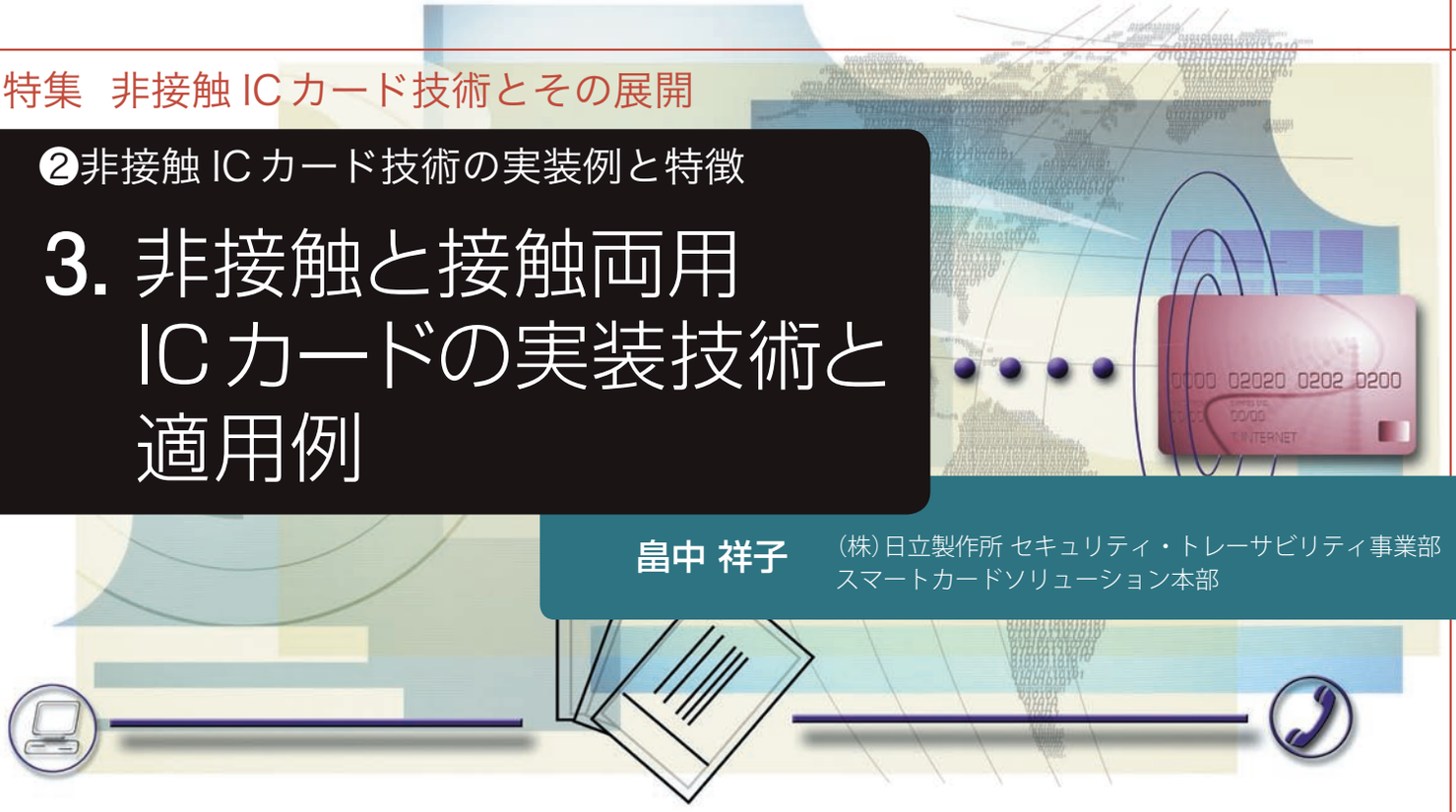
❷非接触 IC カード技術の実装例と特徴

3. 非接触と接触両用 IC カードの実装技術と適用例



畠中 祥子　(株)日立製作所 セキュリティ・トレーサビリティ事業部 スマートカードソリューション本部

IC カードの種類と動向

近年，IC カードは，手軽で便利な IC 乗車券として「Suica」や「PiTaPa」，プリペイド型電子マネーとして「Edy」などが使われており，生活に欠かせないカードとして急速に普及しつつある．国内に出回っている IC カードには，接触式 ISO 7816，非接触式 ISO 14443，ソニー(株)が独自に開発した非接触式 FeliCa の 3 種類がある．この種類は，IC カードと IC リーダ間の通信方式によって分類されている．

接触式 ISO 7816 は，IC リーダに IC カードを差し込み，IC カード表面にある接触端子を介して IC リーダと通信する方式で，この端子から安定した電力供給を受け取ることができる．この特徴から，公開鍵暗号方式 RSA などの強い暗号処理を IC カード内で瞬時に行うことができるため，金融分野を中心に高セキュリティが求められる分野で使われている．

一方，非接触式は，IC カードを IC リーダに差し込むことなく，かざすだけでアンテナを使って瞬時に通信することができる．通信方式には，ISO 14443 方式と FeliCa 方式の 2 方式があり，主に交通分野や流通分野で利用されている．

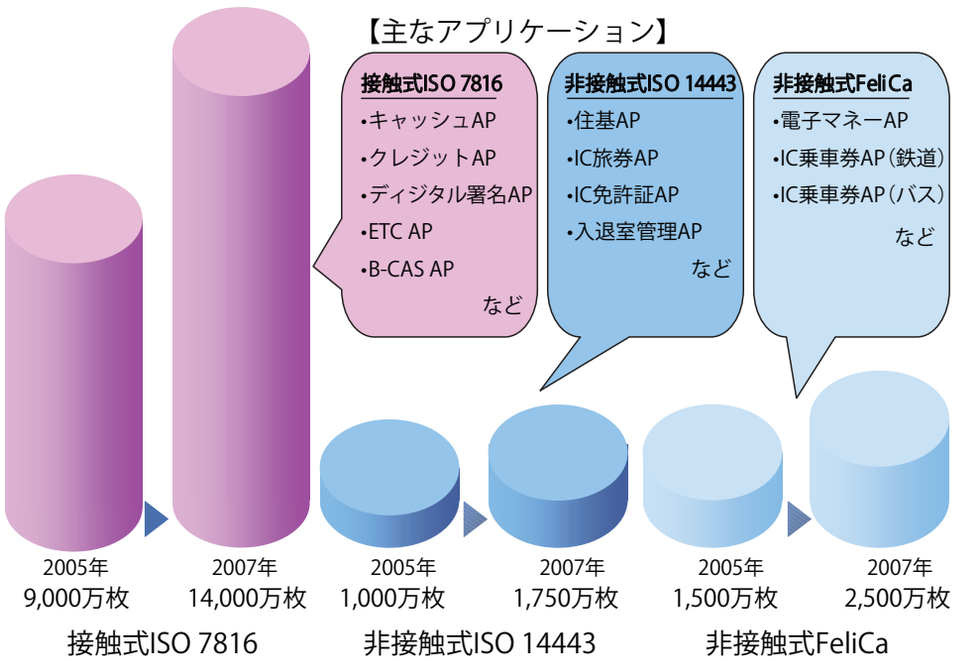
図 -1 に，国内の IC カードの市場規模とアプリケーション (AP) を，上述した 3 つの通信方式別に，2005 年の実績と 2007 年の予想を示す．2005 年は，合計で 1 億 1,500 万枚であり，2007 年には 1 億 8,250 万枚へ約 1.5 倍の増加が見込まれている．内訳は，接触式 ISO 7816 が約 75%，非接触式 ISO 14443 が約 10%，非接触式 FeliCa が約 15% で同じ割合のまま推移し，用途に応じて使い分けが進んでいる．利便性の面から非接触式 IC カードの割合が増加すると思われがちであるが，実はセキュリティの面から，高度な暗号処理も IC カード内で安定して実行できる接触式 IC カードが主流を占めると予想されている．図 -1 の市場規模については，IC カードの市場動向や方向性を調査したレポート [1] を参照した．

IC カードが広がるにつれて，ユーザから複数の IC カードを 1 枚にしたいというリクエストがある．そこで本稿では，接触式と非接触式とを 1 枚で利用するための，ハイブリッド式カードとデュアル式カードについて述べる．

ハイブリッド式カードを実装する技術

たとえば，お財布の中にあるキャッシュカードとクレジットカードを 1 枚にしたいといったリクエストのように，2 枚が同じ接触式 IC カードであれば，1 枚の IC カードで複数の AP を搭載できるマルチ AP 用カードを使うことで解決できる．この IC カードは，オペレーティングシステム (OS) を持っていて，同じ IC カード上に複数の AP を搭載しても，AP 同士が干渉し合わないようなファイアウォール機能を保有している．また，IC カード発行後にも新しい AP を追加や削除する機能を保有している IC カードもある．

ところが，接触式と非接触式の IC カードを 1 枚にする場合には，接触式 IC チップと非接触式 IC チップの 2 つの IC チップを 1 枚の IC カードに埋め込む必要がある．このような IC カードが「ハイブリッド式カード」と呼ばれ，接触式 IC チップには，PC ログイン用のディジタル署名 AP など，非接触式 IC チップにはアクセスコントロール用の入退室管理 AP などが搭載され，主に社員証として使われている．



●図 -1　IC カードの通信方式別市場規模

デュアル式カードが開発された背景

上述のハイブリッド式カードは，接触用 IC リーダからも非接触用 IC リーダからも 1 枚の IC カードへアクセスできるが，IC チップが物理的に 2 つに分かれているために，IC チップ間でデータを共有することができない．つまり，IC カードは 1 枚になっても，1 つの AP を接触用 IC リーダと非接触用 IC リーダの両方からアクセスすることができない．これを可能にするために，1 つの IC チップで，接触式と非接触式の 2 つの通信方式を持つデュアル式カードが必要とされる．

ハイブリッド式カードとデュアル式カードの違いを，電子マネーのチャージを例に説明する．

店舗で，小銭を使わずに便利な支払いができる電子マネーであるが，その残高が不足したときに，いかに簡単にチャージできるかという点でさまざまなアイディアが工夫されている．店舗で現金と引き換えたり，インターネットを使ってクレジット決済で購入したり，そして最近注目されているのが，ATM で銀行口座から預金を引き出すと同時にチャージする方法である．ATM を利用する方法は，IC カードの AP として，接触式 IC チップ上にキャッシュ AP，非接触式 IC チップ上に電子マネー AP の 2 つを使用する．

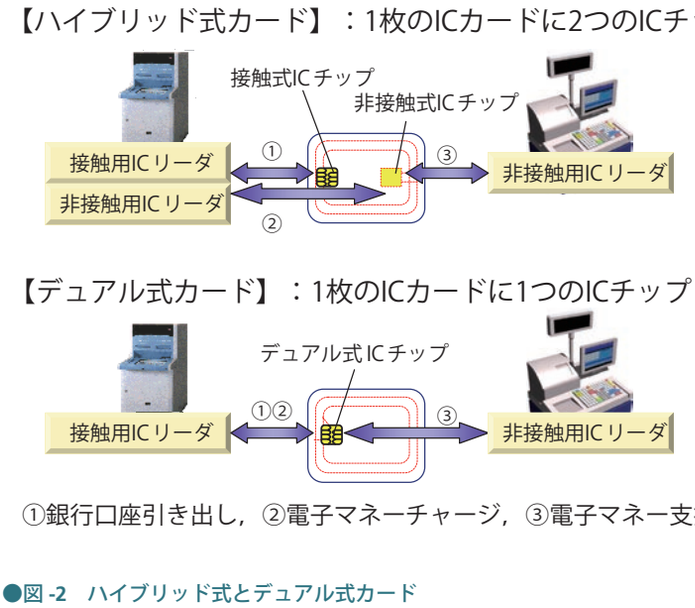
図 -2 に，ハイブリッド式カードとデュアル式カードの実現方法の違いを示す．ハイブリッド式カードでは，2 つの IC チップが分離していて，データを共有できないため，ATM の接触用 IC リーダから，接触式 IC チップ上のキャッシュ AP にアクセスし，取引に必要な認証処理などを行い，チャージする金額を銀行口座にある残高から差し引いた後，接触用 IC リーダから非接触用 IC リーダへ切り替えて，非接触用 IC リーダから非接触式 IC チップ上の電子マネー AP にアクセスして電子マネーをチャージする必要がある．

これに対して，デュアル式カードでは，接触用 IC リーダから，デュアル式 IC チップ上のキャッシュ AP にアクセスした後，そのままデュアル式 IC チップ上の電子マネー AP にアクセスしてチャージすることができる．デュアル式カードを使うと，銀行口座引き出しと電子マネーチャージの 2 つの処理を，1 つの処理フローで完結して実行し，途中で IC カードがすり変えられるなどのトラブル発生を未然に防ぐことができる．また，ATM の IC リーダを 1 つにすることでコスト低減のメリットが見込まれている．

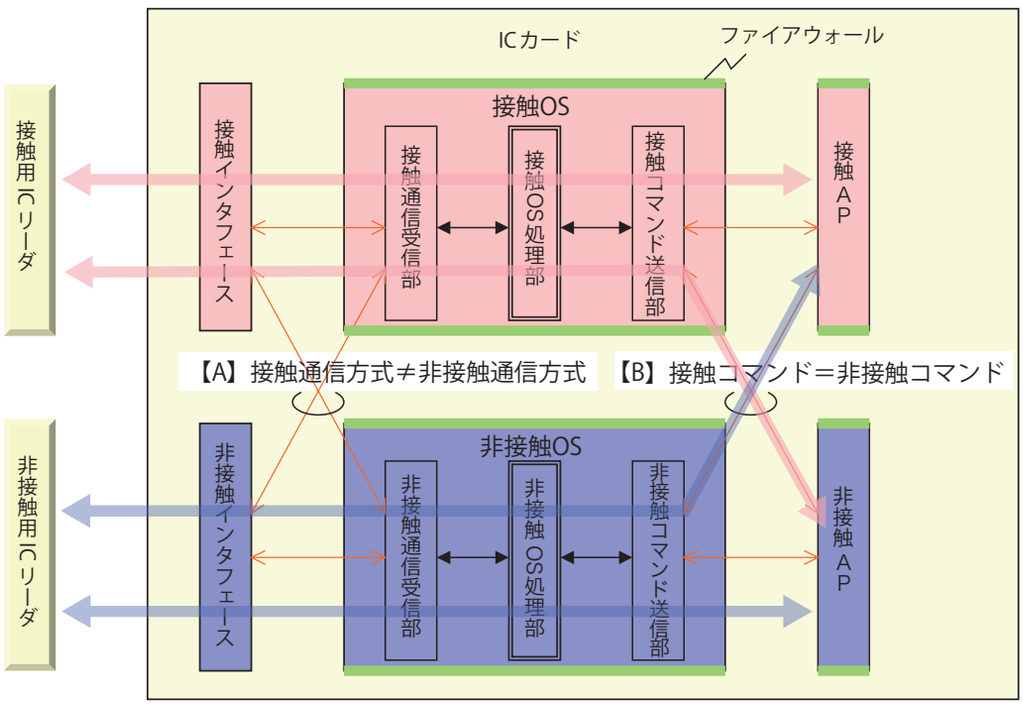
デュアル式カードを実装する技術

●デュアル式カードの前提条件

デュアル式カードの実装について，マルチ AP 用カードの代表的な例として MULTOS を用いて述べる．デュアル式カードとは，1 つのデュアル式 IC チップ上に，



●図 -2　ハイブリッド式とデュアル式カード



●図 -3　ISO 14443 × ISO 7816 のデュアル実装方法

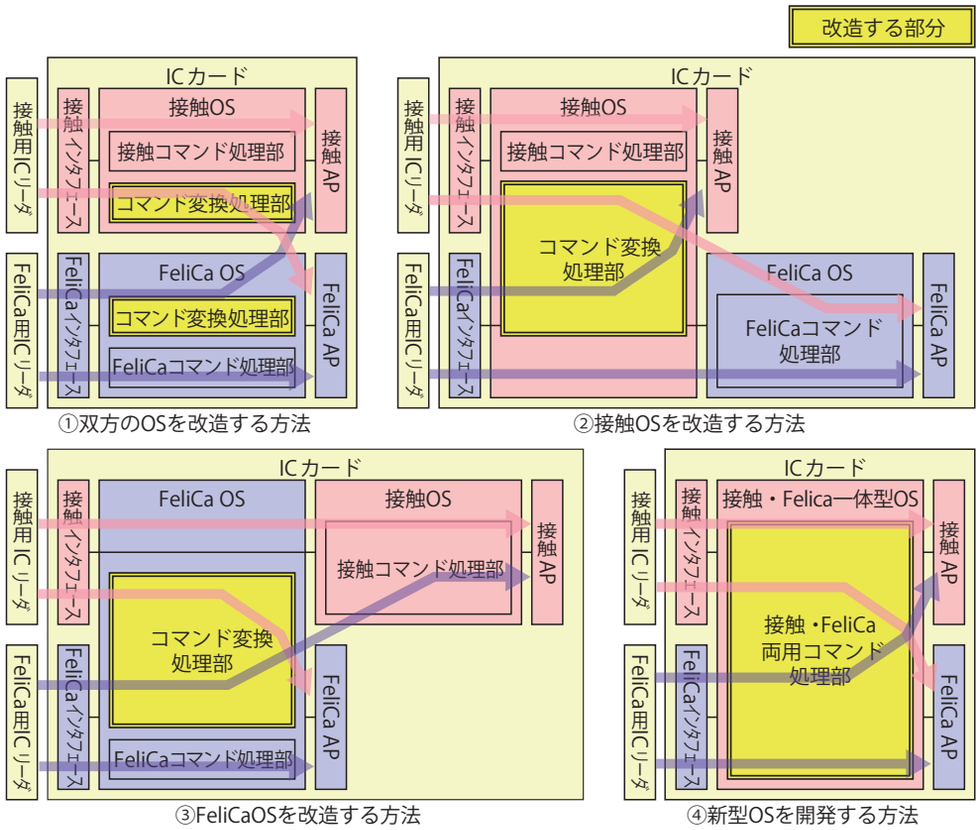
接触式と非接触式の 2 つの通信方式を実装し，接触用 IC リーダと非接触用 IC リーダのどちらからも同一 AP にアクセスできる IC カードである．

このとき，まず，接触用 IC リーダから非接触 AP へ，非接触用 IC リーダから接触 AP へ，どのようにクロスアクセスするかが課題となる．次に，AP やデータのセキュリティのレベルを下げずに，どのようにしてアクセスする通信の数を 1 つから 2 つへ増やすかが技術的な課題となる．

非接触式 IC カードの通信方式は，ISO 14443 方式と FeliCa 方式の 2 方式があるため，それぞれを接触式 IC カードと両用にする実装技術について述べる．

●非接触式 ISO 14443[2] と接触式 ISO 7816[3] の実装例

IC カードの構造は，図 -3 に示すように，IC カードを処理させるための命令（コマンド）やデータを，IC リーダから入出力するインタフェース層，入力したコマンド



●図 -4　FeliCa × ISO 7816 のデュアル実装方法

やデータを処理するための IC カードのハードウェアやメモリを管理する OS 層，OS 上で具体的な機能を実行する AP 層の 3 つの層に分けられる．

この層のうち，IC カードのセキュリティを守るファイアウォールは，OS 層と AP 層によって構築されている．このため，クロスアクセスを実装するときに，この 2 つの層に改造を加えないことが望ましい．

層と層の切れ間でクロスアクセスを実装するということは，【A】インタフェース層と OS 層の間でクロスアクセスする方法と，【B】OS 層と AP 層の間でクロスアクセスする方法，の 2 通りがある．【A】は，各通信方式を双方の OS で受け取れるようにする方法であるが，ISO 14443 と ISO 7816 とで通信方式が異なっているため実現できない．【B】は，各 OS からのコマンドを双方の AP で受け取れるようにする方法であるが，ISO 14443 と ISO 7816 とでコマンドを共通利用できるため実現可能である．

補足すると，接触式 ISO 7816 を定義している規格は，Part1 ～ 3 で IC カードのサイズ・接点の位置などの物理的特性から伝送プロトコルまでを規定し，Part4 以降でコマンド仕様を規定している．非接触式 ISO 14443 の規格は，Part1 ～ 4 で物理的特性，電波の周波数・アンチコリジョン方法から伝送プロトコルまでを規定し，コマンドは ISO 7816 の Part4 以降を参照する流れとなっている．このように，接触式と非接触式とで，物理的特性や伝送プロトコルはハードウェア的にも異なるが，上位は同じコマンド処理となっている．

またこの方法は，OS 層や AP 層に改造を加えないため，設計がシンプルで開発にかかる工数が少ないだけでなく，OS 層と AP 層に実装されたファイアウォールをそのまま利用できるため，セキュリティレベルを保持できるという点で大きなメリットがある．

この方法は，すでに MULTOS で製品化されており，主に，台湾のキャッシュ AP と IC 乗車券 AP で広く利用されている．

●非接触式 FeliCa[4]と接触式 ISO 7816 の実装例

非接触式 FeliCa と ISO 7816 でクロスアクセスを実装するには，双方で通信方式が異なっていることと，コマンドを共通利用できないことから，【A】方法も【B】方法も実現できない．このため，OS 層に接触コマンドと FeliCa コマンドを変換するコマンド変換処理部を実装する必要がある．図 -4 に，コマンド変換処理部を実装する 4 つのパターンを示す．

方法	セキュリティ面		処理速度面		改造面	
	接触 AP	FeliCaAP	接触 AP	FeliCaAP	接触 OS	FeliCaOS
①双方改造	△ 2 つの OS で低い方	△ 2 つの OS で低い方	○ 1 つの OS 処理にかかる	○ 1 つの OS 処理にかかる	△ 改造あり	△ 改造あり
②接触改造	○ 1 つの OS に依存	△ 2 つの OS で低い方	○ 1 つの OS 処理にかかる	× 2 つの OS 処理にかかる	△ 改造あり	○ 改造なし
③ FeliCa 改造	△ 2 つの OS で低い方	○ 1 つの OS に依存	× 2 つの OS 処理にかかる	○ 1 つの OS 処理にかかる	○ 改造なし	△ 改造あり
④新型開発	○ 1 つの OS に依存	○ 1 つの OS に依存	○ 1 つの OS 処理にかかる	○ 1 つの OS 処理にかかる	× 新規開発	× 新規開発

●表 -5　FeliCa とのデュアル実装方法の比較

①双方の OS を改造する方法

この方法は，双方の OS にそれぞれクロスアクセスするためのコマンド変換処理部を実装する方法である．接触 AP へのアクセスは，接触 OS を通る場合と FeliCaOS を通る場合との 2 通りある．したがって，接触 AP を守るセキュリティレベルは，2 つの OS のどちらか低い方のレベルに準拠することとなる．FeliCaAP へのアクセスも同様に 2 通りある．このため，そのセキュリティレベルも同様に 2 つのうち低い方の OS に準拠する．

②接触 OS を改造する方法

この方法は，接触 OS のみで接触コマンドと FeliCa コマンドとを変換する方法である．接触 AP を守るセキュリティは，接触 OS のレベルが保持されるが，FeliCaAP のセキュリティは，接触 OS か FeliCaOS のどちらか低い方となる．

③ FeliCaOS を改造する方法

この方法は，FeliCaOS のみで接触コマンドと FeliCa コマンドとを変換する方法である．上述の②とは逆に，FeliCaAP を守るセキュリティは，FeliCaOS のレベルが保持されるが，接触 AP のセキュリティは，接触 OS か FeliCaOS のどちらか低い方となる．

④新型 OS を開発する方法

この方法は，接触コマンドも FeliCa コマンドも処理できる新型 OS を開発する方法である．このときのセキュリティレベルは，接触 AP，FeliCaAP ともに，新型 OS が実装するレベルとなる．

表 -5 に，①～④の 4 つの方法について，セキュリティ面，処理速度面，改造面から見た評価を示す．

接触 AP に着目すると，セキュリティ面および処理速度面で，接触式単体のときと同等レベルを保持できる方法②が最も適している．FeliCaAP に着目すると，逆に，セキュリティ面および処理速度面で，非接触式 FeliCa 単体の時と同等レベルを保持できる方法③が最も適している．接触 AP と FeliCaAP の両方のバランスをみると，方法①と方法④が候補となる．現在，市場に出回っている接触式単体の IC カードおよび非接触式 FeliCa 単体の IC カードと同等レベルかそれ以上のセキュリティおよび処理速度のサービスを提供するには，接触 OS と FeliCaOS を併せ持つ，新たな OS が開発される方法④が期待される．

サービス例

接触式と非接触式の 2 つの通信方式を持つデュアル式カードを使っている例として，住民基本台帳 IC カードと小額決済機能付き IC クレジットカード，最新の動向として生体認証用 IC カードについて簡単に紹介する．

●住民基本台帳 IC カード

住民基本台帳 IC カードは，全国の市町村を結ぶ住民基本台帳ネットワークシステムを利用するための IC カードで，主に公的個人認証を処理している．公的個人認証では，政府系サービスとして高いセキュリティを守るために，接触式 IC カードを使って高度な暗号処理を行っている．

また，この IC カードは，各種申請用 AP や図書館利用 AP など各自治体が独自に AP を追加（削除）すること

も可能であり，利便性が必要なサービスでは，非接触式 ISO 14443 から各種 AP へアクセスされている．

●小額決済機能付き IC クレジットカード

小額決済機能付き IC クレジットカードは，これまでのクレジット決済に加えて，主に現金が使われている小額の決済もサービスできる IC カードである．

クレジット決済は，消費者が実際に支払うタイミングが取引の後となる後払いの決済であり，そのセキュリティを守るために，接触式 IC カードを使って高度な暗号処理を行っている．小額決済では，利便性を考慮して，取引金額を制限することで，非接触式 IC カードでのサービスが開始されている．

現在利用されている IC クレジットカードには，クレジット決済用の接触式 IC カード，小額決済用の非接触式 IC カード，2 つのサービスを 1 枚で実現するハイブリッド式カードに加えて，2 つのサービスを 1 つの IC チップで実現するデュアル式カードも登場している．

●生体(指静脈)認証用 IC カード

IC キャッシュカードと一体となっている生体（指静脈）認証用 IC カードは，金融機関の ATM で 4 桁パスワードによる本人認証を強化するための生体認証 AP を搭載した IC キャッシュカードである．ATM には，IC カード上のキャッシュ AP を利用するために，接触用 IC リーダが取り付けられている．生体認証 AP は，キャッシュ AP と組み合わせて利用されているので，同じ接触用 IC リーダからアクセスできるように接触式 IC チップ上に搭載されている．

生体認証用 IC カードが広がるにつれ，生体認証 AP を，非接触式 IC チップ上の貸し金庫管理 AP や入退室管理 AP と組み合わせて利用したいというリクエストがある．利用される環境に応じて，接触用 IC リーダと非接触用 IC リーダのどちらからもアクセスできるように，生体認証 AP をデュアル式 IC チップ上で実現している．

今後の展望

冒頭で述べたように，強い暗号処理を IC カード内で高速かつ安定して行うことが必要であり，その結果として接触式 IC カードが主流となっている．しかしながら，利便性の面から，ハイブリッド式やデュアル式など非接触式の市場が伸びてくると予想される．近い将来には，IC チップの低電力消費化など技術開発が進み，非接触式 IC カードの割合が増加していくだろう．

参考文献

1) (株) 富士キメラ総研，カード市場マーケティング要覧 2006 年版．
2) ISO/IEC 7816 (all parts)，Identification Cards ― Integrated Circuit(s) Cards with Contacts.
3) ISO/IEC 14443 (all parts)，Identification Cards ― Contactless Integrated circuit(s) Cards ― Proximity Cards.
4) モバイル FeliCa プログラミング，(株)アスキー．

（平成 19 年 5 月 7 日受付）

畠中 祥子　shoko.hatanaka.rx@hitachi.com

(株) 日立製作所セキュリティ・トレーサビリティ事業部所属．1989 年同社入社，1997 年より IC カードを利用するシステムのビジネスに従事．