リテール・バンキング・システムのICカード対応に関する現状とその課題

田村裕子（たむらゆうこ）／廣川勝久（ひろかわかつひさ）

要　旨

磁気ストライプを貼付したキャッシュカードが偽造され、不正に預金が引き出される事件が社会問題化したことを受けて、わが国の金融機関では、キャッシュカードの偽造を未然に防止するためにICカード化を進めることを表明した。しかしながら、現時点ではICキャッシュカードの発行枚数は微々たるものにとどまっているのが実情であり、偽造カード犯罪の未然防止対策として有効に機能しているとはいえない。今後、ICカードの導入によりセキュリティの向上を進めていくうえでは、業界内でのATMオンライン提携を前提とすれば、業界が一丸となって推進することが望ましいと考えられる。ただし、ICカードへの移行のあり方によっては、システムの安全性が期待通りに向上しないケースがあることから、事前に金融業界内で十分な検討を行うことが必要と考えられる。

本稿では、キャッシュカードとしてICカードを利用することによって、ATM等を利用したリテール・バンキング・システムの安全性がどのように向上するかについて整理するとともに、ICカードに対応したシステムへの移行のあり方について検討を行う。

キーワード：ICカード、リテール・バンキング・システム、カード所持者認証、ICカード認証、フルICカード対応

本稿は、2007年3月6日に日本銀行で開催された「第9回情報セキュリティ・シンポジウム」への提出論文に加筆・修正を施したものである。なお、本稿に示されている意見は、筆者たち個人に属し、日本銀行の公式見解を示すものではない。また、ありうべき誤りはすべて筆者たち個人に属する。

田村裕子　日本銀行金融研究所（E-mail: yuuko.tamura@boj.or.jp）
廣川勝久　日本銀行金融研究所（E-mail: hirokawa@imes.boj.or.jp）

1．はじめに

磁気ストライプを貼付したキャッシュカードの偽造による不正預金引出しが社会問題化したことを受けて、2005年1月には、銀行業界として、偽造キャッシュカード問題に関する対策についての取り組みを強化することを申し合わせるとともに、キャッシュカードの偽造防止技術の1つとしてICカードを導入することを表明した（全国銀行協会［2005］）。しかし、2005年12月末時点の調査では、発行されたすべてのキャッシュカードにおけるICカードの比率は1.2%であり（金融庁［2006］）、その後顕著に発行枚数が増加しているという様子もないことから、磁気ストライプ・カード（以下、MSカード）からICカードへの切り替えはあまり進んでいないのが実態のようである。金融機関の偽造カード対策としては、キャッシュカードのICカード化よりも、預金引出限度額の引下げと異常取引の検知といった運用による対策が中心となっているといえる。しかし、こうした対応は偽造カードの不正使用による被害額を限定するという考え方に基づくものであることから、偽造カード問題に対する最終的な到達点とは考えにくく、ICカード化の推進等によってセキュリティ対策を抜本的に向上していくことが必要であるとの主張もある（岩下［2006］）。

わが国のクレジット業界は、2005年度には約半数のクレジットカードをICカード化し、さらに2007年度には全体の約70%をICカード化するとの市場規模予測を発表している（日本クレジットカード協会［2004］）。クレジット業界においてICカード化が着実に進んでいる理由としては、まず、カードの有効期限の存在が挙げられる。クレジットカード発行機関は、有効期限満了に伴うカード更新の際にICカードへの切り替えを進めることが可能である。これに対し、銀行業界では、MSカードに有効期限を設定していないことから、ほとんどの銀行は、顧客がICカードへの移行を希望した場合にのみキャッシュカードのICカード化を行っている。さらに、クレジット業界ではICカード発行に伴う費用をカード所持者に負担させることがないのに対し、銀行業界では預金者にICカード発行の手数料を負担させるケースが多いことも、銀行での発行枚数が低迷している理由の1つとして挙げられる。ICカードの発行に伴う費用については、大手銀行では1行当たり約50～90億円、地方銀行でも数十億円との見積もり[1]もあり（安岡・平塚［2005］）、莫大な費用が必要であると想定されるが、今後、費用の分担をどのように行うかが重要な論点となっている。

こうした状況のもと、キャッシュカードとして現在発行されているほとんどのICカードは、利便性と互換性の観点から、ICカードの処理が実行できない端末においても利用できるよう、従来と同様の磁気ストライプも貼付されている。その

1 ただし、ここでの見積もりは、ICキャッシュカードの発行とATMの改修にかかる費用のみであり、ネットワークやホスト・システムの改修については積算されていない。

ため、提携先のATMであっても、ICカードによる処理が実行可能な端末を利用した場合には、ICカードと端末間においてはIC機能を利用した取引を行うことが可能である。しかし、ATMからホスト・システムへの電文がMSカードを利用したときと同一である場合、ホスト・システムはICカードとMSカードのどちらが利用されたかを区別できないため、引き続き磁気データをコピーした偽造カードが利用可能となり、ICカードの機能が享受できない。

さらに、従来のリテール・バンキング・システムは、自行の管理下、あるいは、業界内に閉じた環境で運用されていたことから、設備や運用での安全対策により、システム全体としてある程度の安全性を確保してきた。しかし、今後、ICカードを利用してデビットカード業務等、リテール・バンキングのサービス範囲を拡大していくことを想定するのであれば、自行の管理下にない環境に設置された端末やオープンなネットワークを利用することになるため、従来のシステムでは想定されなかった脅威が顕現化することが考えられる。この場合、運用による対策では十分ではなく、仮にICカードとホスト・システム間に存在する端末やネットワーク上において不正が行われた場合においても、自行が発行したICカードと自行のホスト・システム間での取引が安全に実行可能となる技術面での対策について検討しておくことが重要となる。業界内でのATMオンライン提携を前提とすれば、業界が一丸となってICカードの導入を推進していくとともに、リテール・バンキング・サービス業務の拡大を前提としたシステムの安全性確保について検討していくことが望ましいと考えられる。

全国銀行協会は、キャッシュカードのICカード化、および、端末のICカード対応に加えて、全金融機関のホスト・システム、および、端末とホスト・システム間のネットワークを2010年度末までにICカードに対応できるよう改修することが望ましいとしている（内田［2006］）。しかし、現状を鑑みれば、当該期限までにすべての金融機関のホスト・システム、および、ネットワークを一斉にICカード対応させるといったシステム・マイグレーションの実現は困難と考えられることから、今後、どのようなタイムスパンでシステムを移行させていくべきか、改めて金融業界内で検討していくことが必要であろう。

本稿では、キャッシュカードのICカード化によって、リテール・バンキングの安全性がどのように向上するかについて整理するとともに、そうしたシステムへの移行のあり方について検討を行う。まず、2節ではICカードを利用したリテール・バンキングとその業務を取り巻く環境について紹介する。3節では、ICカードを利用するシステム全体のセキュリティを考えるうえで、ICカードの能力を十分に発揮できるシステム設計のあり方について検討を行う。4節では、システム全体としてICカード対応するためのアプローチとICカード対応に伴う課題について検討する。5節では、以上の検討結果を整理して本稿を締めくくる。

2．ICカードを利用したアプリケーション

(1) キャッシュカードのICカード化

キャッシュカードは、顧客の預金口座を一意に特定するための情報（口座番号等）を提示するデータ・キャリアとしての機能を有している。従来は、MSキャッシュカードについても、カードの偽造が困難であると考えられていたことから、運用上適切に管理されている限りにおいて、キャッシュカードを提示するユーザは当該カードに対応するユーザ本人であるとする本人認証のセキュリティ・トークンとして使用されてきた。しかしながら、磁気ストライプに記録される情報の読取りや書込みが可能な装置が比較的容易に入手できるようになり、ATM等の端末に真正であると誤認させるカードの偽造が容易になったことから、MSキャッシュカードをセキュリティ・トークンとしては利用できなくなってきている。こうした問題に対して、偽造が困難であるといわれるICカード[2]が対策の一環として挙げられた。

ICカードについても、ICに書き込むべきデータが入手できた場合、専用装置を有する攻撃者であればICカードの偽造が可能であると考えられる。ICカードが偽造への耐性を有するとは、ICの製造が困難であることを指すのではなく、ICカードがその演算・判断・記憶の機能を活用することで内部データへの不正なアクセスを防止するとともに、システム全体のリスク管理にかかわる機能を分担できるデバイスであることを意味する。そのため、ICカードを導入することでシステムの安全性を向上させるためには、ICカードをシステムのセキュリティ機能の一端を担うものとして、その機能を十分に活用することができるようなシステム設計が必要となる。

(2) ICカードを利用したリテール・バンキング

金融機関が提供するリテール・バンキングにはさまざまな業務があり、その代表的なものとしては、以下のキャッシュカード業務、デビットカード業務、クレジットカード業務が挙げられる。

- キャッシュカード業務：キャッシュカードを利用して実施する業務であり、預金口座に関する入金・出金・残高照会・カード振込（振替）等が挙げられる。現在利用されているキャッシュカードとしては、MSカードとICカードがある。
- デビットカード業務：店頭での支払い決済において、その利用代金を、顧客の預金口座から引き落とし、利用店の口座に入金する決済サービス業務。決済のタイミングが即時であるサービスはオンライン・デビットカード業務と呼ばれ

2 本稿でICカードと呼ぶときは、わが国の金融機関がキャッシュカードとして導入を進めている端子付き（接触型）のCPU（中央演算装置）を搭載したICカードを指すものとする。

る。他方、金融機関が預貯金を直接の裏付けとして、清算処理を後日行う取引は、当該金融機関のホスト・システムにアクセスすることなく払出しが可能であるため、オフライン・デビットカード業務と呼ばれる。デビットカードとしてはMSカードが利用されている。

・クレジットカード業務：店頭での支払い決済において、その利用代金をクレジットカード発行機関が立て替え、後日、顧客の預金口座から引き落とすサービス業務。口座からの引き落とし方法については、一括引き落としやリボルビング払い等の種類がある。クレジットカードとしては、MSカードとICカードがある。

わが国におけるICキャッシュカードを利用するシステムの業界標準である「全銀協ICキャッシュカード標準仕様（第2版）」（以下、全銀協仕様。全国銀行協会［2006］）においても、①国内キャッシュカード業務、②国内オンライン・デビットカード業務、③国内オフライン・デビットカード業務、④クレジットカード業務等がICキャッシュカードを利用した代表的な業務として挙げられている[3]。

（3）ICカードを利用した取引を取り巻く環境

従来、キャッシュカードとATMを利用した取引は、金融機関の店舗内等の自行管理下で行われることが基本であった。しかし、オンライン提携の拡大に加え、デビットカード取引の導入等、自行の管理下にないノードやネットワークを利用したサービス業務が拡大していることから、金融機関のキャッシュカードとATMを利用した取引を取り巻く環境は大きく変化している。例えば、自行管理下にある端末での自行カード取引のような、全ノードが自行の管理下にあるシステムでは、そのリスク管理は基本的に自行の「権限と責任の範囲」内であることから、システムへの安全対策は比較的講じやすいといえる。一方、自行の管理下にない部分を含む取引システムでは、おのおのの組織のリスク管理の考え方も異なることから、他の組織との間での権限と責任の範囲の明確化や調整が重要になることが想定される。ICカードを利用した取引を取り巻く環境については以下のように分類することができる。

①システムを構成する全ノードが自行の管理下にあるケース（図1における（A）のみからなるシステム）

②他行の管理下にある部分を含むケース（図1における（A）と（B）を含むシステム）：金融機関であっても、それぞれの組織でリスク管理の考え方が異なる場合があるため、提携方法の検討が必要となる。

③金融機関以外の組織の管理下にある部分を含むケース（図1における（A）と（C）を含むシステム）：金融機関以外の組織では、そのリスク管理の考え方の

3 全銀協仕様では、ICキャッシュカードの利用業務を、「標準化対象業務」、「任意業務」、「領域貸与業務」に分類している。ここで挙げた業務は、標準化対象業務とされているものである。

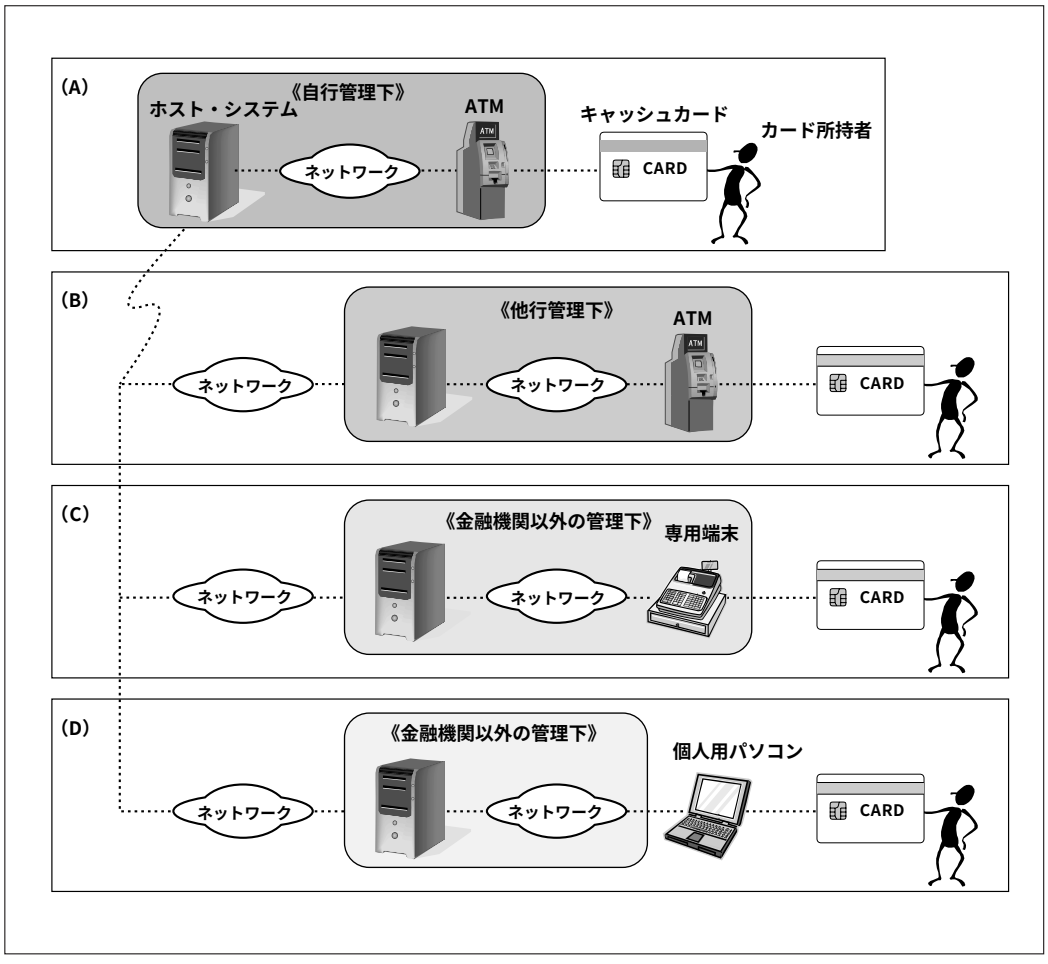
相違を前提にした提携方法の検討が必要である。

④カード所持者の管理下にある部分を含むケース（図1における(A)と(D)を含むシステム）：サービス提供の範囲にカード所持者が保有するパソコンやICカード用装置等を含める場合、それらに対してATMや加盟店端末等と同等の管理状態を期待することは困難である。

⑤異なる環境が混在するケース（図1における(A)と(B)・(C)・(D)のいずれも、あるいは、その一部を含むシステム）：どのようなリスク管理を行うべきかが課題となる。

いずれのケースにおいても、関係組織間での権限と責任の範囲の明確化とともに、リスク管理の考え方の相違を前提にした組織間提携方法の検討が必要であることから、発生し得る例外・異常等について運用までを含めた処理方法の調整・合意が重要となる。

図1　業務を取り巻く環境



今後は、ICカードを利用してデビットカード業務等、リテール・バンキングのサービス範囲を拡大していくことが想定される。図1における（A）、（B）のような、自行の管理下に閉じたシステム、あるいは、業界内に閉じたシステムであれば、設備や運用での安全対策により、システム全体としてある程度の安全性が確保可能であると考えられる。しかしながら、デビットカード業務やインターネット・バンキング業務等は、図1の（C）、（D）における自行の管理下にない環境に設置された端末やオープンなネットワークを利用することになるため、運用による対策では不十分となる場合が想定される。そのため、仮に他組織の管理下にあるノードやネットワーク上で不正が行われた場合においても、安全な処理が実行可能となるような技術面での対応について検討することが必要である。

本稿では、リテール・バンキング・サービスの拡大に伴って顕現化することが想定される脅威を明確にするとともに、ICカードの機能を活用することによってどのような対応が可能となるかについて検討を行う。

3．ICカード導入の効果

本節では、MSカードのみを利用した従来のシステムで想定される脅威への対策技術として、ICカードが果たす役割について整理する。

（1）ICカードを利用したシステムについて

本節で取り扱うリテール・バンキング・システムは、以下のノードとネットワークによって構成されるものとする。

・キャッシュカード：預金口座に対応して発行されるカード。また、キャッシュカードが真正であるとは、当該カードが金融機関によって正規の手続で発行されたものであることを示す。キャッシュカードの形態としては、以下のICカード、MS・IC併用カード、MSカードの3種類が存在する。
　－ICカード：専用のリーダで読み取る端子付きのCPU内蔵型のデバイス。
　－MS・IC併用カード：ICカードに磁気ストライプが貼付されたカード。端末がICカード対応している場合にはICカードとして、そうでない場合にはMSカードとして処理される。
　－MSカード：磁気ストライプのみが貼付されたカード。
・カード所持者：当該キャッシュカードが示す預金口座名義に対応するユーザ。
・ホスト・システム：金融機関の業務を実行するシステムであり、ネットワークを介して各アプリケーションを提供するコンピュータやキャッシュカードの発行システム等を含む。ホスト・システムが真正であるとは、当該ホスト・システムが金融機関によって管理されているものであることを示す。以下、ICカー

ドの生成したデータの処理が実行可能である場合、ICカード対応していると呼ぶ。
・端末：キャッシュカードとホスト・システム間の通信を媒介するデバイス。PINパッド、キャッシュカードのリーダ・ライタ等が一体化して端末を構成している場合や、各デバイスが独立して存在する場合等、さまざまなケースがある。以下、端末がICカードの処理を実行可能である場合、ICカード対応していると呼ぶ。
・ネットワーク：端末とホスト・システムを接続する通信路網。従来の電文にICカードが生成したデータ等を追加可能である場合、ネットワークがICカード対応していると呼ぶ。

さらに、リテール・バンキング・システムを構成する、すべての端末、ホスト・システム、ネットワークがICカード対応していることを、「フルICカード対応」と呼ぶこととする。つまり、フルICカード対応したシステムでは、ICカードとホスト・システム間において、ICカードの生成したデジタル署名等のIC関連項目の送受信が可能となる。

ネットワークを介して実行される取引では、当該取引が正しく実行されていることを電文の通信によって確認する必要がある。取引が正当であることを確認するための代表的な要素としては、以下の3項目が挙げられる[4]。

・カード所持者認証[5]：取引に利用されたキャッシュカードのカード所持者であることを確認すること。
・カード認証：取引に利用されたキャッシュカードが真正であることを確認すること。
・取引データの正当性確認：取引内容を一意に示すことのできるデータが、カードの存在を前提に生成されたものであることを確認すること。

取引データの正当性を確認するうえでは、取引がカード所持者によって真正なカードを利用して行われることが前提であり、当該事項の確認はカード所持者認証とカード認証によって実行される。そのため、取引データには、取引内容を示すデータに加えてカード所持者認証とカード認証の認証結果が含まれる。

本節(2)、(3)では、ICカードの導入によって、カード所持者認証とカード認証の安全性がどのように向上するかについてそれぞれ検討する。また、取引データの正当性確認におけるICカード導入の効果については、本節(4)で検討を行う。

4 本稿では、キャッシュカードに加えて、PINや生体情報を利用して顧客の認証を行うケースについて検討を進めるが、顧客認証を利用するデバイスとしては現在インターネット・バンキングでの本人認証に利用されているワンタイム・パスワード生成器等も考えられる。
5 ここでのカード所持者認証とは、カード所持者が秘密に記憶しておく情報や身体的・行動的特徴に関する情報を利用することで、キャッシュカードと被認証者の対応関係を確認するものを指す。

(2) カード所持者認証について

イ．カード所持者認証の形態

カード所持者認証は、キャッシュカードがカード所持者を特定可能なID（口座番号等）を提示し、「被認証者が提示したデータ（以下、入力データ）」と、「金融機関によってカード所持者認証用のデータとして登録されているIDに対応付けられたデータ（以下、参照データ）」の対応関係を確認することで実行される。以下では、入力データとして、被認証者が記憶している情報である暗証番号（PIN: personal identification number）[6]を利用するものをPIN認証[7]、被認証者の身体的・行動的特徴に関する情報を利用するものを生体認証と呼ぶこととする。

カード所持者認証は、入力データや参照データがどのデバイスに格納されているか、また、認証処理をどのデバイスで実行するかによって、そのタイプを分類することができる。金融分野におけるPINのオンラインでの取扱いに関する国際標準であるISO 9564-1（ISO［2002］）では、PINの認証処理を実行するデバイスとして、①端末、②カード発行機関のホスト・システム、③カード発行機関以外の組織のホスト・システムが想定されている。また、参照データの格納先としては、上記①のケースでは、カードとカード発行機関のホスト・システムが想定され、上記②、③のケースでは、カード発行機関のホスト・システムが想定されている。さらに、オフラインでのPINの取扱いに関する国際標準であるISO 9564-3（ISO［2003］）では、PINの認証処理と参照データの格納をともにICカードで行う形態が記述されている。本節(1)で想定したシステムで実装する場合、ISO 9564-1、9564-3で記述されているカード所持者認証の形態は表1の4つのタイプに分類することができる（図2参照）。

また、生体認証については、ISO/IEC 7816-11（ISO and IEC［2004］）において、生体認証処理と参照データの格納をともにICカードで行うタイプと、参照データをICカードに格納したうえで、端末で認証処理を実行するタイプが記述されている。これらは、キャッシュカードとしてICカードを利用した場合のタイプ1とタイプ2にそれぞれ相当する。

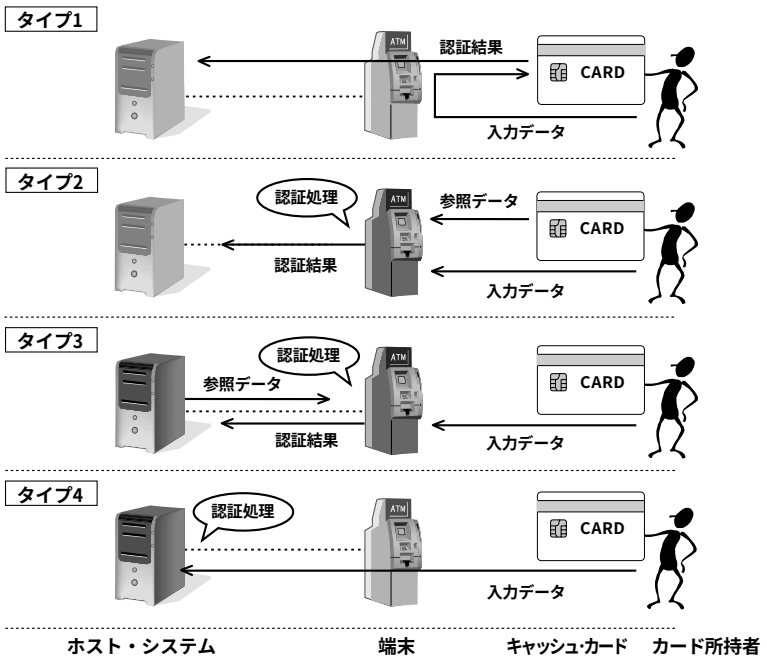
表1　カード所持者認証の4つのタイプ

カード所持者認証の形態	認証処理を実行するデバイス	参照データを格納するデバイス
タイプ1	キャッシュカード	キャッシュカード
タイプ2	端末	キャッシュカード
タイプ3	端末	ホスト・システム
タイプ4	ホスト・システム	ホスト・システム

6 記憶している情報としてパスワードを利用するケースもあるが、本節では、金融分野において広く利用されているPINを利用するケースを例として取り上げる。また、PINの長さについては、ISO 9564シリーズでは4桁から12桁と規定されており、EMV仕様もそれに準拠している。

7 PIN照合やPIN検証と呼ばれることも多い。

図2　カード所持者認証の4つのタイプ



全銀協仕様では、タイプ1とタイプ4で実行されるPIN認証と、タイプ1とタイプ2で実行される生体認証を記述している（表2参照）。

タイプ1とタイプ2は、カード所持者認証を実行するうえで、ホスト・システムとリアルタイムで通信する必要がないため、オフラインでの実行が可能である。ただし、カード所持者認証の結果内容等を含む取引データについては、端末からホスト・システムに送信されるため、そうした手順までを含めて検討を行う。

PINや生体情報を利用するカード所持者認証では、さまざまな脅威が想定される。そのなかでも、なりすましに着目すると、表1で整理したいずれの形態においても、入力データについては、カード所持者からの盗取、入力データ提示時の覗き見等による盗取、端末からの盗取が脅威として想定されるため、こうした攻撃への対策を講じておくことが必要となる。これらはMSカードとICカードのどちらを利用した場合にも共通して想定される脅威であることから、入力データ（PIN、生体情報）はカード所持者によって適切に管理されているほか、データの入力時における盗取への対策が講じられていることとして検討を進める。

そのほか、カード所持者認証一般における脅威に関する検討を行うに当たって、PIN認証と生体認証のいずれのカード所持者認証方式においても共通して想定される脅威を取り上げる。なお、生体認証に特化して想定される脅威、および、その対策技術については、田村・宇根［2007］で整理されている。

表2　わが国のリテール・バンキングにおけるカード所持者認証の形態

カード所持者認証の形態	PIN認証	生体認証
タイプ1	ICカード（全銀協仕様）	ICカード（全銀協仕様）
タイプ2	（ゼロ暗証化前のMSカード）	ICカード（全銀協仕様）
タイプ3	——	——
タイプ4	現行MSカード、ICカード（全銀協仕様）	——

ロ．MSカードを利用したカード所持者認証

表1で分類したカード所持者認証のうち、タイプ2による生体認証については、MSカードのメモリ容量が小さく[8]、生体特徴に関するデータを格納できないことから実装は困難である。そのため、MSカードを利用する場合、タイプ2〜4のPIN認証と、タイプ3と4の生体認証が実装可能である[9]。

PIN認証におけるタイプ2の実装については、MSカードに参照データが格納されていることから、不正なカード・リーダによる参照データの盗取が脅威として想定される。そのため、参照データから入力データが特定可能なケースであれば、第三者によるなりすましが可能となる。実際、過去に発行されたMSキャッシュカードにはPIN認証をタイプ2で実装したものが存在したが、現在は、ゼロ暗証化[10]によって、そうしたMSキャッシュカードの利用は想定されていない。

タイプ2とタイプ3では、端末がホスト・システムに認証結果を送信するため、ネットワーク上における当該データの改ざん・偽造が脅威として想定される。データの改ざん・偽造を検知する方法としては、端末によるデジタル署名（あるいは、MAC）を利用することが考えられるが、端末による不正処理の実行を脅威として想定する場合には、当該データが端末によって偽造されることが考えられる。したがって、端末による不正処理が想定される環境では、カード所持者認証が正しく実行されたか否かを確認することは困難となる。

さらに、タイプ3では、ホスト・システムから参照データが端末に送信されるため、参照データから入力データが推測可能である場合には、当該データの盗取が脅威となる。また、適当に設定した入力データに対応するよう、参照データを改ざんすることも脅威として想定される。そのため、ホスト・システムによる暗号化等による秘匿、および、デジタル署名等の付与による改ざん・偽造防止が必要である。

8　わが国のキャッシュカードに利用されているJISⅡ型のMSカードについては、そのメモリ容量は69バイト（552ビット）とされている。

9　生体認証に利用する個人の身体的・行動的特徴はセンシティブな情報であることから、一般にはホスト・システムに格納するタイプ3やタイプ4での実装は少ないと想定される。

10　キャッシュカードにPINを記録しない方式への変更。1988年以降、発行済みのPINを記録したMSカードについては、一度ATMを利用すれば、PINの記録部分を0000に自動的に書き換えるという手段がとられている。

タイプ4では入力データが端末を経由してホスト・システムに送信されるため、端末とホスト・システム間については暗号化等による入力データの秘匿性確保が必要である。

ハ．ICカードを利用したカード所持者認証

キャッシュカードとしてICカードを利用する場合には、PIN認証と生体認証のいずれにおいても、タイプ1〜4の実装が可能である。

以下では、MSカードを利用したカード所持者認証において想定された脅威がICカードの利用によって対策可能であるか否かについて検討を行う。ICカードが、秘密に格納しているデータを盗取する攻撃についてはさまざまな指摘があるが（田村・宇根［2007］）、本節では、適切に実装されたICカードについてはそうした対策が講じられているものとして検討を進める。そのため、タイプ2で想定されるキャッシュカードからの参照データの盗取については、キャッシュカードのICカード化によって対策が可能となる。

（イ）カード所持者認証結果の改ざん・偽造

認証結果の改ざん・偽造は、タイプ2とタイプ3に加えて、タイプ1においても想定される脅威である。カード所持者認証結果の送信については、フルICカード対応しているか否かによって、可能な対応に差異が生じる。

フルICカード対応しているシステムであれば、認証結果を示す電文にIC関連の新規項目を追加することができるため、認証結果を含むデータにICカードの生成したデジタル署名等を付与することで、当該データの改ざん・偽造を防止することが可能となる。ただし、端末のみがICカード対応しているシステムでは、従来電文形式での通信が行われるため、当該データが改ざん・偽造された場合においても、ホスト・システムはそれを検知することができない。端末が認証結果にデジタル署名等を付与することで防止することも考えられるが、端末による不正処理を脅威として想定する場合には、端末による認証結果の偽造が脅威として想定される。

（ロ）キャッシュカードと端末間におけるデータの盗取

ICカードを利用する場合にはタイプ1による実装が可能となるが、入力データが端末からICカードに送信される際、通信路からの入力データの盗取が脅威として想定される。そのため、端末とICカード間の通信については、暗号化等によって入力データ盗取への対策を講じておく必要がある。例えば、EMV仕様（EMVCo［2004a, b］）では、PINパッドとICカード間の通信路の盗聴が脅威として想定される場合には、PINパッドに入力されたPINを暗号化してICカードに送信することが記述されている。

また、ICカードを利用したタイプ2においては、ICカードと端末間からの参照データの盗取が脅威として想定されるが、参照データをICカード内で暗号化したうえで端末に送信することで対策を講じることが可能となる。

（3）カード認証について

イ．カード認証の形態

カード認証は、キャッシュカードが提示したデータと、当該データに対応して金融機関に登録されるデータとの対応関係を確認することで実行される[11]。

カード認証の代表的な方法としては、以下に紹介する動的認証（DDA: dynamic data authentication）と静的認証（SDA: static data authentication）が挙げられ（田村・宇根［2006］）、EMV仕様や全銀協仕様においてもこれらの認証方式の採用が想定されている。

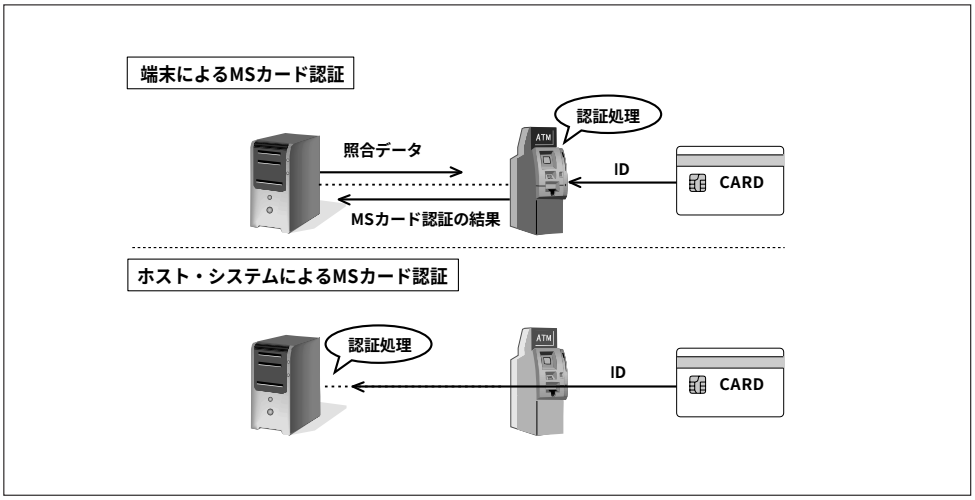
・動的認証：キャッシュカードは内部に秘密鍵を所持しており、認証の都度、当該秘密鍵を利用して新たに生成したデータを認証者（認証処理を実行するデバイス）に提示することにより実行される。動的認証は、通信路上のデータを盗取することによる不正を防止するため、動的認証においてキャッシュカードが生成するデータは毎回異なり、過去のデータから新しいデータの推測が困難であるよう設計される。具体的には、認証者によって乱数が提示され、キャッシュカードは乱数を含むデータに対して秘密鍵を利用した演算結果（デジタル署名、あるいは、MAC）を生成する。認証者は、演算結果を検証し、キャッシュカードが当該秘密鍵を保持していることの確認によってその真正性を判断する。
・静的認証：キャッシュカードは、金融機関によって予め与えられたデータを格納しており、認証時に当該データを提示する。キャッシュカードは当該データを提示し、認証者は当該データが金融機関によって生成されたものであることを確認する。キャッシュカードのメモリ容量がある程度大きい場合には、金融機関のデジタル署名（あるいは、MAC）がキャッシュカード内に格納される。ただし、静的認証では、キャッシュカードが提示するデータを端末や通信路等から盗取することによって、真正であると誤認させるカードの作製が可能となることに注意が必要である。

カード認証を行う手段としては、端末がカード認証を行い、その結果をホスト・システムに送信する形態と、ホスト・システムが認証者として直接キャッシュカードを認証する形態が考えられる（図3、図4参照）。

端末がカード認証を実行する形態において、認証に必要となるデータが予め端末内に格納されている場合には、ホスト・システムとリアルタイムで通信する必要がない。ただし、カード認証の結果内容等を含む取引データについては、端末からホ

11 本節では、メモリに格納されるデジタル・データのみを利用する形態に絞って議論する。カード内部のメモリに格納されるデジタル・データのみを利用するもののほかに、複製困難なカードの物理的情報を利用することでICカード認証を実行することも考えられるが（例えば、人工物メトリクス）、ここでは取り扱わないこととする。

図3　MSカード認証のタイプ



スト・システムに送信されるため、そうした手順までを含めて検討を行う。

ロ．MSカード認証

MSカードは演算処理能力を持たないため、認証方式としては静的認証のみが実装可能であるが、MSカードのメモリ容量は少ないことから、デジタル署名やMACを格納することは困難である。一般には、キャッシュカードに対応する預金口座を一意に特定可能なID[12]をMSカードに書き込み、ホスト・システム内のデータベースに当該IDが存在するか否かによって、MSカード認証が実行される（図3参照）。

現時点では、MSに書き込むべきデータが入手できれば、容易にキャッシュカードの偽造が可能である。そのため、MSカード認証においては、まず、IDの盗取が脅威として想定され、その手段としては、MSカードからIDを不正に読み出す、あるいは、端末からIDを盗取することが考えられる。

端末によるMSカード認証では、ホスト・システムから照合に利用されるデータ（以下、照合データ）が端末に送信されるため、当該データからMSカードが提示するIDが推測可能である場合には、照合データの盗聴が脅威となる。そのほか、適当に設定したIDに対応するよう照合データを改ざんすることも脅威として想定される。そのため、ホスト・システムによる暗号化等による秘匿、および、デジタル署名等の付与による改ざん・偽造防止が必要である。また、カード所持者認証と同様、端末による不正処理の実行が脅威として想定される環境では、ホスト・システムはMSカード認証が正しく実行されたか否かを確認することが困難である。

12 MSキャッシュカードには、銀行番号、支店番号、口座番号等の預金払戻しに必要な情報が記録されている（金融情報システムセンター調査部［2005］）。

さらに、ホスト・システムによるMSカード認証においては、MSカードが提示するIDが端末とホスト・システム間から盗取されることが脅威として想定されるため、端末における暗号化等の対策が必要である。

ハ．ICカード認証

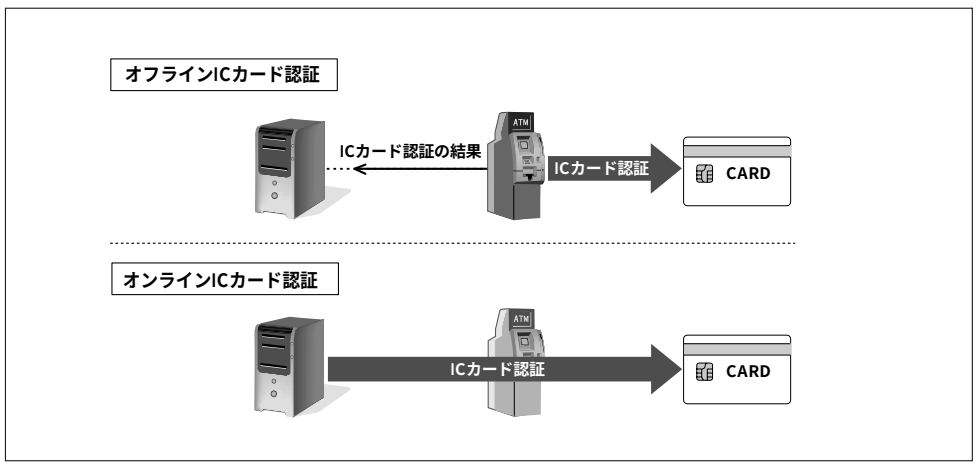
ICカードは暗号処理が実行可能であることから動的認証が実装可能である。本節(3)イ.で述べたように、静的認証については、予めキャッシュカード内に格納されているデータそのものを外部に出力することで実行されるため、ICカードを利用する場合についても、キャッシュカード内部に格納すべきデータが入手できれば、カード認証において真正であると誤認させるカードの作製が可能であるといえる。この点については、MSカード認証と同様の議論が可能となるため、以下ではICカード認証を動的認証によって実行するケースについて検討を行う。

まず、動的認証によるICカード認証では、認証に利用する秘密鍵は外部に出力されないように格納されるほか、ICカードと端末間で通信されるデータについても、そのデータを利用して不正な処理が実行困難であるよう設計されていることから、MSカード認証において想定されたIDの盗取については、キャッシュカードのICカード化によって対策が可能となる。

（イ）オフラインICカード認証

少なくとも端末がICカードに対応している場合には、端末によるオフラインICカード認証が実行可能であり、ICカード認証の結果については、端末からホスト・システムに送信されることとなる（図4参照）。ICカード認証結果の送信については、フルICカード対応であるか否かによって、想定される脅威に差異が生じる。

図4　ICカード認証のタイプ



①端末のみがICカード対応している場合

端末のみがICカード対応している場合、端末がホスト・システムに送信する電文形式は従来と同様であり、ICカード認証の結果を電文に追加することができない。そのため、ホスト・システムはICカード認証とMSカード認証のどちらの認証方式によってキャッシュカードの真正性確認が実行されたのかを判断することができず、不正なMSカードが利用された場合においても、それを検知することができない。ただし、ホスト・システム、および、ネットワークがICカードに対応していない場合においても、キャッシュカードがICカードであるか否かのフラグを電文項目に追加することにより、その区別が可能となれば、MSカードを利用した取引での限度額を引き下げる等の運用での対策を講じることができるようになる[13]。

ただし、フラグの追加が可能であっても、端末による不正な処理の実行が脅威として想定される環境では、端末から送信されるデータが改ざん・偽造されたものでないことの確認は引き続き困難である。

②フルICカード対応している場合

フルICカード対応であるシステムでは、端末がホスト・システムに送信するICカード認証結果を示す電文にIC関連の新規項目を付加することができる。このとき、IC関連の新規項目として、ICカード認証結果等にICカードが生成したデジタル署名等を採用すれば、不正な処理を実行する端末を脅威として想定した場合においても、ICカード認証結果の改ざん・偽造を防止することが可能となる。

（ロ）オンラインによるICカード認証

フルICカード対応したシステムでは、ICカードが生成・提示したデータのホスト・システムへの送信、および、ホスト・システムによるデータ検証が実行可能である。そのため、ホスト・システムとICカード間で実行されるオンラインでのICカード認証が実行可能であり、仮にICカードとホスト・システム間に存在する端末やネットワーク上で不正が行われた場合においても、ICカード認証を安全に実行することができる。

一方、端末のみがICカード対応である場合には、オンラインでのICカード認証は実行できない。

（4）フルICカード対応システムにおける効果

以下では、本節(2)、(3)で整理した内容をまとめるとともに、フルICカード対応した場合における取引データの正当性確認とICカードのリスク管理について検討を行う。

13 既に、ホスト・システムがICカードとMSカードを識別可能となるよう、システムを改修しているとの報告もある（金融財政事情研究会［2005］）。

イ．カード所持者認証における効果

表2で整理したタイプ1～3は、ICカード、あるいは、端末で認証処理を実行するため、認証結果をホスト・システムへ送信する処理が必要となる。そのため、端末による不正処理が脅威として想定される環境で実装する場合には、認証結果が改ざん・偽造されることも考えられる。この場合、フルICカード対応システムであれば、カード所持者認証の結果にIC関連情報（ICカードによるデジタル署名等）を付与することによって、認証結果の改ざん・偽造を防止することが可能となる。

全銀協仕様が想定しているオンライン取引では、カード所持者認証をタイプ4で行うこととしている。タイプ4では、キャッシュカードの種類（MS、IC）やシステムのICカード対応状況によって想定される脅威に差異はない。ただし、本節では、キャッシュカードの偽造についてはカード認証で検知することとし、カード所持者認証ではキャッシュカードが真正であることを仮定して検討を行っている。そのため、カード認証によって偽造カードの検知が困難である場合には、カード所持者認証も正しく実行できないことがある。例えば、タイプ4においては、カード所持者を特定するためのID（データベースから当該カード所持者の参照データを特定するための情報）がキャッシュカードによって提示されるため、攻撃者が適当に選んだ入力データに対応するようIDを変更することも考えられる。MSカードであれば、適当なIDを格納する偽造カードの作製が可能であることから、そうした脅威にも留意が必要となる。

ロ．カード認証における効果

ICカード認証については、端末のみがICカード対応している場合であればオフラインでのICカード認証が可能である。しかし、認証結果をホスト・システムに送信する処理までを考えた場合、ホスト・システムはICカードとMSカードのどちらが使用されたか確認できないため、不正なMSカードの利用が脅威となる。そのため、少なくともICカードとMSカードの区別を可能とする仕組みが必要である。

さらに、デビットカード取引等、端末による不正処理が脅威として想定される環境においては、認証結果の改ざん・偽造が検知困難であることから、カード認証が正しく実行されたか否かをホスト・システムは確認できない。そのため、ICカードが生成したIC関連項目をホスト・システムに送信できるフルICカード対応が望ましいと考えられる。

ハ．取引データの正当性確認における効果

カード所持者認証とカード認証の実行後、当該認証結果に基づき、ホスト・システムは要求された取引内容を処理することになる。この場合、キャッシュカードとホスト・システム間に存在する端末やネットワーク上で不正が行われることが脅威として想定される場合、ホスト・システムは当該取引内容を示す取引データが通信路上で改ざん・偽造されていないことを確認する必要がある。さらに、過去に利用された取引内容の不正な利用を防止するため、取引データについては、一意に取引

内容を示すことが可能となるように生成されることが求められる。

フルICカード対応しているシステムでは、従来電文にIC関連項目が追加可能である。このため、ホスト・システムは認証結果等を含む取引データに対するICカードのデジタル署名等の確認によって、当該データが改ざん・偽造されたものでないことを確認するとともに、取引時においてICカードが利用されたことを確認することができる。これにより、自行の発行したICカードと自行のホスト・システム間での安全な取引が実行可能となる。

例えば、EMV仕様では、ICカードとホスト・システム間で実行される取引内容の通信を「AC生成とカード発行者認証（application cryptogram generation and issuer authentication）」として記述しており、本プロトコルの実行によってICカードとホスト・システム間で取引内容の承認を行うとともに、データが改ざんされていないことを相互に確認可能となっている。

以下に、本プロトコルの手順を紹介する。

1. 端末とICカードは、要求された支払い処理（トランザクション）について、①オフラインで処理が可能か、②オンラインで処理すべきか、③処理を拒否するかを決定する判断基準を有している。こうした決定は、端末による「端末アクション分析」[14]と、ICカードによる「カードアクション分析」[15]の結果を総合して決定され、その決定内容はホスト・システムに送信される。送信されるデータはアプリケーション・クリプトグラム（AC）と呼ばれ、取引承認（TC: transaction certificate）、オンライン承認要求（ARQC: authorisation request cryptogram）、取引拒否（AAC: application authentication cryptogram）のいずれかを示すものとして生成される[16]。ACについては、当該ICカードによって生成されたものであり、かつ、改ざんされていないことをホスト・システムが検証できるよう、ICカードによるMACとして生成される。MACが付与されるメッセージには、カード所持者認証およびICカード認証の結果のほか、取引内容に関する情報や、当該取引の時点でACが生成されたことが検証できるよう、端末によって生成された乱数等が含まれる。オンライン処理を要求（ARQC）した場合、ACはリアルタイムでホスト・システムに送信される。それ以外の場合には、ACは端末に保管される。
2. オンライン処理が要求された場合、ホスト・システムは、要求に対する結果

14 端末アクション分析では、カード所持者認証の結果や予め端末に設定されたオフライン取引の上限取引金額とICカードの取引上限金額との比較結果等と、カード発行者の判定基準やアクワイアラの判定基準をもとに、ICカードに対して要求する取引内容を判定する。

15 カードアクション分析では、オフラインでのPIN認証の結果等の情報とカード発行者の判定基準をもとに、ICカード側の応答を決定する。

16 取引内容の決定については、端末とICカードのどちらかがAACを要求した場合にはAACが選択される。それ以外においてどちらかがARQCを要求した場合にはARQCが選択される。TCが選択されるのは、端末とICカードのどちらもTCを要求した場合のみである。

（拒否、または、承認）をICカードに返信する。この返信はオーソリゼーション・レスポンス・クリプトグラム（ARPC: authorisation response cryptogram）と呼ばれるものであり、ホスト・システムによって生成され、かつ、改ざんされていないことが検証できるよう、MACとして生成される。MACが付与されるメッセージには、ICカードから送信されたARQCとホスト・システムが取引を承認するか否かを示すデータであるARC（authorisation response code）が含まれる。

3. ARPCを受信したICカードは、ホスト・システムによるARCの内容を確認したことを示すため、再度、取引承認（TC）または取引拒否（AAC）を示すACを生成する。2度目に生成されるACは、取引内容を示す情報や端末によって生成された乱数のほか、ホストから送信されたARQCを含む[17]。

ニ．フルICカード対応によるその他の効果

フルICカード対応したシステムについては、ICカードへのリスク管理上の制御が可能になるという効果もある。こうした例の1つに、PINのブロック状態の解除が挙げられる。PIN認証によってカード所持者認証を行う場合には、総当たりによるPINの特定を防止するため、一般にPINの誤入力に関する許容回数が設定されている。許容回数を超える誤入力が検出された場合には、当該キャッシュカードを利用して取引が実行できないよう制御される（PINのブロック状態）。その場合には、金融機関にPINのブロック状態の解除を申請する必要があり、現行のシステムでは、当該キャッシュカードのカード所持者であることを示すことができる証明書とともに金融機関の窓口へ直接届け出る等の対応が必要である。

しかし、本人確認を別の手段（例えば、電話での質疑応答）で実施可能な環境であれば、その確認結果に基づき、オンラインでホスト・システムがPINのブロック状態を解除することが考えられる。フルICカード対応したシステムであれば、ICカードはホスト・システムの認証を実行することが可能であるため、PINのブロック解除が正しい指示であることを確認することができる。例えば、EMV仕様では、本節(4)ハ．で紹介したプロトコルの実行によって、ICカードがホスト・システムを認証したうえで、ホスト・システムからのPINのブロック解除の指示を受けることとなっている。このとき、PINのブロック解除の指示については暗号化されてICカードに送信される。

オンライン処理によるPINのブロック解除が実施可能となることは、一見些細なことのように思える。しかし、PIN認証を実効性を持って実施するためには、PINの誤入力を適切に管理する必要がある。こうした処理が可能となることによって、ユーザの負担を抑えつつ、PIN認証を厳格化できるという意味でセキュリティ上重要な効果を持つと考えられる。

17 2度目のAC生成においてMACが付与されるデータには、ホスト・システムから受信したARQCを含む発行者認証データ（issuer authentication data）等が追加される。

4．フルICカード対応へのアプローチとその課題

前節で整理したように、ICカードの機能を十分に活用するためには、ICカードとホスト・システム間に存在するすべてのノード、および、ネットワークがICカードに対応していることが必要となる。現状をみると、わが国の各金融機関はキャッシュカードをICカード化するとともに、ICカード対応の端末（ATM）の導入を進めている段階であり、ホスト・システムやネットワークはICカードが生成するデジタル署名を送受信、検証可能な仕組みとはなっていない。

全銀協仕様では、フルICカード対応となった時点において、ホスト・システムがICカード認証を実行する形態を「基本形」と呼んでいる。現在は、「経過期間」と呼ばれる、基本形への準備段階であり、ネットワークやホスト・システムがICカード対応していないことから、オフラインでICカード認証を行い、端末とホスト・システム間の通信は従来と同一の電文形式で行われることとなっている。

こうした状況のもと、今後、わが国の金融機関がリテール・バンキング・システムをフルICカード対応させていくに当たって、どのような移行へのアプローチが存在するか検討を行う必要がある。

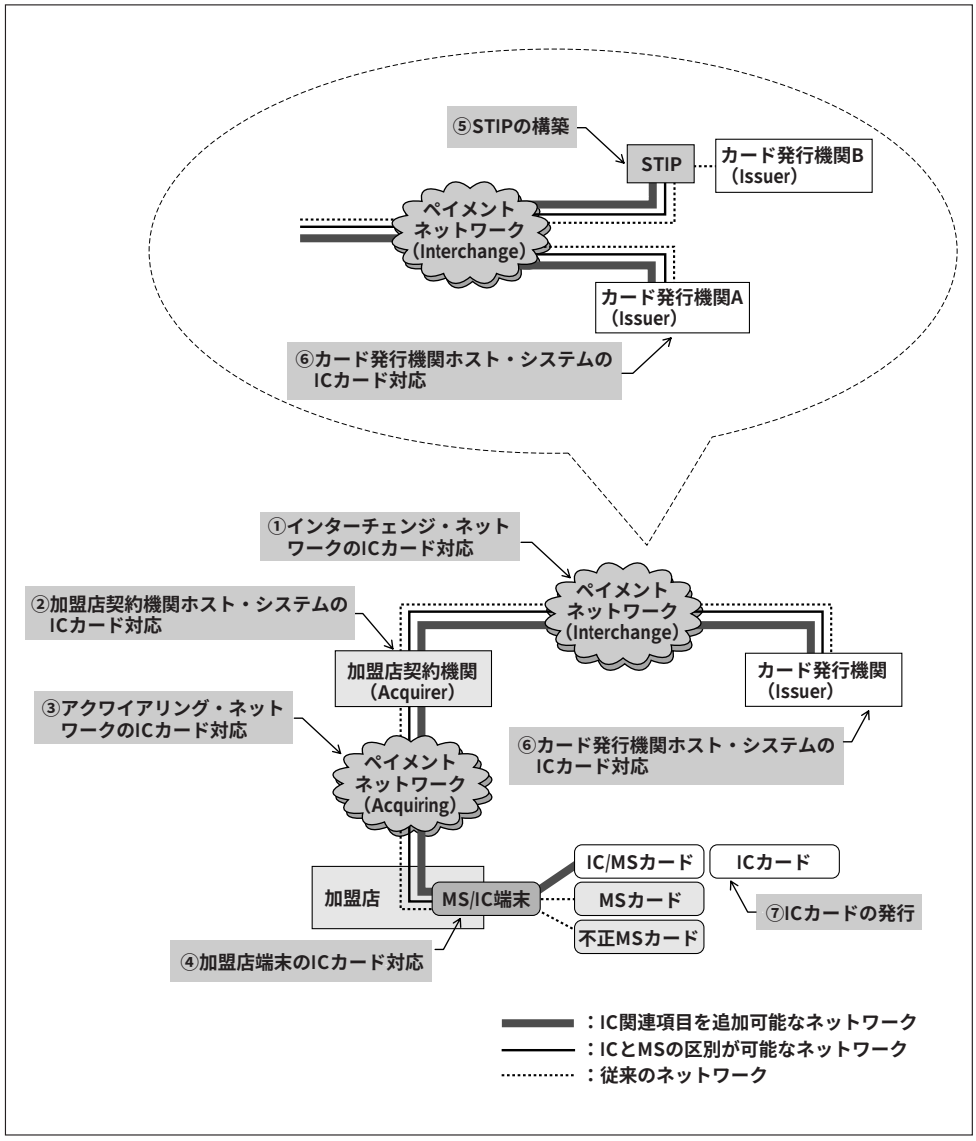
(1) 国際クレジットカード・ブランドが示したアプローチ例

クレジットカード業界は、銀行業界に先駆けてクレジットカードのICカード化を進めてきた。クレジットカードの決済システムをICカード対応させるためには、世界中で発行されているクレジットカードをICカードに移行させるとともに、世界中のカード発行機関のホスト・システム、ペイメント・ネットワーク（国際クレジットカード・ブランド等が管理するインターチェンジ・ネットワーク、加盟店契約会社等が管理するアクワイアリング・ネットワーク）、加盟店端末をICカード対応させる必要がある。そのため、国際クレジットカード・ブランドは、一斉のフルICカード対応ではなく、MSカードとICカードの混在を前提としたシステム・マイグレーションを示した。MSカードとICカードの混在を可能とするシステムとは、MSカードをMSカードとして、また、ICカードをICカードとして処理することが可能であることを意味する。ICカードを利用したシステムへのシステム・マイグレーションでは、少なくとも、管理下をフルICカード対応させたカード発行機関のシステムの安全性を確保することが重要となる。

例えば、Visaでは、システム全体としてのICカード化対応を以下の手順で行っている（図5参照。Visa［2006］, Visa International AP Region［2001］）。

① インターチェンジ・ネットワークのICカード対応
② 加盟店契約機関ホスト・システムのICカード対応
③ アクワイアリング・ネットワークのICカード対応
④ 加盟店端末のICカード対応

図5　Visaが示したシステム・マイグレーション



⑤ スタンド・イン・プロセッシング（STIP: stand-in processing）の提供（⑥が実行できない場合）
⑥ カード発行機関ホスト・システムのICカード対応
⑦ ICクレジットカードの発行

Visaでは、ICカードの処理が可能な態勢を整えたうえで、ICクレジットカードを発行することによって、ICカードがICカードとして処理されないという状況を回避するシステム・マイグレーションを示している。

まず、ICカードがデジタル署名等を生成し（AC等）、IC関連項目として電文に追加した場合においても、それが通信途中で欠損してしまうことがないよう、インターチェンジ・ネットワークをICカード対応させ、そのうえで、加盟店契約機関のホスト・システム、および、アクワイアリング・ネットワークをICカード対応させる。こうした態勢を整えることができれば、ホスト・システムをICカード対応させたカード発行機関とそうでないカード発行機関が混在している場合においても、加盟店端末がICカード対応であれば、前者ではIC機能を活用したセキュリティ対策を行うことが可能となる。また、加盟店端末がICカード対応していない場合には、取引開始の時点からMSカードとして取り扱われるため、端末からカード発行機関のホスト・システムにデータが送信される途中でデータが欠損し、取引が実行不可になることを回避できる。加盟店端末とカード発行機関のホスト・システム間のネットワークをICカード対応させた次の段階として、加盟店端末のICカード化が進められる。

さらに、ホスト・システムのICカード対応前に、クレジットカードのICカード化を進めようとするカード発行機関のために、スタンド・イン・プロセッシングを準備する。スタンド・イン・プロセッシングは、カード発行機関に代わってICカードとの電文通信を行う（AC検証、および、ARPC生成）サービスのことをいう。ただし、本サービスを利用する場合には、カード発行者の秘密鍵を当該サービス提供機関に預ける必要がある。

Visaは、VisaNetと呼ばれるインターチェンジ・ネットワークを少なくとも2001年の時点においてICカード対応させており（Visa International AP Region［2001］）、そのうえで、地域[18]ごとにシステムのICカード対応に関する期限を設定している（Visa［2006］）。例えば、中欧・中東・アフリカ地域（CEMEA）では、2004年10月までにすべての加盟店契約会社のホスト・システムと、アクワイアリング・ネットワークをICカード対応させたうえで、2006年1月までにすべての加盟店端末をICカード対応させることを規定している。つまり、2006年1月の時点で、上記手順の①～③が完了していることになるため、カード発行機関のホスト・システムがICカード対応できれば、当該ホスト・システム以下にフルICカード対応可能なシステムが構築できることになる。一方、中南米・カリブ海地域（LAC）では、2004年までに加盟店契約機関のホスト・システムがICカードとMSカードの区別が可能となるような仕組みを整えることが規定されている。このように、世界の各地域によってICカード対応のスケジュールは異なっており、ICカード対応が進んでいない地域もみられるが、中欧・中東・アフリカ地域のように、フルICカード対応が可能となっている部分が存在していることがわかる。

国単位でみると、フランスでは、2006年末においてクレジットカードの99.6%が

18 Visaは、世界を、アジア太平洋地域（AP: Asia Pacific）、カナダ（Canada）、中欧・中東・アフリカ地域（CEMEA: Central and Eastern Europe, Middle East and Africa）、ヨーロッパ（Europe）、中南米・カリブ海地域（LAC: Latin America and Caribbean）、米国（US: United States）の6つの地域に分けて管理している。

EMV仕様に準拠したICカードとなり、端末の96.4%がICカード対応となっているとの報告がある（Groupement des Cartes Bancaires “CB”［2007］）。英国においてもChip and PINと呼ばれるICカード化推進計画のもと、急速なICカード対応が進められている。

また、アジア太平洋地域（AP）では、地域内もしくは同一国内において、EMV非準拠の端末でEMV準拠カードを処理したために偽造カードを利用した不正取引が発生した場合について、2006年1月以降は、その責任をカード発行機関から加盟店契約会社に移行すると発表している（ビザ・インターナショナルAP［2007］）。このように、Visaでは、フルICカードへの移行スケジュールとともに、問題が発生した場合における権限と責任の範囲についても示している。

（2）全行一斉移行を前提にした場合における問題点

全銀協仕様では、経過期間において発行されるICカードは、基本形においても対応できるものとなっていることが想定されている。そのため、他の金融機関がフルICカード対応を進める中、ホスト・システムがICカード対応していない金融機関が存在した場合、当該金融機関のICカードは他の金融機関の端末では基本形（オンラインICカード認証）を実行しようとするため、ホスト・システムでは取り扱うことができなくなる等の問題が発生する。こうした理由から、全銀協仕様では、全行一斉にフルICカード対応に移行することが望ましいとしている。

すべての金融機関が一斉にフルICカード対応に移行することを想定すると、最後の1機関の準備が整うまで移行できないことになる。その場合には、3節で整理したように、端末のみがICカード対応している場合に想定される脅威が顕現化してしまう可能性も否定できない。リテール・バンキングの安全性を確保するためには、他の金融機関がICカード対応するまでの間は、ホスト・システムをICカード対応させたうえで、発行したICキャッシュカードを自行の端末でのみ使用可能とすることも考えられる[19]。しかし、その場合、顧客の利便性は大幅に損なわれる。

（3）フルICカード対応に向けての課題

イ．サービス業務拡大における課題

現在、わが国の金融機関はデビットカード取引やインターネット・バンキング等の提供に伴い、自行の管理下にないノードやネットワークを利用したサービス業務を拡大していることから、金融機関のキャッシュカードを利用した取引を取り巻く環境を考慮して安全対策に関する検討を行うことが必要である。例えば、自行の管理下にある端末を利用する限りにおいては、設備・運用によってある程度の安全性

19 現在も、自行の端末でのみ利用可能なICカードを発行している金融機関があるが、生体認証の実施を目的としたケースが多い。

が確保できていると考えられる。しかしながら、リスク管理の考え方が異なる組織のもとで管理されるATMやデビットカード端末等については、端末が不正に操作されることを脅威として想定したうえで対策を講じておくことが必要になると考えられる。また、ATMについては、筐体が重厚であることから、偽のATMの作製は困難であることが想定されるが、偽端末が比較的容易に作製できるようなアプリケーションでは、そうした偽端末の設置によるICカード、PIN、生体情報等の盗取を脅威として想定したうえで対策を講じておくことも重要である。

異なる組織の管理下にあるシステムと提携する場合には、運用によってある程度の対策が可能であった問題や、これまでは想定されていなかった脅威が顕現化することが考えられる。そのため、十分な検討のうえで、必要な対策を講じておくことが重要であるとともに、仮に、何らかの事件・事故が発生した場合においても、その他のシステム（他のカード、他のサービス、他のシステム等）に影響を与えることがないような仕組みを準備しておくことが有効であろう。また、発生した問題に対しては、その責任の所在を明確にすることができるよう、カード所持者、自行、他組織との権限と責任の範囲を明確化しておくことが重要であり、運用までを含めた処理方法に関して、他組織との調整・合意が必要であると考えられる。

ロ．システムの拡張性

リテール・バンキング・システムのフルICカード対応を進めていくうえでは、今後予想されるシステムの拡張にも速やかに対応できるようなシステム構築をしておくことが望ましいと考えられる。

例えば、システム内で利用される暗号アルゴリズムは、一般にはコンピュータ・パフォーマンスや暗号技術の進展に伴い、その安全性は低下することから、ある一定の期間ごとに移行が必要になる。現在の金融システムで多く利用されているとみられる、2-key トリプルDES、公開鍵長を1,024ビットとするRSA、SHA-1等は、今後10～15年にわたって十分な安全性を確保することが難しいことが指摘されており、米国連邦政府機関のシステムでは、これらのアルゴリズムの使用を2010年末までとする方針を示している。こうした移行に関する問題は暗号アルゴリズムの2010年問題と呼ばれており、金融分野においても対応していくことが求められている（宇根・神田［2006］）。暗号アルゴリズムの移行については、今後同様の問題が発生した場合においても適切に対応できるよう準備しておくことが重要である。

また、汎業界における情報セキュリティ技術の国際標準化を担当するISO/IEC JTC1/SC27では、オープンなネットワークで生体認証を利用するための仕組み（ACBio: authentication context for biometrics）について国際標準化のための審議が行われている（ISO and IEC［2007］）。現在、わが国のリテール・バンキングでは、生体認証を実行する端末はATMに限られているが、今後、自行の管理下にない汎用の端末や装置を利用して生体認証を実行することも考えられる。しかし、オフラインで生体認証が行われる場合、ホスト・システムは、生体認証が正しく実行されたか否かを判断することが困難である。ACBioは、ホスト・システムが生体認証結

果の正当性を判断するためのものであり、利用された装置での処理は十分な精度・品質を有するか、処理は安全に実行されているか等の情報を含むものである。今後、オープンなネットワークでのサービスの提供を想定するのであれば、こうした技術を採用した場合においても容易に対応できるようなシステムの拡張性が必要であると考えられる。

5．おわりに

現在、わが国の金融機関は、キャッシュカードのICカード化、および、端末のICカード対応を進めており、ICカード対応の端末を利用する場合に限ってみれば、ICカードと端末間で実行される処理の安全性が従来と比較して向上しているといえる。これまでわが国の金融機関が採用してきた、企業内・業界内に閉じたクローズド・システムであれば、端末とホスト・システム間については設備と運用によって十分な安全対策を講じることが可能であったことから、ICカードと端末間の処理さえ安全に実行できれば、システム全体としてある程度の安全性が確保可能であったと考えられる。しかしながら、銀行の管理下にない環境に設置された端末やオープンなネットワークを利用することによってリテール・バンキングのサービス範囲を拡大するに当たっては、運用による対策では不十分となるリスクがある。そのため、仮に他組織の管理下にあるノードが不正動作した場合においても安全な処理が実行可能となる技術面での対応について検討することが必要である。また、何らかのトラブルが発生した場合においても適切に対応できるよう、提携する他組織とのリスク管理の考え方の相違を前提にした提携方法について検討しておくことが重要であると考えられる。

現行のシステムについては、MSキャッシュカードが残存する間は、MSカードの偽造による不正取引は引き続き脅威として想定されるため、端末とキャッシュカードのみであっても、できるだけ速やかにICカード化することが望ましい。さらに、次の段階として、ICカードの有する機能を十分に活用するためには、端末のみならず、ネットワークやホスト・システムをICカード対応させることが重要となる。ある期限までに全行一斉にフルICカード対応するというシステム・マイグレーションは実現困難であると考えられるが、フルICカード対応への移行が先延ばしになれば、積極的にICカード対応を進めようとする金融機関を足止めさせてしまうことになるため、各金融機関がビジネス・ディシジョンを行うことができるシステム・マイグレーションが求められる。こうした観点からは、国際クレジットカード・ブランドが示しているアプローチが参考になると考えられる。また、今後、システムの移行を進めていくに当たっては、暗号化技術の発展やさらなるサービスの拡大等を考慮しておくことも重要である。ビジネスニーズの変化や技術発展への対応を意識した拡張性を考慮しつつ、早期にフルICカード対応への移行を検討することが必要であろう。

参考文献

岩下直行、「金融機関の情報セキュリティ対策のあり方について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、17～29頁

内田浩示、「全銀協ICキャッシュカード標準仕様の改訂について」、『金融』2006年5月号、全国銀行協会、2006年、25～30頁

宇根正志・神田雅透、「暗号アルゴリズムにおける2010年問題について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、31～71頁

金融財政事情研究会、「特集：急展開するICキャッシュカード」、『週刊金融財政事情』2005年3月28日号、金融財政事情研究会、2005年、12～29頁

金融情報システムセンター、「金融機関業務のシステム化に関するアンケート調査結果」、『金融情報システム』平成18年10月増刊61号、金融情報システムセンター、2006年

金融情報システムセンター調査部、「キャッシュカードシステムの課題と欧米金融機関の対応例」、『金融情報システム』平成17年夏号、金融情報システムセンター、2005年

金融庁、『偽造キャッシュカード問題に対する金融機関の取組み状況（平成17年12月末）』、金融庁、2006年（http://www.fsa.go.jp/news/newsj/17/ginkou/f-20060223-3.pdf）

全国銀行協会、『「偽造キャッシュカード対策に関する申し合わせ」について』、全国銀行協会、2005年（http://www.zenginkyo.or.jp/news/17/news170125.html）

――――、『全銀協ICキャッシュカード標準仕様（第2版）』、全国銀行協会、2006年

田村裕子・宇根正志、「金融取引におけるICカードを利用した本人認証について」、『金融研究』第25巻別冊第1号、日本銀行金融研究所、2006年、73～131頁

――――・――――、「ICカードを利用した本人認証システムにおけるセキュリティ対策技術とその検討課題」、『金融研究』第26巻別冊第1号、日本銀行金融研究所、2007年、53～100頁（本号所収）

日本クレジットカード協会、『ICクレジットカード導入について』、日本クレジットカード協会、2004年（http://www. jcca-office.gr.jp/dealer/pdf/ic_card.pdf）

ビザ・インターナショナルAP、『VISA ICカード 方針と促進策』、ビザ・インターナショナルAP、2007年(http://www.visa-asia.com/ap/jp/merchants/productstech/policiesandincentives. shtml)

安岡 彰・平塚知幸、「ICカードが促す金融機関経営の変容」、『知的資産創造』2005年6月号、野村総合研究所、2005年

EMVCo, *EMV Integrated Circuit Card Specifications for Payment Systems- Book 2 Security and Key Management, Version 4.1*, EMVCo, 2004a.

――――, *EMV Integrated Circuit Card Specifications for Payment Systems- Book 3 Application Specification, Version 4.1*, EMVCo, 2004b.

Groupement des Cartes Bancaires “CB”, Migration in France: Key- Figures, Groupement des Cartes Bancaires, 2007. (http:// www.cartes-bancaires.com/en/dossiers/emv_dda.html)

International Organization for Standardization (ISO), *ISO 9564-1, Banking- Personal Identification Number (PIN) management and security- Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*, ISO, 2002.

――――, *ISO 9564-3, Banking- Personal Identification Number (PIN) management and security- Part 3: Requirements for offline PIN handling in ATM and POS systems*, ISO, 2003.

――――, and International Electrotechnical Commission (IEC), *ISO/IEC CD 24761, Information technology -Security techniques - Authentication context for biometrics*, ISO, 2007.

――――, and ――――, *ISO/IEC 7816-11, Identification cards- Integrated circuit cards- Part 11: Personal verification through biometric methods*, ISO, 2004.

Visa, *Visa International Operating Regulations Chip Mandates and Liability Shifts*, Visa, 2006. (http://partnernetwork.visa.com/dv/mandates/pdf/ChipMandates.pdf)

Visa International AP Region, *The Heart of Smart*,Visa International AP Region, 2001. (http://www.visa.com.tw/ newsroom/includes/uploads/Heart_of_Smart_Consumer_Research.pdf)