技術基礎講座
【非接触ICカード技術】

ICカードは認証や決済を伴う権利行使の手段として広く使用されるようになりました．その中で非接触ICカードは多くの優れた特徴を持ち，普及が進んでいます．本講座では5回にわたり非接触ICカードの技術的な側面を中心に解説します．第1回目は非接触ICカードの総論として，その特徴，機能と市場の動向について説明します．

非接触ICカードとは

非接触ICカードとは電気的な接点を持たず，電磁波を用いてデータの読み書きを行うチップ付きカード全般を指します[(1)～(4)]．RFID（いわゆる無線タグ）とはかなり混用されていますが，ここではISO/IEC14443で規定されている近距離の通信機能，およびセキュリティ機能を併せ持つ，近接型カードに絞って説明します．一般的な非接触ICカードの機能構成を**図1**に示します．

非接触ICカードの特徴

■非接触ICカードが持つ長所

① カードサイズはISO/IEC7810で規定されている85.6×54.0×0.76 mmの大きさ（ID-1）におおむね準拠しています．このサイズは持ち運びやいろいろなサービスを受ける際の提示に便利な大きさです．また，このサイズはプラスチックや磁気のカードとしてICカードが広がるずっと前から広く使われていました．広く使われている規格のため，このサイズに合わせて安心して機器やサービスを開発できるというメリットもあります[(5)，(6)]．

② 非接触ICカードはリーダライタ（読み書き用の装置）に対してかざす，もしくは置くことにより動作します．そのため，接触ICカードのようにユーザがいちいちケースから取り出して挿入する必要がなく，所有者が立ち止まらずに高速で動作させることが可能です．

③ 現在主流の近接型カードは通信，電力供給に使う

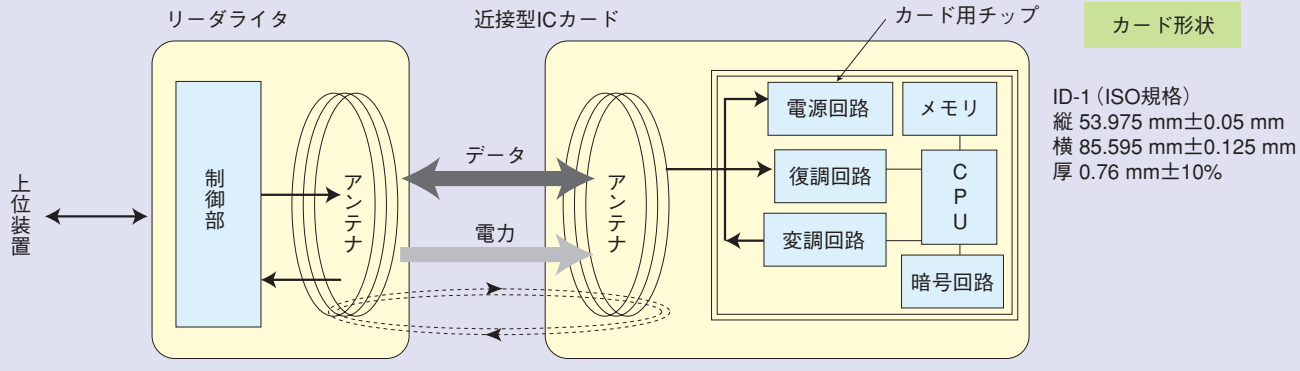

図1　一般的な非接触ICカードシステムの機能構成

電磁波の帯域として13.56 MHz帯（HF帯）を用いており，1～10 cm程度の距離でリーダライタと通信します．この帯域を使うことでID-1の形状にアンテナを埋め込み，電力供給を行うことが可能になります．また，カードとリーダライタの通信距離は長すぎても，短すぎても使い勝手に影響します．使用者がかざす・置くという使い方を前提にした場合，1～10 cmは，適切な通信距離です．

④　接点を持たないため，リーダライタと擦れることがなく，表面の磨耗が生じにくいため，カードが長持ちします．またリーダライタ側も磨耗に起因するメンテナンスが不必要になるなど，コストを抑えることができます．

⑤　電池を内蔵しておらず，電磁波により電力を供給するためリーダライタさえあれば動作します．電池を内蔵しているカードでは，安定した電力供給ができる反面，電池切れの心配が常にあり、その対策が必要になります．

■短所とその対処法

⑴　通信に電磁波を用いるため，盗聴されるリスクがある

これに対してはカードとリーダライタ間で，通信開始時の認証や，セキュリティ上重要な情報の暗号化を行うことにより対処できます．また，接触ICカードを使ってもケーブルに機器をはさんで情報を盗むワイヤータッピングなどのリスクはあるため，非接触ICカードのセキュリティが接触に比べ劣るという説は正しくありません．

⑵　カードとの通信の途中に電源が切れる（電源断）ことによるカードの内部状態の異常や破損をきたす恐れがある

これは必ず起こり得るため，次の機能の導入が必要です．

・トランザクション処理機能：ICカード内のある処理（トランザクション）は，完全に終了するか，全く痕跡を残さないか，のどちらかになること（アトミシティ）を保障する機能

・ハードウェア診断機能：電源断によるメモリ不整合やその他のハードウェアの問題がないかを診断し，回復する機能

これらの機能を確実に実装すれば，通常の使い方で大きな問題が起きることはありません．

⑶　カードやリーダライタのコストが高い

通信用のアンテナや回路を組み込むことで，接触型ICカードに比べて製造コストが若干上昇しますが，生産数量が増加すれば接触型とのコストの差は小さくなります．

ただし，接触型ICカード用リーダライタなどのカードインフラがすでにかなり普及しており，それを活用することがカード利用者の利便性を高めることにつながります．そのため，接触通信用の端子と，非接触通信用のアンテナの両方を持ったコンビネーション型（コンビ型）のICカードもかなり広く使われるようになっています．

非接触ICカードの機能

一般にセキュリティシステムには次の3つの機能が存在します[(7)]．これらの観点でICカード（非接触・接触を問わず）の機能を分類することができます．

⑴　識別（Identification）

識別とは，カード所有者があるカテゴリに属している（ある社の社員であるなど）ことを区別することです．

識別は，①カードの所持や，それに加えてカード券面に刷ってある写真等の情報を人間が確認する，②カードのチップに格納されているID情報をシステムが読み出し確認する，のいずれかが普通使われます．これはもっとも簡単に実現できますが，これだけでは拾ったカードや券面を偽装したカードを使用されるリスクを防げません．

⑵　認証（Authentication）

認証は，あるサービスに対して，それを受ける正当性（legitimacy）があることの証明を行うことです．ICカードを使った認証は次の3種類が存在します．それぞれの流れを**図2**に示します．

①　本人認証（Personal Authentication）：カードを使って権利行使を行おうとする人が正当な所有者

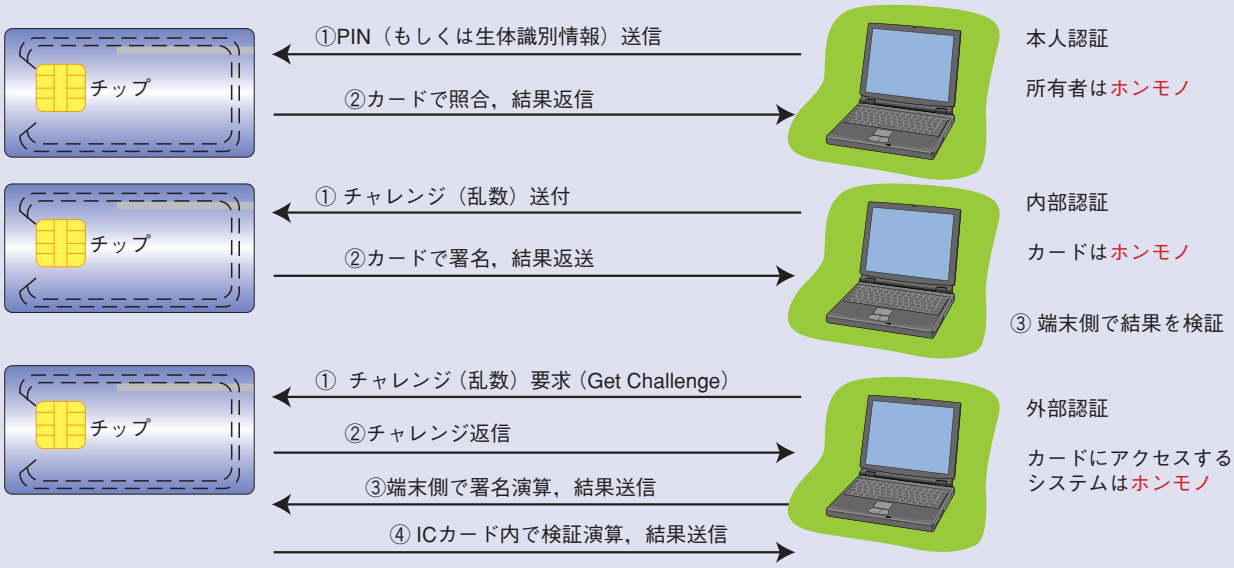

図2　ICカードにおける認証の一般的な流れ

である（その人に対して発行されたカードである）ことを認証します．今でももっとも広く使われている手段は個人識別番号（PIN: Personal Identification Number）をその人に入力させることです．ただし，PINの欠陥（忘れる，盗まれる）もよく知られており，指紋，虹彩などの生体識別情報（Biometrics）を用いた認証はすでに実用化されています．現在はカードから生体識別情報を取り出して認証する方式（Store On Card）が広く使われていますが，より安全にカードから情報を取り出さずカード内で認証演算まで行うOn Card Matchingもすでに実用化されています[8]．

② 内部認証（Internal Authentication）：カードが正当なものである（偽造された，盗まれたものでない）ことを認証する行為です．現在，規格となっている方式はカードに対して外部から乱数を送ってカードで暗号演算を施し，その結果を外部で検証を行うチャレンジレスポンス方式です．使用する暗号演算は公開鍵暗号，共通鍵暗号のいずれでも可能ですが，公開鍵暗号のほうがカード外部で秘密鍵を管理する必要がなく，高いセキュリティを確保することが容易にできます．

③ 外部認証（External Authentication）：内部認証とは逆に，カードにアクセスする装置（システム）が正当なものである（偽装されたものでない）ことを認証します．カードで発生した乱数を外部で暗号演算し，それをカードで検証する方式が規格で定められています．

これら3種類の認証をすべて行えばもっともセキュリティ強度を高めることができます．ただし，例えば通常の入退出管理システムでその都度本人認証を行うと処理時間が増し，著しく処理能力が低下するため，コンピュータルームのような特定の場所を除き，省略することが普通です．この場合においても，カードから読み出せるIDによる識別だけでは偽造カードに対する対策がないため，内部認証のみ実施することは広く行われています．

⑶　許可（Authorization）

許可とは，認証がなされたカード所有者に対して，規定された範囲のサービスを提供することを認めることです．カードを使ったサービスとしては，例えば次のものがあります．

・カードに格納されている電子マネーを用いて支払いを行う．支払った額だけカード内の残高を減らす．
・カードに格納されているID，パスワードを読み出してシステムにログインする．
・カードに格納されている暗号鍵を用いて外部から送られてきた電子署名を検証する．
・カードに格納されている個人情報（例えば健康情報）を読み出す．
・カードでセッションごとに使い捨てにする暗号鍵（セッション鍵）を生成する．

ICカードには耐タンパ性が高い（内部のデータの不正な読出し，改ざんが困難）[9] という特長があるため，ここで述べたようなセキュリティを必要とするサービス提供には最適なデバイスであるということがいえます．

非接触ICカードの市場動向

現在，非接触カードはIDカードや交通系が主な適用先です．2007年の時点では，発行されているカードのうちで接触カードが6割以上を占めています[10]．これは現在もっとも発行枚数が多い金融カード（ICキャッシュカード，ICクレジットカード）がほとんど接触型ICカードであることが最大の理由です．そのほかにも携帯電話に内蔵されるSIMカードや高速道路での支払いに使われるETCカードなど，接触ICカードを使っている分野は多くあります．ただし，銀行が非接触電子マネー一体型のコンビ型カードの発行を開始する，クレジットカード会社が非接触電子マネーを国内外で開始するなど，金融分野でも非接触化の流れが定着しつつあります[3]．

この結果，今後は急速に非接触ICカードの枚数が増加すると予想されます．また，これまで金融，交通などの分野に比べてICカードそのものの普及が遅れていた公共分野でもe-パスポートやIC免許証の発行開始，公的個人認証サービスを利用した電子申告・電子納税の推進，たばこ自販機用の成人認証カードの導入決定，さらには社会保障カードの実現に向けた検討など話題が目白押しで非接触ICカードの普及を牽引すると予想されます．これら公共分野ではISO/IEC14443タイプBのカードが主に使われています．

なお，ISO14443の中の各方式の違いについては，第3回で説明します．

■参考文献

⑴ 大谷・永井：“コンタクトレスICカードの国際標準化，”NTT技術ジャーナル，Vol.14, No.7, pp.75-76，2002.
⑵ 技術基礎講座：“ICカード技術　第1回　ICカードの特徴，”NTT技術ジャーナル, Vol.17, No.2, pp.62-63, 2005.
⑶ “ICカード総覧2007～2008，”シーメディア, 2007.9.
⑷ http: //www.safety-pass.com/business/service/elwise.html
⑸ 山本・細田：“ICカード情報流通プラットフォーム，”電気通信協会，2001.5.
⑹ 細田：“タイプBカード，”COMPUTER & NETWORK LAN, Vol.22, No.6, 2004.
⑺ シュナイアー：“セキュリティはなぜ破られたか，”日経BP社, 2007.2.
⑻ http://www.ntt.com/release/2006NEWS/0010/1016_2.html
⑼ 細田・中濱：“セキュアなストレージとしてのICカードとその応用，”信学誌, Vol.89, No.11, 2006.
⑽ “カード市場マーケティング要覧2007年度版，”富士キメラ総研, 2007.8.

◆問い合わせ先
NTTサービスインテグレーション基盤研究所
ICカードサービス推進プロジェクト
E-mail　sd-info@lab.ntt.co.jp