■11 群（社会情報システム）－ 7 編（金融情報システム）

4 章 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

（執筆者：田村裕子）［2009 年 3 月 受領］

■概要■

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を背景に，2005 年以降，我が国ではキャッシュカードの IC カード化が進められている．2008 年 3 月末時点での金融庁による調査 [1]では，発行されたすべてのキャッシュカードに対する IC カードの比率は 5.6%となっており，増加傾向を維持しつつも十分に普及しているとは言いがたいのが実情である．一方，ATM における IC キャッシュカード対応に関しては 63.9%となっており，ATM 側での IC キャッシュカード対応は一定のレベルに達しつつあるといえる．

こうした IC カード化に伴って留意すべき主な問題点として，①IC カード化の過渡期における磁気ストライプによる取引の問題と，②制御困難な環境下における IC カードによる取引の安全性の問題があげられる．

磁気ストライプによる取引の問題に関しては，キャッシュカードとして現在発行されている IC カードの多くが利便性と互換性を維持するために従来と同じ磁気ストライプを有し，当該データによる取引を実行できるという状況に起因する．ATM からホスト・システムへのデータが磁気ストライプ・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 カードと磁気ストライプ・カードのどちらが利用されたかを区別できない．その結果，カードの種類によってサービス内容を制御できず，磁気データをコピーした偽造カードによって IC カードでの取引を不正に実行できてしまうおそれがある．今後，キャッシュカードの IC カード化とそのためのシステム対応をどのように進めていくかについて検討する必要がある．

制御困難な環境下における取引の安全性の問題については，IC カードによって提供されるサービスが，デビットカード業務などのオープンなネットワークを利用したものに拡大していく場合に留意する必要がある．金融機関の管理下にない環境に設置された端末やネットワークを利用するケースでは，従来のシステムでは想定しなかった脅威が顕現化する可能性があり，新たなセキュリティ対策の実施が必要となる可能性がある．端末やネットワークにおいて不正が行われたとしても，自社発行の IC カードと自社のホスト・システムとの間での取引が安全に実行できるように対策を検討することが重要となる．

本章では，こうした問題に対処するうえで重要な検討項目として，キャッシュカードとして IC カードを利用する場合に ATM など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，また，IC カードに対応したシステムにどのように移行すべきかを，田村・廣川による検討結果 [2]を参照しつつ説明する．

【本章の構成】

まず，我が国のキャッシュカードの IC カード化とそれを利用したリテール・バンキングを取り巻く環境について説明する（4-1 節）．そのうえで，磁気ストライプのカードでの取引システムで想定される脅威への対策として IC カード導入の効果を整理し（4-2 節），IC カード対応に伴う課題を，クレジットカード業界における取組みを参照しながら検討する（4-3 節）．

■11 群 － 7 編 － 4 章

4-1 IC カードを利用したアプリケーション

（執筆者：田村裕子）［2009 年 3 月 受領］

4-1-1 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情報（口座番号など）を提示するためのデータ・キャリアとしての機能を有している．磁気ストライプ・キャッシュカードは，当初その偽造が困難とみられ，運用上適切に管理されている限り，「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」とする本人認証方式に利用できるとされてきた．しかし，近年，磁気ストライプ上に記録される情報の読取りや書込みを容易に実行可能な装置の入手が容易となり，ATMなどの端末に真正であると誤認させるカードの偽造も容易となったことから，最近ではICカード[1]への移行が進められている．

IC カードについても，IC 部分に書き込むべきデータが入手できると，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となる．「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・記憶の機能を活用して内部データへの不正なアクセスを防ぎ，リテール・バンキング・システム（単に，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となることを意味する．IC カードの導入によって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にシステムを設計することが必要となる．

4-1-2 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・バンキングの代表的な業務としては，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あげられる[2]．キャッシュカード業務は，キャッシュカードを利用して実施する業務を指し，預金口座に関する入金・出金・残高照会・カード振込（振替）などをいう．現在，磁気ストライプのキャッシュカードとICキャッシュカードがある．

デビットカード業務は，店頭での支払いにおいて，その支払金額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という業務である．決済が即時である場合にはオンライン・デビットカード業務と呼ばれ，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場合は，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ことから，オフライン・デビット業務と呼ばれる．現在，磁気ストライプのキャッシュカードと IC キャッシュカードによるオンライン・デビットカード業務が行われている．

クレジットカード業務は，店頭での支払いにおいて，その支払金額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という業務である．口座からの引落

[1] 本章において IC カードと呼ぶときは，我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 を搭載した IC カードを指す．

[2] 我が国の IC キャッシュカード・システムの業界標準の「全銀協 IC キャッシュカード標準仕様（第 2 版）」（全銀協仕様）[3] 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などが IC キャッシュカードを利用した代表的な業務としてあげられている．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」に分類しており，上記の各業務は標準化対象業務に対応する．

し方法には一括引落しやリボルビング払いなどがある．クレジットカードとしては磁気ストライプ・カードと IC カードがある．

4-1-3 IC カードを利用した取引を取り巻く環境

上記のとおり，現行のリテール・バンキングにおいては磁気ストライプのカードが利用されるケースが多いが，今後も足元の傾向が続き，IC カードへの移行が進展するとみられる．ATM などを利用してオンラインで実行されるリテール・バンキングに焦点を当てたときに，IC カードを利用した取引の環境がどのようなものになると想定されるかを検討する．

従来，キャッシュカードと ATM を利用した取引は，金融機関の店舗内などの管理下で行われることが基本であった．オンライン提携の拡大に加え，デビットカード業務の導入など，直接の管理下にないネットワークなどを利用した業務が拡大すれば，IC カードを利用した取引を取り巻く環境は大きく変化する．具体的には以下の五つのケースが考えられる．

- ネットワークを含む取引システム全体が管理下にあるケース．
- システムの一部がほかの金融機関の管理下にあるケース（金融機関によってリスク管理の考え方が異なる場合があり，システム運用に関する調整・検討が必要）．
- システムの一部が金融機関以外の組織の管理下にあるケース（当該組織ではリスク管理の考え方が金融機関と有意に異なり，システム運用に関する調整・検討が必要）．
- システムの一部が IC カードの所持者の管理下にあるケース（IC カードの所持者のパソコンや IC カード用装置などがシステムの一部に含まれ，それらに対して ATM や加盟店端末などと同等の管理状態を期待することは困難）．
- システムが様々な主体の管理下にある部分から構成されるケース．

個々の金融機関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を確保・維持可能であると考えられる．ただし，今後，IC カードを利用したリテール・バンキングのサービス範囲の拡大が予想されるなか，デビットカード業務やインターネット・バンキング業務のように，金融機関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ようになれば，他組織の管理下に設置された端末やネットワーク上で不正が行われるというケースも考慮したうえで技術的な対策について検討することが必要となる．

また，上記のいずれのケースにおいても，関係組織間・関係者間での権限と責任の範囲の明確化が重要である．また，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り，発生し得る例外・異常について運用を含めた処理方法の調整・合意が重要となる．

■11 群 － 7 編 － 4 章

4-2 IC カード導入による効果

（執筆者：田村裕子）［2009 年 3 月 受領］

4-2-1 IC カードを利用したシステムについて

ここでは，以下の要素から構成されるキャッシュカードによる取引のシステムを考える．

- 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であり，IC カード，磁気ストライプ・IC 併用カード，磁気ストライプ・カードの 3 種類がある．専用のリーダで読み取る端子付きの CPU 内蔵型のデバイスを IC カード，磁気ストライプのみが貼付されたカードを磁気ストライプ・カード，IC カードに磁気ストライプが貼付されたカードを磁気ストライプ・IC 併用カードと呼ぶ．
- 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などを含む．
- 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．
- 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．

こうしたシステムによる取引では，①カード所持者が当該預金口座名義のユーザであること，②カードが真正であること，③取引データが当該カードの存在を前提に生成されたものであることをそれぞれ確認して取引自体の正当性を確認するケースが多い．取引データの正当性の確認は，カード所持者とカードの確認が成功することが前提となることから，取引データにはこれらの確認の結果を示すデータが含まれることになる．以下では，システムを構成するすべてのホスト・システム，端末，ネットワークが IC カードの処理を実行可能であるとき，システムが「フル IC カード対応」であるという．

4-2-2 カード所持者認証について

一般に，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する ID（口座番号など）を提示し，被認証者が提示したデータ（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データ（参照データ）の対応関係を確認することで実行される．カード所持者認証としては，暗証番号（PIN）を利用する PIN 認証や生体情報を利用する生体認証がある．本認証の形態は参照データの格納場所と認証処理を実行するエンティティによって 4 分類可能であり，PIN の取扱いに関する国際標準 ISO 9564-1[4]と ISO 9564-3[5]の規定をベースとすれば，カード所持者認証の形態は**表 4･1** のケース 1～4 に分類される．なお，いずれのケースにおいても，認証結果は最終的にホスト・システムに送信される．

表 4・1　ISO 9564 シリーズをベースとするカード所持者認証の四つのケース

形態	データ格納や処理実行の場所		各認証方法に利用可能なカードの種類	
	参照データの格納場所	認証処理の実行場所	PIN 認証	生体認証
ケース 1	キャッシュカード		IC キャッシュカード（全銀協仕様）	
ケース 2	キャッシュカード	端末	（ゼロ暗証化前の磁気ストライプ・カード）	IC キャッシュカード（全銀協仕様）
ケース 3	ホスト・システム		（全銀協仕様に規定なし）	
ケース 4	ホスト・システム		磁気ストライプ・カード，IC キャッシュカード（全銀協仕様）	

カード所持者認証において想定される脅威として，カード所持者からの入力データの盗取，入力データ提示時ののぞき見などによる盗取，端末からの入力データの盗取があげられるが，ここでは，入力データが適切に管理・保護されていると仮定する．このとき，磁気ストライプ・カードと IC カードの効果を整理すると**表 4･2** のとおりである．

表 4・2　カード所持者認証において想定される脅威と対応

形態	磁気ストライプ・カード	IC カード（PIN 認証，生体認証ともに可能）
ケース 1	（いずれの認証も実行困難）	・認証結果の改ざんに対し，フル IC カード対応では認証結果のデータへのディジタル署名の付与などが必要．フル IC カード対応でない場合，ケース 2 の磁気ストライプ・カードと同様． ・カード・端末間の入力データ盗取に対し，暗号化などが必要．
ケース 2	【PIN 認証のみ実行可能】 ・不正な端末による参照データの盗取への対応が必要． ・認証結果の改ざん・偽造に対し，端末によるディジタル署名の付与などが必要．不正な端末の場合は防止困難．	・認証結果の改ざんに対してはケース 1 と同様． ・カード・端末間の参照データ盗取に対し，IC カードによる参照データの暗号化などが必要．
ケース 3	・不正な端末による参照データの盗取・改ざんに対し，暗号化やディジタル署名の付与などが必要． ・認証結果の改ざん・偽造に対してはケース 2 と同様．	・不正な端末による参照データの盗取・改ざんに対し，暗号化やディジタル署名の付与などが必要． ・認証結果の改ざんに対してはケース 1 と同様．
ケース 4	端末・ホスト・システム間の通信データの盗取に対し，暗号化などが必要．	端末・ホスト・システム間の通信データの盗取に対し，暗号化などが必要．

このように，磁気ストライプ・カードと比べると，IC カードによる暗号機能を活用することによって各種の脅威に対抗可能となる．ただし，フル IC カード対応でないシステムの場合，磁気ストライプ・カードと同様の対応が必要となるケースもある点には留意が必要である．

4-2-3 カード認証について

カード認証は，一般に，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ているデータとの対応関係を確認することで実行され，その代表的な方法として「動的認証」と「静的認証」があげられる [6]．動的認証は，認証のたびにキャッシュカード内部の秘密鍵を利用して新たに生成されたディジタル署名などが認証者（認証処理を実行するデバイス）に提示されるかたちで実行される．例えば，認証者から提示された乱数

にキャッシュカード側でディジタル署名が生成され，認証者が当該署名を検証してカードの真正性を判断する方法がある．静的認証は，ある一定のデータがキャッシュカードに格納され，当該データが認証者に提示されるかたちで実行される．認証の形態としては，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「オフライン・カード認証」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「オンライン・カード認証」がある．

(1) 磁気ストライプ・カードの場合

磁気ストライプ・カードは，カード自体が演算処理能力をもたず動的認証が実現困難であるほか，メモリ容量が少なくディジタル署名や MAC も格納困難である．一般に，対応する預金口座を特定する ID を磁気ストライプに書き込んでおき，ホスト・システム内のデータベースに当該 ID が存在するか否かを確認することで認証が行われることから，カードから ID を不正に読み出す，端末から ID を盗取する，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といった脅威があげられる．オフライン認証の場合，ホスト・システムから照合に利用されるデータが端末に送信されるが，当該データから ID を不正に読み出すという脅威も想定される．こうしたことから，データの暗号化などによる秘匿やディジタル署名などの付与による改ざん・偽造の防止が求められる．ただし，端末による不正処理が想定される環境では，ホスト・システムによるカード認証の適切性が確認困難となることがある．また，オンライン認証の場合，カードから提示される ID の端末・ホスト・システム間での盗取が想定され，端末における暗号化などが必要となる．

(2) IC カードの場合

IC カードは暗号処理が実行可能であり動的認証を実行可能である．静的認証については，キャッシュカード内部のデータが入手できればカードの偽造が可能になってしまい，磁気ストライプ･カードの場合と同様の議論となるため，ここでは動的認証の場合に焦点を当てる．

(a) オフライン IC カード認証

オフラインICカード認証では，ICカード認証の結果のデータが端末からホスト・システムに送信されることになるが，当該データに関して想定される脅威はシステムがフルICカード対応か否かに依存する．端末のみがICカード対応しているケースでは，端末がホスト・システムに送信するデータ形式は従来と同様であり，認証対象のキャッシュカードがICカードか磁気ストライプ・カードかをホスト・システムが判断できず，偽造された磁気ストライプ・カードであっても検知困難である．キャッシュカードがICカードか否かのフラグをデータ項目に追加するなどの方法でカードの区別が可能な場合は，運用での対策も可能となる[3]．ただし，そうした場合であっても，端末による不正な処理の実行が脅威として想定される場合には，端末から送信されるデータの真正性は引き続き確認困難である．

フル IC カード対応しているケースでは，端末がホスト・システムに送信するデータに IC 関連の新規項目を付加可能であり，IC カード認証結果のほかに，IC カードによるディジタル署名などを追加することによって，IC カードの認証結果を示すデータの偽造を防止可能となる．

[3] 既にホスト・システムが IC カードと磁気ストライプ・カードを識別可能となるようにシステムの改修が実行されているとの報告もある [7].

(b)　オンライン IC カード認証

フル IC カード対応しているケースでは，オンラインでの IC カード認証が実行可能であり，IC カードが生成・提示したデータをホスト・システムに送信し，ホスト・システムによる当該データの検証が可能である．仮に，IC カードとホスト・システムとの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でも，IC カードの認証を適切に実行可能である．なお，端末のみが IC カード対応のケースでは，オンラインでの IC カード認証は実行できない．

4-2-4 フル IC カード対応したシステムにおける効果

(1)　カード所持者認証における効果

カード所持者認証のうちケース 1～3 においては，IC カードや端末において認証処理が実行され，認証結果がホスト・システムへ送信される．端末による不正処理が脅威として想定される環境では認証結果のデータが改ざん・偽造される可能性があるが，フル IC カード対応システムであれば，認証結果のデータに IC 関連情報（IC カードによるディジタル署名など）を付与することによってそうした改ざん・偽造の検知が可能となる．

全銀協仕様におけるオンライン取引のカード所持者認証はケース 4 が想定されている．ケース 4 では，カード認証によってカードの偽造を検知可能であれば，キャッシュカードの種類やシステムの IC カード対応状況によって想定される脅威に大きな差異はない．しかし，仮に，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）が攻撃者の手にわたり，当該 ID と整合的に入力データを偽造されてしまうと，磁気ストライプ・カードの場合にはカード偽造による不正行為が成功する可能性もある点には留意が必要である．

(2)　カード認証における効果

IC カードの場合，端末のみが IC カード対応しているケースであってもオフライン・カード認証が可能である．ただし，認証結果のデータをホスト・システムに送信する処理までを考えた場合，ホスト・システムがカードの種類を識別できず，不正な磁気ストライプ・カードの利用が脅威となる．そのため，少なくともカードの種類を識別可能にする必要がある．

更に，デビットカード取引など，端末の不正処理が脅威として想定される環境においては，認証結果のデータの改ざん・偽造が検知困難であり，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ことから，IC カードによって生成されたデータをホスト・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．

(3)　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，ホスト・システムは，それらの認証結果に基づいて，要求された取引内容を処理する．その際，キャッシュカードとホスト・システムとの間に存在する端末やネットワーク上で不正が行われる可能性がある場合，ホスト・システムは当該取引内容を示す取引データの一貫性を確認する必要がある．更に，過去に利用された取引内容の不正な再利用を防止するために，取引内容を一意に特定できるように取引データを生成す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においては，IC カードによって生成されるデータを従来からのデータ形式に追加可能である．そこで，ホスト・システムは，認証結果などを含む取引データに対する IC カードのディジタル署名などによって取引データの一貫性を確認

可能であるほか，取引時において IC カードが利用されたことを確認可能であるため，当該金融機関発行の IC カードと同ホスト・システムとの間での安全な取引が実行可能となる．

(4) そのほかの効果

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．例えば，PIN のブロック状態を解除するという処理においては，通常，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証明書とともに金融機関の窓口へ直接届け出るなどの対応が必要である．これに対して，フル IC カード対応したシステムであれば，IC カードがホスト・システムを認証可能であるため，PIN のブロック解除が正しい指示であることを IC カード自身が確認可能であり，金融機関の窓口に行くことなく PIN のブロック解除が可能になる．こうした処理が可能となることは，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もつと考えられる．

■11 群 － 7 編 － 4 章

4-3 フル IC カード対応へのアプローチとその課題

（執筆者：田村裕子）［2009 年 3 月 受領］

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エンティティとネットワークが IC カード対応していることが必要となる．我が国では，各金融機関がキャッシュカードの IC カード化と IC カード対応端末（ATM）の導入を進めている段階であり，IC カードのディジタル署名などの機能を十分に活用する体制には至っていない．本節では，今後我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際の課題について，国際クレジットカード・ブランドの事例を参照しつつ考察する．

4-3-1 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．発行済みのクレジットカードを IC カードに置き換えるとともに，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（ブランドなどが管理するインターチェンジ・ネットワーク，加盟店契約会社など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が，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，磁気ストライプ・カードと IC カードの混在を前提としたシステムの移行を進めている．カードの混在を可能とするシステムとは，磁気ストライプ・カードを磁気ストライプ・カードとして，IC カードを IC カードとして処理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移行では，少なくとも，先行してフル IC カード対応し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 [8, 9]．

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
⑤ カード発行機関ホスト・システムの IC カード対応
⑥ IC クレジットカードの発行

このように，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という手順が採用されており，IC カードが IC カードとして処理されないという状況が回避されている点がポイントである．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 [9]，世界の各地域におけるシステムの IC カード対応に関する期限を 2001 年以降に設定している [8]．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，アクライアリング・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が完了することになり，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・システムがフル IC カード対応となることになる．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 カードと磁気ストライプ･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と IC カード対応が可能となっている地域の混在が可能になっていることがわかる．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 [10)]．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明確にしている．

4-3-2 全行一斉移行を前提にした場合における問題点

全銀協仕様においては，フル IC カード対応となった時点でホスト・システムが IC カード認証を実行する形態を「基本形」に移行することを予定しており，2012 年度を目処に検討が進められている．現在は，「経過期間」と呼ばれる基本形への準備段階であり，ネットワーク及びホスト・システムが IC カード対応しておらず，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データ形式で行われることとなっている．

また，全銀協仕様では，経過期間中に発行される 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おり，ほかの金融機関がフル IC カード対応を進めるなか，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 カードはほか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・システムでは取扱いができなくなるなどの問題が発生する．そうした理由から，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，最後の金融機関の準備が整うまで移行できないことになり，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に留意する必要がある．リテール・バンキングの安全性を確保するためには，ほかの金融機関が 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．ただし，その場合には顧客の利便性が損なわれてしまうというデメリットがある．

4-3-3 フル IC カード対応に向けての課題

(1) サービス業務拡大における課題

現在，我が国の金融機関は，デビットカード取引やインターネット・バンキングなどの提供に伴い，直接の管理下にないエンティティやネットワークを利用したサービス業務を拡大しており，キャッシュカードを利用した取引を取り巻く環境の変化を考慮して安全対策の検討を行うことが求められる．例えば，リスク管理の考え方が異なる組織によって管理されるATM やデビットカード端末などを利用する場合，端末が不正に操作されるケースも想定した対策の実施が必要になる．また，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，偽端末の設置による IC カード，PIN，生体情報などの盗取を想定した対策も重要となる．

異なる組織の管理下にあるシステムと提携する場合にも，取引環境の変化に伴って想定す

べき脅威も変化することを考慮して必要な対策を検討することが重要である．仮に何らかの事件・事故が発生したとしても，そのほかのシステム（ほかのカード，ほかのサービス，ほかのシステムなど）に影響を与えないような仕組みも準備しておくことが重要である．発生した問題に対して責任の所在を明確にするために，カード所持者，金融機関，他組織の権限と責任の範囲を明確化し，対処方法に関して他組織と調整･合意しておくことが求められる．

(2) 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，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システム設計が望ましい．例えば，システム内で利用される暗号アルゴリズムの安全性は時間の経過とともに低下する筋合いにあり，いずれより安全性の高い暗号アルゴリズムへの移行を検討することが求められるようになる．そうした場合においても適切に対応できるように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 においては，オープンなネットワークにおいて生体認証を利用するための仕組み（ACBio：authentication context for biometrics）の国際標準案が ISO/IEC 24761 として審議されている [11]．現在我が国のリテール・バンキングにおいては，生体認証を実行する端末は ATM に限られているが，今後，直接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．ただし，現時点においてオフラインで生体認証が行われるとすれば，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できない．ACBio の基本的な機能は，ホスト・システムが生体認証の結果の正当性を判断するためのデータを提供しその検証を実行可能にするというものであり，ホスト・システムは生体認証に利用された装置の精度・品質に関する情報も入手できるように設計されている．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，こうした技術の採用の可能性も考慮するという意味での拡張性に配慮したシステム設計が有用であると考えられる．

■参考文献

1) 金融庁，“偽造キャッシュカード問題等に対する対応状況（平成 20 年 3 月末），”金融庁，2008.
2) 田村裕子・廣川勝久，“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，”金融研究，vol.26，no.s1，pp.101-127，日本銀行金融研究所，2007.
3) 全国銀行協会，“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.
4) 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.
5) ISO, “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.
6) 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，vol.25，no.s1，pp.73-131，日本銀行金融研究所，2006.
7) 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，pp.12-29，金融財政事情研究会，2005.
8) Visa, “Visa International Operating Regulations Chip Mandates and Liability Shifts,” Visa, 2006.
9) Visa International AP Region, “The Heart of Smart,” Visa, 2001.
10) 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.
11) 寶木和夫, “SC27（IT Security Techniques／セキュリティ技術）総会報告”, 情報技術標準 NEWSLETTER, vol.79，情報処理学会，pp.12-15，2008.