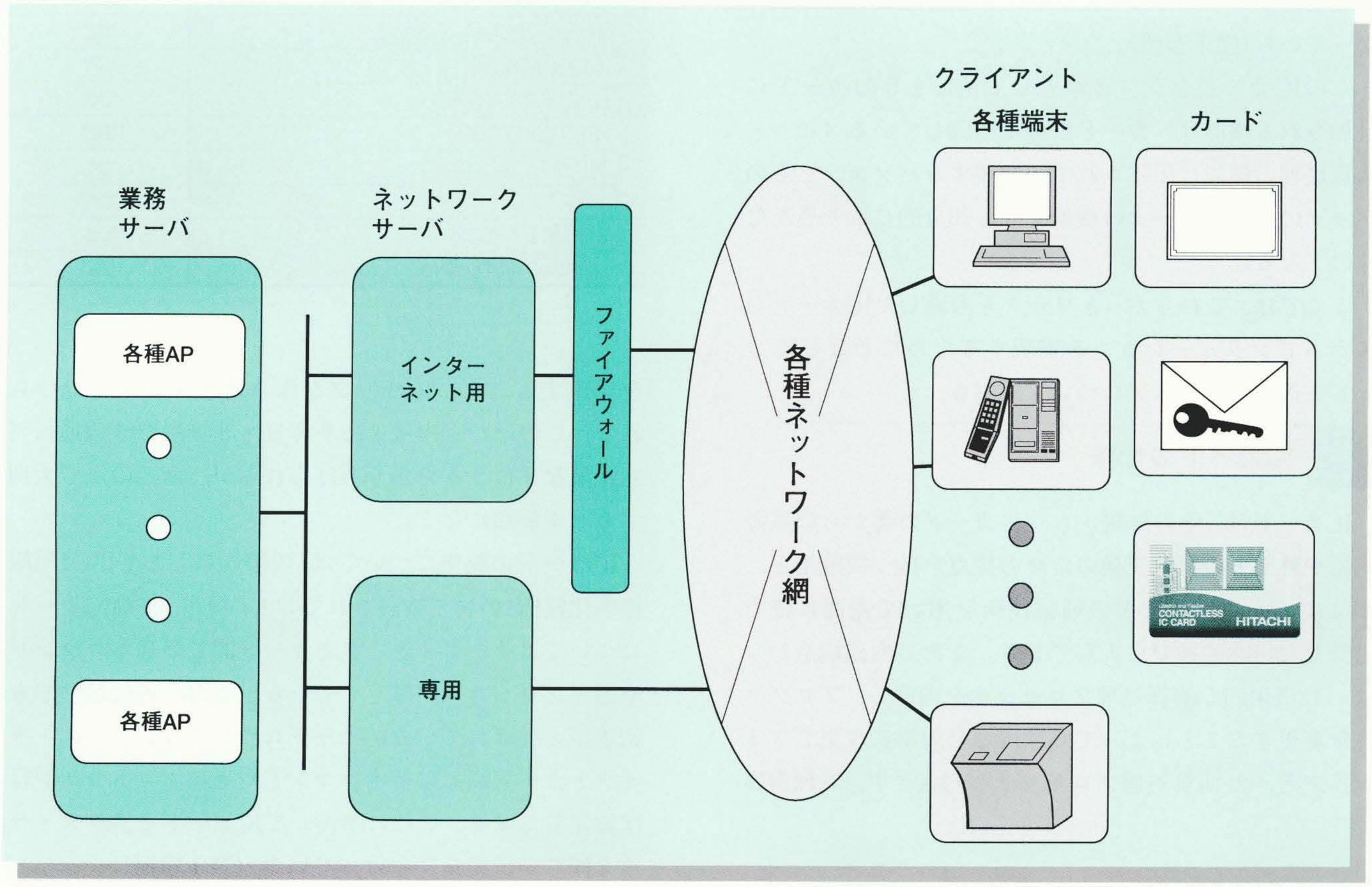
ICカードを支える基本ソフトウェア

IC Card Control Software

朝倉　久　*Hisashi Asakura*
稲葉純二　*Junji Inaba*
伊藤　修　*Osamu Itô*



注：略語説明　AP（Application Program）

システムにおけるICカードの位置づけ

各種ネットワークの普及・広域化に伴い，今後，これらのネットワークを経由した各種業務やアプリケーションの入口を開ける鍵として，ICカードはシステムのキーデバイスとして重要になる。

情報のディジタル化と広域ネットワークの急速な発展に伴い，EC（Electronic Commerce：電子商取引）や電子チケット，電子マネーなどの各種システムにICカードを取り入れた「ICカードシステム社会」が実現しつつある。

カード単体でとらえると，ICカードには改ざん・コピー偽造などの不正を防ぐための高度な技術が求められると同時に，システムとしてとらえると，専用用途から多目的・多分野用途まで，またセキュリティの低い分野から高い分野まで，その目的に応じた操作性・利便性が求められている。そのため，ICカードに使われるマイクロプロセッサの技術開発によって情報の機密性を確保するだけではなく，システムとして機能するためのICカードのアプリケーションや上位装置・上位アプリケーションでの機密性・操作性・利便性を確保することが必要である。

日立製作所は，今後のICカードシステム発展のために，従来の上位クライアント端末までの各種アプリケーションソフトウェアとアプリケーション開発支援ソフトウェアに加え，非接触ICカード内部のソフトウェア，およびアプリケーションソフトウェアと非接触ICカードのインタフェースをサポートするソフトウェアを開発している。

1 はじめに

ICカードは，欧州を中心に公衆電話から普及が始まってきている。最近，多くの分野でその導入が検討され，各種実験が行われている。

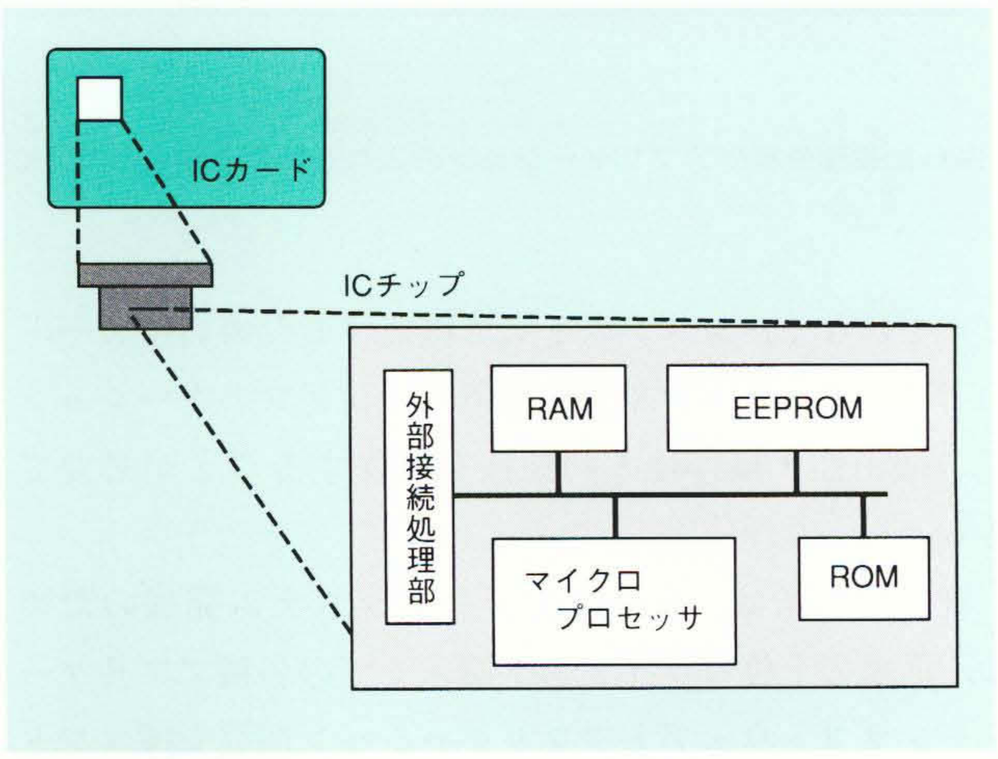
ICカードの構造はきわめてシンプルであり，プラスチックのカードの中に演算処理部，メモリ部および外部接続処理部とが一体となったチップが埋め込まれた形状になっている(**図1**参照)。

このICカードをシステムとして見たときのカードに付加される機能は，カード自身に内蔵しているメモリ・演算処理の機能に限定されず，接続するパソコンとそのバックのネットワークの機能までも部分的に取り込んだものとなる。

ここでは，これらネットワークも考慮したICカードシステムでソリューションを実現するために必要なICカード支援ソフトウェアについて述べる。

2 ICカードの仕様

ICカードは，その外観から，(1) カード外部からの電源供給や外部との情報交換のための接点を持つ接触型と，(2) これらを電磁波などの通信技術を用いて表面に接点を持たない非接触型に大別できる。また，内部構造からは，(1) 汎用的な演算処理プロセッサを内蔵し，プログラムを変更することによって処理内容を簡単に変更できるタイプと，(2) 演算処理プロセッサを内蔵せず，処理内容を変更するごとにICチップを作り直すタイプに分けられる。このほか，内蔵メモリ容量・非接触型での通信可能距離などによる分類もあげられるが，前述の点で大別すると4種類になる。



注：略語説明
RAM(Random Access Memory)，ROM(Read-Only Memory)
EEPROM(Electrically Erasable Programmable ROM)

図1 ICカードの構造
ICカードは，カードの中にチップが埋め込まれているだけの簡単な構造である。

表1 ISO/IEC(国際標準化機構 国際電気標準会議)で規定しているコマンド例
この表以外に，各業界でもICカードのコマンドを独自に規定している。

コマンド名	略 称
INTERNAL AUTHENTICATE	'88'
SELECT FILE	'A4'
READ BINARY	'BO'
READ RECORD(S)	'B2'
GET RESPONSE	'CO'
ENVELOPE	'C2'
GET DATA	'CA'
WRITE BINARY	'DO'
WRITE RECORD	'D2'
UPDATE BINARY	'D6'
PUT DATA	'DA'
UPDATE RECORD	'DC'
APPEND RECORD	'E2'

ICカードの規格については，国際規格としてISO(国際標準化機構)の場で検討されており，現在，接触ICカードについてはリーダ・ライタとカード間での基本コマンドや通信プロトコルが確定している。また，非接触型でも密着型と呼ばれているICカードについては，リーダ・ライタとカード間での基本コマンドや通信プロトコルがほぼ確定しており，これに準拠してICカードとリーダ・ライタ間での情報交換を行っている[1](**表1**参照)。

今回開発したのは，この密着型ICカード内部のコントロールウェアと，上位装置に組み込んで上位アプリケーションとのインタフェースをサポートするリーダ・ライタソフトウェアである。

3 ICカードのコントロールウェア

3.1 コントロールウェアの基本機能

コントロールウェアとしての基本的な機能として，従来のコンピュータと同様に，以下のようなものがある(**図2**参照)。

(1) 上位のリーダ・ライタとの情報交換をするための送信受信処理や，メッセージ組立・復元処理を行う「通信制御処理機能」

(2) 送信受信のためのデータや，演算処理中のデータを一時的に蓄えるバッファの「管理制御機能」

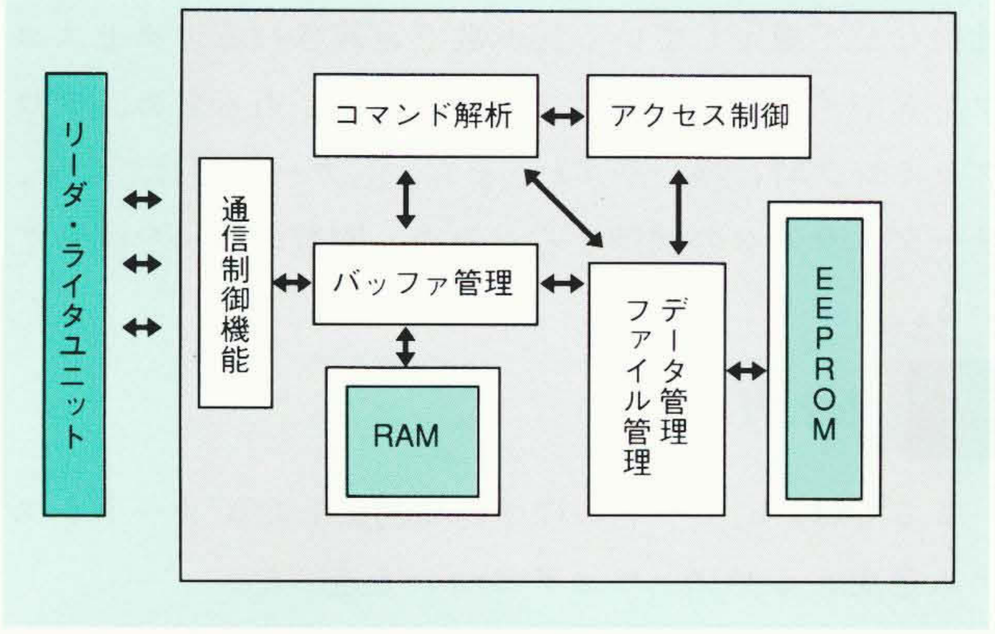


図2　コントロールウェアの構造

ICカードのコントロールウェアの特徴は，アクセス制御機能を持つことである。

(3)　受信したメッセージからコマンドを判定解析し，該当コマンドルーチンへメッセージ振り分け処理を行う「コマンド解析機能」

(4)　EEPROMに，実際に作成されるファイルの管理と，そのファイル内部のデータへのアクセスとファイル形式に応じたレコードポインタ(開始位置，最終レコード位置，現在アクセス中レコード位置)を保持し，必要に応じて更新するなどの管理を行う「ファイル管理・データ管理機能」

(5)　ICカード内部情報アクセスに関して，ファイルやバッファへのアクセス権限の有無などの確認(認証)を行う「アクセス制御機能」

これらの機能を用いて，ICカードのマルチアプリケーション機能，セキュリティ管理機能を応用機能としてサポートしている。

3.2　コントロールウェアの応用機能

3.2.1　マルチアプリケーション機能

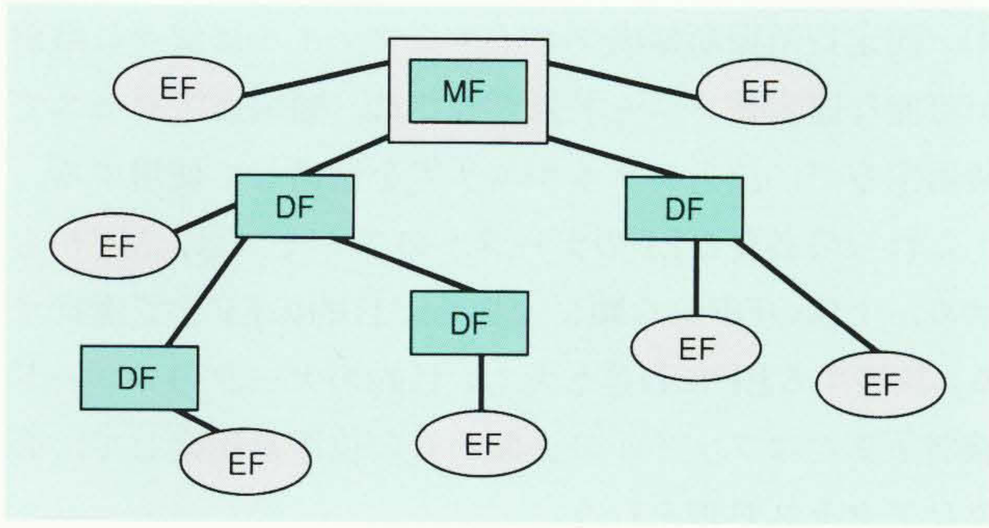
密着型ICカードを多目的・多分野で活用できるようにするために，この機能を実現している。

ICカードではメモリをファイルとして分割管理しており，このファイル分割を利用している。

ファイルは構成・構造上3種類に分かれており，その役割・機能は以下のとおりである。

(1)　MF(Master File：主ファイル)：ICカード内部のすべてのファイルの根幹のファイルで，特別な専用ファイル

(2)　DF(Dedicated File：専用ファイル)：業務アプリケーションなどを意味づけるファイルで，下位に複数の専用ファイルや基礎ファイルを配置できる。



注：略語説明　MF(Master File；主ファイル)
EF(Elementary File；基礎ファイル)
DF(Dedicated File；専用ファイル)

図3　論理ファイルの構成例

ICカード内部の論理ファイルの構成例を示す。このように，ICカードのファイルはシーソー構造で表現される。

(3)　EF(Elementary File：基礎ファイル)：実際にデータを格納するファイル

DFは，ファイルID(Identification)(2バイト)とファイル名称の2種類の方法で管理している。また，EFは，ファイルID(2バイト)で管理している。

ファイルの構造や階層構造について次に示す(**図3**参照)。

EFは，4種類の格納構造・アクセス方法を持っており，その内容は次のようになっており，それぞれ定義されたファイルを業務用途に応じて使い分ける(**図4**参照)。

(1)　透過ファイル：ファイルはデータの連続として表され，ファイルエリア全体をマッピングして直接アクセスで使用する。

(2)　固定長順編成ファイル：ファイルは個々に識別が可能な固定長レコード列で表され，順編成アクセスで使用する。

(3)　可変長順編成ファイル：ファイルは個々に識別が可能な可変長レコード列で表され，順編成アクセスで使用

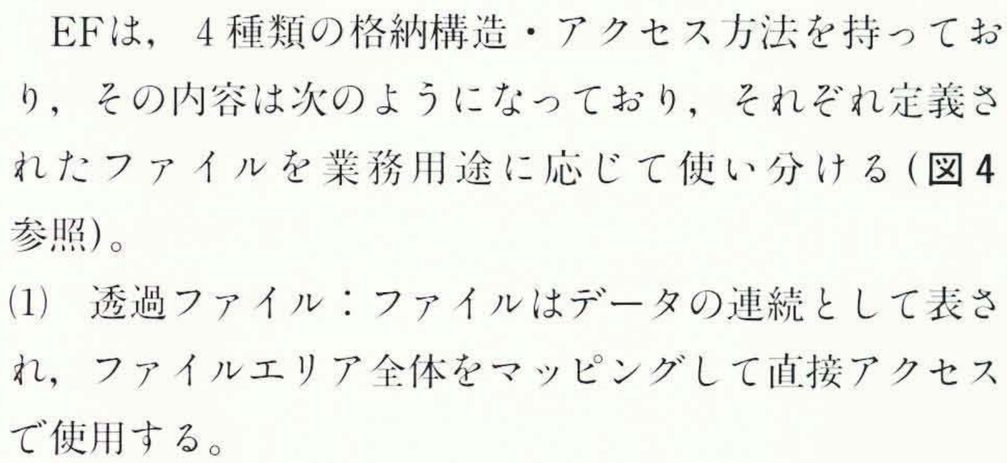


図4　EF(基礎ファイル)の構造

ICカードの基礎ファイルの四つの構造を示す。固定長循環順編成ファイルは，ロギング用ファイルに使うなど，用途別に使用する。

する。

(4)　固定長循環順編成ファイル：ファイルは個々に識別が可能な固定長レコード列で表され，順編成アクセスで使用するが，該当ファイルエリアを循環して使用する。

これらの必要なEFのデータへのアクセスは，MFから始め，上位のDFから順に選択し，目的のEFまで選択する。該当するEFに到達したら，目的のデータのレコード識別子またはファイルの先頭からの位置を指定して，必要なアクセス処理を行う。

この手順の中で用いるDF選択処理は，ファイルIDでもファイル名称でも検索し，該当ファイルを選択できるようにしている。FD名称を目的別・分野別に定義して，ファイル名称による検索選択機能を用いることで，同一ICカードを多目的・多分野で利用することが可能になる。

3.2.2　セキュリティ機能

ICカードのセキュリティレベルを多様に設定する必要のあるアクセスコントロールにも対応できるように，この機能を実現している。

セキュリティに関しては，(1) ICカードがリーダ・ライタを含む端末装置の正当性を認証する機能(外部認証機能)，(2) 逆にリーダ・ライタを含む端末装置がICカードの正当性を認証する機能(内部認証機能)，(3) 格納されているファイル個別にアクセスの正当性(キー)を認証する機能，(4) さらにこれらの認証に用いるキーに重み(ランク)づけを行い，認証の結果に応じてこの重みづけをさらに組み合わせることにより，アクセス権限をチェックする機能をサポートしている。業務に応じてこれらを設定，組み合わせることにより，必要なセキュリティレベルを確保できる。

MFとDFごとにこれらのキーとキーの重みづけ情報を設定することで，セキュリティを持つICカードとして使用することができる。設定内容は利用システムごとに独立したもので，ユーザーが責任をもって運用する必要がある。

4　リーダ・ライタソフトウェア

リーダ・ライタソフトウェアは，パソコン上で密着型非接触ICカードのアプリケーションプログラムを開発するために必要なリーダ・ライタ用ドライバライブラリであり，リーダ・ライタを接続する回線の制御用コマンド，リーダ・ライタを制御するコマンド，リーダ・ライタを介してICカードに対する制御を行うコマンド，および暗号処理制御コマンドで構成する。

ICカードのアプリケーションインタフェースは，ISO仕様などで規定している16進数で定義されるアクセスコマンドやインタフェースフォーマットであるため，プログラミング時に扱いやすい。また，ICカードだけでなく，リーダ・ライタの制御なども含め，関数の統一を図っている。

5　おわりに

ここでは，ICカードの標準化に対応したICカードシステムを支えるソフトウェアについて述べた。

今後，ICカードはネットワークシステムのキーデバイスとしての地位を高め，われわれの社会生活を大きく変える可能性を秘めている。ICカードの普及のために解決すべき課題はまだ多くあるが，さまざまな試みの中で，それはいずれ解決されていくものと考える。

ICカードが，システムに組み込みやすく，より使いやすい，より便利な，より安心なものとして使われるように，また，各業界での利用動向を踏まえ，今後も，ICカードとその支援ソフトウェアの充実を図っていく考えである。

参考文献

1)　International Standard ISO/IEC 7816-4

執筆者紹介

朝倉　久
1974年日立製作所入社，汎用コンピュータ事業部 CARDシステム開発センタ 所属
現在，ICカードシステムの開発に従事
情報処理学会会員
E-mail：hasakura@kanagawa. hitachi. co. jp

稲葉純二
1982年株式会社日立インフォーメションテクノロジー入社，新事業推進本部 カード機器開発プロジェクト 所属
現在，ICカードシステムの開発に従事
E-mail：jinaba@kanagawa. hitachi. co. jp

伊藤　修
1993年株式会社日立インフォーメションテクノロジー入社，新事業推進本部 カード機器開発プロジェクト 所属
現在，ICカードシステムの開発に従事
E-mail：oitoh@kanagawa. hitachi. co. jp