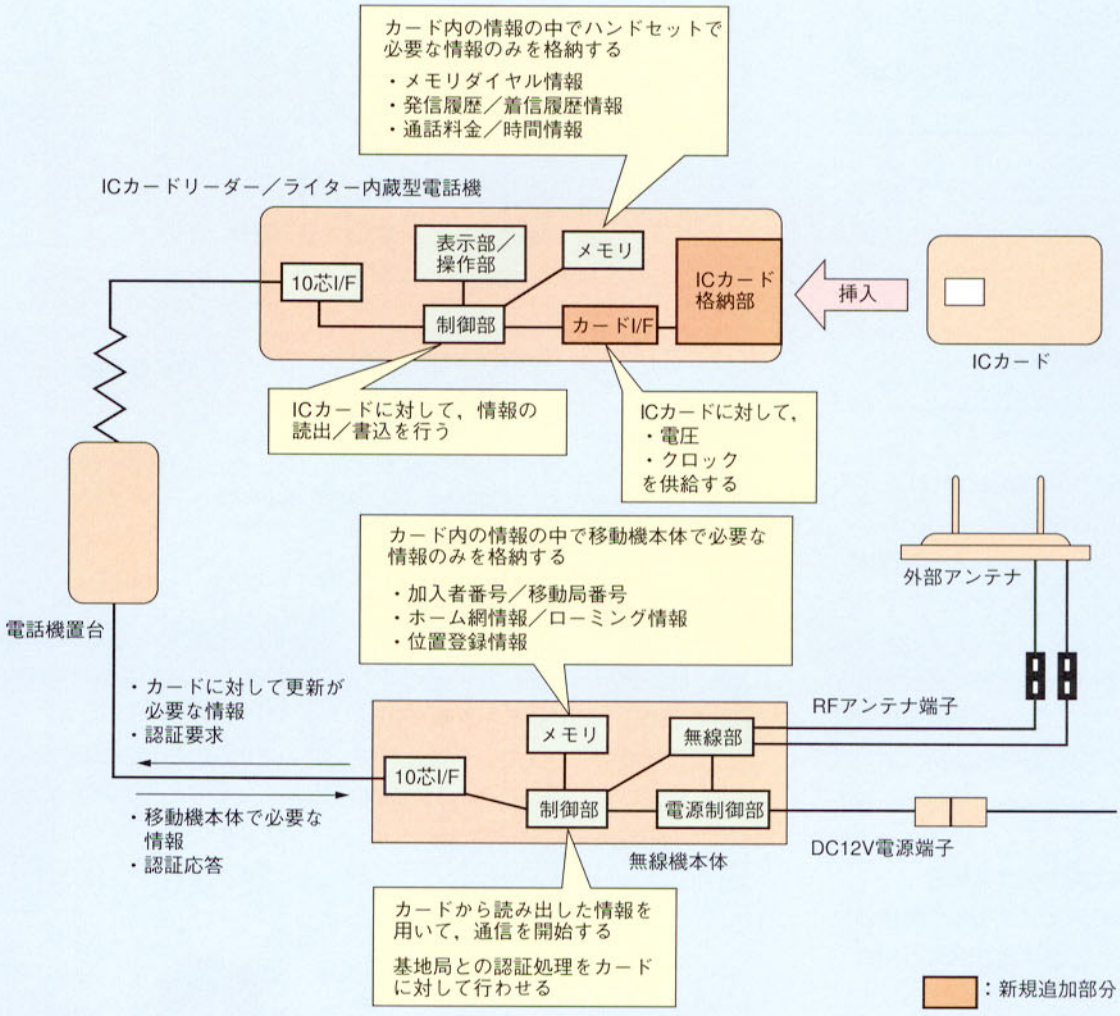

図3　デジタル・カーホンE401の装置構成
Figure 3　Digital Car Phone E401 Configuration.

左から無線機本体（上部に音声認識アダプタ装着），ICカードリーダー／ライター内蔵型電話機（下部は電話機置台），ハンズフリー用マイク

図4　デジタル・カーホンE401の外観
Figure 4　Digital Car Phone E401.

ーブル[2]を専用の分岐装置で分岐させ，その先に電話機を複数台接続することで，1台の無線機を複数の電話機で共有できる．この場合，親電話機に装着されているICカードの加入者情報を使用する．

(5)　オーナー設定機能

本車載機を複数のICカードで使用する場合，その中の1枚のICカードをオーナーカードとして本車載機に登録しておけば，他のICカードを装着し，車載機の諸機能の設定を変更した後でも，オーナーとして登録しておいたICカードを再び装着したときには，前回その車載機で使用していた環境設定に戻して動作させる．

表2　DoCoMoアプリケーションカードの主要諸元
Table 2　DoCoMo Application Card Major Specification.

項　目	諸　元
ボーレート	約2,688～13,440bit/s
動作周波数	1～5MHz
動作電圧	3V／5V
通信方式	半二重調歩同期方式
伝送プロトコル	T=0プロトコル
EEPROM容量	8kバイト
カード形状	フルサイズカード

図5　DoCoMoアプリケーションカードの外観
Figure 5　DoCoMo Application Card.

■ICカード対応車載機におけるその他の新規追加機能

(1)　漢字対応ショートメール機能

本機能はカナ文字，英字，数字の半角文字のメールをショートメールセンター経由で相手の移動局に送信するという従来のショートメール機能に対して，新規で漢字，記号の全角文字の送受信も可能としたショートメール機能の拡張版である．

(2)　音声認識アダプタ対応

本音声認識アダプタを本車載機の無線機に接続し，電話機置台に専用のハンズフリー用マイクを接続することにより，音声による発着信を可能とする．あらかじめ本音声認識アダプタに登録していた接続先をマイクに対して発声すると，音声認識アダプタは入力された音声とあらかじめ登録されている音声を照合し，一致するものがあれば，それと対で登録していた電話番号を読み出す．その後，「デンワ」と発声すると，その電話番号で発信する．着信時でも「デンワ」と発声すれば，電話を受けられる．また，本アダプタは非電話アダプタの機能も兼ねているため，専用ケーブルで本音声認識アダプタとパソコン本体のRS-232Cインターフェースを直結して，データ通信も可能としている．

(3)　時計機能

本車載機に時計機能を新規で追加し，発信履歴情報および着信履歴情報の中に発信および着信した時刻情報を付加している．

あとがき

以上，PDC方式におけるICカードインターフェース標準規格の概要とその標準規格に基づいて開発したICカードおよびICカード対応車載機の技術および機能の概要について述べた．これにより，高セキュリティー性を保ちつつ，1つの加入者情報で複数の移動機を使用できるという利便性の向上が実現できる．今後は本ICカードの機能を利用したアプリケーションサービスの拡張，さらに将来的にはICカードに対してアプリケーションプログラムのダウンロードなどを実現する移動機の開発に取り組む予定である．

文　献

[1] デジタル方式自動車電話システム，標準規格RCR STD-27F 1997.2.
[2] 自動車携帯電話サービスを利用するための技術参考資料（デジタル方式）．