非接触インタフェース経由取引の技術とビジネスリスク管理の課題

ひろかわかつひさ
廣川勝久

要　旨

金融サービスにおけるリテール取引は、サービス内容や提供範囲の拡大、関係する技術の進展、関係法令の見直し等に伴い変化を続けている。最近の関係法令の見直しにおいては、「資金決済に関する法律」（資金決済法）が 2009 年 6 月に成立し、リテール取引の環境は新規参入等によるシステムの関係者の多様化を含めて、さらに変化していくとみられる。

技術面では、高度なセキュリティ機能の実現を目的とした IC カードの利用が目立つ。特に、非接触 IC カード（以下、コンタクトレス IC カードという）や一部の携帯電話に代表される非接触インタフェースを用いたリテール取引が注目を集め、高い利便性が評価されている。国内では、コンタクトレス IC カード等による電子マネーのサービスが拡大しているほか、海外では、携帯電話の非接触インタフェース機能の実装仕様に関するガイドラインを策定して携帯電話の利用場面を拡大しようとする動きもある。今後、非接触インタフェースを利用したリテール取引が拡大し、決済システムに及ぼす影響も大きくなる可能性が高いと考えられる。

本稿では、ビジネスリスク管理の視点から、非接触インタフェースをリテール取引で活用する際に留意すべき事項について検討する。非接触インタフェースに利用される技術の特徴等を概観したうえで、国内外の利用環境や運用方針を説明し、リテール取引の環境変化や情報セキュリティ技術をはじめとする技術環境の変化への対応が重要であることを説明する。また、具体的な運用事例の紹介も含め、非接触インタフェースの安全な利用への対応方針についても検討する。

キーワード：ビジネスリスク管理、リテール取引、非接触インタフェース、
IC カード、携帯電話

本稿の作成に当たって、東芝ソリューション株式会社の山田朝彦氏ならびに日本銀行システム情報局の中山靖司企画役から有益なコメントを頂いた。ここに記して感謝したい。ただし、本稿に示されている意見は、筆者個人に属し、日本銀行あるいは東芝ソリューション株式会社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個人に属する。

廣川勝久　日本銀行金融研究所テクニカル・アドバイザー
（E-mail: katsuhisa.hirokawa@boj.or.jp）

1. はじめに

近年、わが国のリテール取引において、コンタクトレスICカードや携帯電話を利用したサービスが注目を集めている。その代表的なサービスが電子マネーである。電子マネーは、普及の一途を辿っているIC乗車券で採用されているコンタクトレスICカードと同種の技術を活用し、現在さまざまな場面において利用可能になってきており、決済金額・決済件数ともに増加傾向を維持している（日本銀行決済機構局［2009］）。また、国内では携帯電話を利用したポストペイ方式の電子マネー等も提供されている。海外においては、携帯電話への非接触インタフェース機能の実装仕様に関するガイドライン[1]を策定することによって携帯電話の利用場面を拡大しようとする動きもあり、コンタクトレスICカードに加えて、携帯電話がリテール取引に利用されるようになる可能性もあるとみられる。

こうしたコンタクトレスICカードや携帯電話を用いた非接触インタフェースによるリテール取引は、事業者自身が主導するサービス内容や提供範囲の拡大、情報通信分野の関連技術の進歩に加えて、制度面からの変化に伴って今後も進展を続けていくものとみられる。2009年6月には、「資金決済に関する法律」（資金決済法）が成立し（金融庁［2009］）、今後、取引システムへの新規参入事業者等による関連サービスの提供が進む可能性があり、リテール取引の環境は関係者の多様化やサービスの多様化を含め、さらに変化していくとみられる。

既存の非接触インタフェースを利用したリテール取引は、今後、規模拡大に加え、サービスの多様化等も進展するとみられており、決済手段の1つとして長期的にセキュリティと利便性の適切なバランスを維持することができるサービスへの発展が望まれる。そのためには、サービスの提供者が、提供するサービスとその利便性を確保するために必要なセキュリティ機能を明確にするとともに、適切なビジネスリスク管理を行うための運用条件等を想定される環境変化も含めて検討することが求められる。

リテール取引システムの重要な構成要素であるコンタクトレスICカードには、カードに内蔵されたアンテナを介して外部からの電力供給を受けセキュリティ機能等を動作させていることから、その動作環境等による電力供給上の制約がある[2]。また、特定のニーズに対応するために処理時間の短縮を優先した実装においては、コンタクトレスICカードとして利用可能な電力がさらに制約を受ける。このため、具体的な実装によってはICカード（端子付き）と同レベルのセキュリティ機能の実現が困難な場合がある点に留意することが必要である。

1 GSM Association [2007] は、GSM（Global System for Mobile communications）仕様の携帯電話に非接触インタフェースを組み込む場合のガイドラインを策定している。

2 ここで、電力供給上の制約とは、用途に応じた通信距離において、カード内のアンテナのサイズ、端末等が作る磁場の人体への影響（例えば、心臓ペースメーカへの影響）等の条件から、より高度なセキュリティ機能の動作に必要な電力が確保できない状態をいう。

どのようなビジネスリスク管理を行うことが望ましいか、また、どのような点に留意してそうした管理を実施すればよいかについて、非接触インタフェースを利用するという観点からは、これまでの公表文献においてはあまり議論されていなかったようである。その背景として、従来コンタクトレスICカード等の非接触インタフェースを利用した取引がそれほど活発ではなかったという事情もあろう。ただし、リテール取引におけるビジネスリスク管理という点では、既存のキャッシュカードやクレジットカードと同様の考え方を適用することが可能である。例えば、クレジットカードにおいては、セキュリティ確保に利用している暗号技術等の技術動向をどのように取引システムに反映させていくか、決済金額に応じたビジネスリスクをどのように管理するかといった点について検討が行われ、その成果が実際のサービス運営に反映されている。コンタクトレスICカード等の非接触インタフェースを利用するリテール取引においても、ビジネスリスク管理を適切に行っていくうえで、上記のような既存のリテール取引における考え方を適宜活用していくことが重要である。

こうした問題意識に基づき、本稿では、わが国において近年注目を集めている非接触インタフェースを利用したリテール取引におけるビジネスリスク管理のあり方について議論する。まず、2節において、取引システムにおける非接触インタフェースの利用箇所を確認し、3節において、非接触インタフェースの技術的特徴とその標準化動向を概観するとともに、セキュリティ機能の観点からICカード（端子付き）とどのような違いが存在するかを明確にする（ただし、より具体的な説明は補論1、補論2で行う）。そのうえで、4節において、求められるビジネスリスク管理についての知見を得るために、海外におけるサービス事例を取り上げ、ビジネスリスク管理としてどのような対応がなされているかを説明する。さらに、5節においては、ビジネスリスク管理上のポイントおよび課題として、サービスや関連技術の環境変化への対応方針をあらかじめ検討しておくこと、最新の技術動向をフォローして環境変化をいち早く察知し、それらに基づいてビジネスリスクを再評価し既存の対応の有効性や新たな対応の必要性の確認につなげていくことが重要である点を強調する。

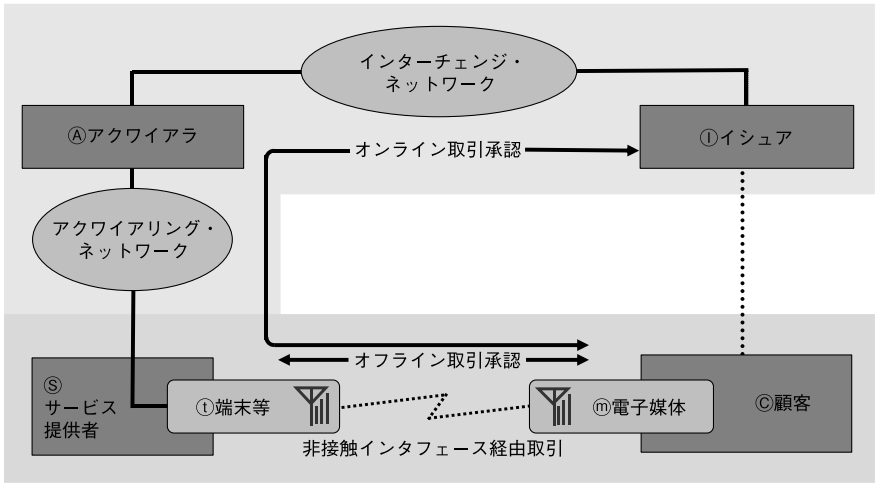
2. リテール取引における非接触インタフェースの利用

(1) 非接触インタフェースの利用箇所

一部のリテール取引システムでは、コンタクトレスICカードや携帯電話（おサイフケータイ®等の非接触インタフェース対応機能付き[3]）が利用されている。従来から使用されてきた磁気ストライプカード（以下、MSカードという）や、セキュリ

3「非接触インタフェース対応機能付き」は、携帯電話回線経由の通信以外にコンタクトレスICカードと同様の通信機能を持つことを示す。

図１　一般化したリテール取引システムの全体イメージ（例）と非接触インタフェース利用箇所



ティの向上を目的に導入されたICカード（端子付き）[4]は、その利用時に端末に挿入したりカード読取部分に通したりする必要がある。これに対して、コンタクトレスICカードや携帯電話（非接触インタフェース対応機能付き）は端末にかざすのみで処理が可能である。本稿では、これらをまとめて非接触インタフェースと呼ぶ。図1は、一般化したリテール取引システムの全体像の例である。同図には本検討の対象である非接触インタフェースの利用箇所を図示している。

ここでは、キャッシュカードがデビットカードとしても使われる場合のように、利用環境がカード発行者の直接管理下にはない状況も考慮するため、主要な関係者として以下を想定する。

Ⓘ　イシュア（カード発行銀行［issuing bank］、カード発行会社［card issuer］等）
Ⓐ　アクワイアラ（提携銀行［acquiring bank］、加盟店契約会社［transaction acquirer］等）
Ⓢ　サービス提供者（銀行自身、加盟店／インターネット仮想店舗運営者等［Service Provider］）
　– サービス提供者はⓣ端末等（ATM、銀行端末、店舗端末／仮想店舗システム）を用いる。

4 ICカードには「ICカード（端子付き）」と「コンタクトレスICカード」がある。一般に用語としての「ICカード」には、前者の意味で用いられる場合と後者を含む総称の意味で用いられる場合とがあるが、本稿では前者の意味で用いる。ただし、特に端子付きであることを明確に示すことが適切な場合は「ICカード（端子付き）」とする。

Ⓒ 顧客（口座保有者、カード所持者、利用者等［customer、account holder、card holder］）
– 顧客はⓜ電子媒体（IC カード、コンタクトレス IC カード、携帯電話等）を用いる。

上記のⒾ～Ⓐ間にはインターチェンジ・ネットワーク（銀行間ネットワーク、カード会社間ネットワーク等）が、Ⓐ～Ⓢ間にはアクワイアリング・ネットワーク（ATM ネットワーク、加盟店端末ネットワーク等）が存在する。本検討においては、顧客が保持する電子媒体としてコンタクトレス IC カード、携帯電話（非接触インタフェース対応機能付き）、および、それらと通信を行う端末等との間に適用する非接触インタフェース技術に着目する[5]。なお、用途や利用者を限定して運用されるリテール取引においては、電子媒体から読み出された利用者を特定するための情報を用いて（電子媒体中で取引ごとに変化する取引承認用の情報を生成することなく）運用上の管理が可能であることを前提に、コンタクトレス IC カードや携帯電話以外に RFID タグ[6]が電子媒体として利用される場合もある。

なお、エンティティとしてのイシュアは、他のイシュアに対して、あるいは、自身に対してアクワイアラとしての取引処理を行う場合もあるが、論理的には別のエンティティによる処理と考えられる。

(2) 非接触インタフェース経由取引の事例

リテール取引への非接触インタフェースの主な適用事例として電子マネー等が挙げられる。「最近の電子マネーの動向について（2008 年度）」（日本銀行決済機構局［2009］）によれば、国内の主要電子マネーの決済件数・決済金額は「電子マネー元年」と呼ばれた 2007 年度以降も増加を続け、発行枚数も 2009 年 1 月に 1 億枚を超えている。国内で普及が進んでいる電子マネーではコンタクトレス IC カードが用いられている。また、携帯電話（非接触インタフェース対応機能付き）によるサービス（おサイフケータイ®等）もある。あるいは、各種のポイントサービスにこれらの非接触インタフェースが利用されていることも多い。

こうしたサービスにおいては、各関係者がそれぞれのメリットを享受している。顧客（利用者）は、例えば、財布から電子媒体（コンタクトレス IC カード等）を取り出さずにそのまま端末等にかざすのみでサービスの提供を受けることが可能であり、使い勝手のよさという意味での利便性等を享受している。サービス提供者は、そうした顧客の利便性向上によって、サービスの利用頻度の高まりによる売上増や取引

5 図 1 のⓈ～Ⓒ間には無線 LAN 経由のインターネット接続や携帯電話による接続（ショート・メッセージング・サービスを利用したものなど）もあるが、これらはコンタクトレス IC カードあるいはその隣接技術とは異なる分野の技術と位置付けられている。

6 RFID タグは物品管理等で用いられている、無線通信によって内部に記憶された ID 情報の読取りを行うタグである。コンタクトレス IC カードと同じ周波数帯を用いるものもある。

処理時間の短縮によるコスト減をもたらす効果を期待していると考えられる。また、結果的に保守の負担が少なくなるという副次的なメリット[7]も存在すると考えられる。

銀行業務においては、非接触インタフェース経由でのサービスは従来とは異なる位置付けのアプリケーションとして認識される傾向がある。例えば、全銀協 IC キャッシュカード標準仕様（以下、全銀協仕様という）ではコンタクトレス IC カードの使用を認めていないほか、全銀協仕様が参照している EMV 仕様[8]（国際クレジットカード・デビットカードの業界標準）においても、コンタクトレス IC カードはオプションの位置付けであり、その使用は条件付きである。このように、銀行業務やクレジットカード・デビットカード業務においては、非接触インタフェース経由での取引の取扱いについてはまだ慎重な対応がなされているといえる[9]。

(3) 非接触インタフェース経由取引における処理内容とセキュリティ

現在提供されている非接触インタフェースを利用した取引システムには、さまざまな形態が存在している。例えば、当初からコンタクトレス IC カードを用いるシステムとして新規に開発されたもの、既存の IC カード利用システムへのオプションとしてコンタクトレス IC カードを追加したもの、電子媒体と端末間を非接触インタフェース化し、端末から先は既存の MS カード利用システムをそのまま利用するもの[10]などがある。

これらのシステムにおける非接触インタフェースの利用時には、上記のようなシステム的な差は意識されないと考えられる。しかし、システム全体としてのセキュリティ機能の観点からは次のように大別することができる。すなわち、①非接触インタフェースの利用が、単に MS カードを置き換える目的で固定情報を読み取るために使われている場合と、② IC カード（端子付き）と同様に暗号技術等に基づくセキュリティ機能の提供を目的とする場合である。

上記①には、既存のリテール取引システムのうち、MS カードを前提に構築された後に IC カードが追加されるかたちで現在に至っているものなどが該当する。このようなシステムでは、MS カード上の磁気記録媒体に記録された固定情報を読み取

7 端末等のカード対応部分に機械的な可動部分がないため保守の負担が少なくなると考えられている。

8 EMV 仕様（EMV Specifications）は、IC カード（端子付き）を前提にクレジットカード・デビットカードのビジネスリスク管理を高度化するため、IC カード内での暗号処理をも含めた仕様として 1996 年に公表された。当初 Europay、MasterCard、Visa の 3 国際ブランドが仕様を策定したが、現在は Visa、MasterCard、JCB、Amex が改訂を含めた同仕様の管理を行っている。EMV 仕様は、公表後、技術革新と運用経験を反映して改訂され、フランス等を中心に普及が進んでいる。国内においても IC クレジットカードの発行が進められているほか、全銀協仕様も本 EMV 仕様を参照している。オプションとしてのコンタクトレス IC カードの利用は、それを利用する国際ブランドが運用基準（Operating Regulations）を定めて試行している段階である。

9 2009 年 11 月に発表された「EMVCo Common Contactless Terminal Roadmap」（EMVCo [2009]）では 3 つのフェーズに分けてセキュリティ機能のレベルアップを前提にした対応計画が示されている。

10 チャージ不要の電子マネーのイメージで紹介されている、おサイフケータイ®等を使ったポストペイ方式の電子マネー等の例がある。

り、取引情報の一部として用いているという特徴がある。

これに対し、上記②に該当するシステムでは、IC カードに内蔵されたマイクロコンピュータが取引の可否判定および事後確認のための制御と暗号化情報の生成を行い、これをシステム全体で利用しているという特徴がある。この暗号化情報は当該取引に固有の情報となるように仕様が定められており、暗号化情報の利用という点で相対的に高いセキュリティを実現可能といえる。

こうした点を踏まえ、コンタクトレス IC カードを用いた電子マネーのシステムをみると、コンタクトレス IC カードと端末等との間で当該取引に固有の暗号化情報を生成し交換しており、単なる MS カードの置換えではなく IC カードのセキュリティ機能を活用した取引システム（すなわち上記②の場合に相当する）といえる。ただし、IC キャッシュカードや IC クレジットカードと比較すると、電子マネー・システムの通常取引では本人確認を行わないため、ビジネス上のリスク管理条件が異なっている。

一方、携帯電話（非接触インタフェース対応機能付き）を用いた一部の取引システムでは、MS カードに相当する情報を携帯電話から対応端末に送信することによって取引を行う（すなわち上記①の場合に相当する）ものがある。この場合、電子媒体と端末等との間の通信が適切に保護されている[11]限りにおいて、取引システム全体としてのセキュリティは MS カードベースのシステムの場合と同等であると考えられる。

このように、外見上は同等にみえる非接触インタフェースではあるが、システム全体として実現されるセキュリティ機能が大きく異なる場合がある。非接触インタフェースの影響を考える際には、既存の利用環境がすべて非接触インタフェースで置換え可能と考えるのではなく、既存の取引システムのどの機能が非接触インタフェース経由で処理されるべきかを適切に理解する必要がある。

3. 非接触インタフェースの技術的特徴および標準化の動向

(1) IC カードと非接触インタフェース

一般にコンタクトレス IC カードと呼ばれているものには、主要なものとして、異なる国際標準に対応した 2 種類がある。すなわち、① IC カード（端子付き）の非接触インタフェース化を意図して標準化されたインタフェース技術[12]を実装し、IC

11 MS カードに相当する固定情報が、電子媒体と端末等との間の暗号化された通信によって伝送されるケースである。

12 ISO/IEC 14443 Identification Cards—Contactless Integrated Circuit(s) Cards シリーズでタイプ A、タイプ B として標準化されているインタフェース、伝送プロトコル等。この国際標準では、ISO/IEC 7816 Identification Cards—Integrated Circuit(s) Cards シリーズで標準化された IC カード（端子付き）と共通の上位レイヤー（内部ファイル構造・セキュリティ機能等）の実装を想定している。

カード（端子付き）と共通の内部ファイル構造・セキュリティ機能等を有するものと、② NFC（Near Field Communication、近距離無線通信）として標準化された通信技術[13]をカードに実装し、上記①とは細部が異なる内部ファイル構造・セキュリティ機能等を有するもの（以下、NFC カード）がある[14、15]。

クレジットカード・デビットカード・キャッシュカード等のリテール取引の分野では、既存のサービスである MS カード取引における偽造カード等への対策として、IC カード（端子付き）を用いたサービスが導入されている。また、クレジットカード・デビットカードでは取引条件等を限定しつつもコンタクトレス IC カードの利用が始められている。一方、電子マネー・ポイントシステム等では、コンタクトレス IC カードあるいは上記の NFC カードによる非接触インタフェースを用いたサービスが提供されている。

これらの IC カード（端子付き）およびコンタクトレス IC カードでは、そのセキュリティ機能を動作させるための電力をカードの外部から供給しているため、次の(2)(3)に示すような電力供給にかかわる技術的特徴と課題がある。

(2) コンタクトレス IC カードへの電力供給

これらのカードでは、内蔵された電子回路（IC）に取引システム全体のなかでカードが分担すべき機能が実装され、カード外から供給されるエネルギー（電力）を受けて動作している。IC カード（端子付き）では、端末等への挿入によって端子を介して端末内の電源とカード内の IC が接続され必要な電力が供給される。それに対して、コンタクトレス IC カードでは、端末等に内蔵されたアンテナから供給されるエネルギー（磁場）をカード内のアンテナで受け、このエネルギーを IC の動作に必要な電力に変換して供給している[16]。アンテナのサイズ等は変換可能な電力に関係するがカードへの内蔵を前提にすることからサイズ上の制約があり、端末等が作る磁場には人体への影響（例えば、心臓ペースメーカへの影響）等も考慮する必要があることからその強さに制約がある。このため、コンタクトレス IC カードは IC カード（端子付き）よりも利用可能な電力に制約を受ける環境にある。

13 ISO/IEC 18092 Telecommunications and Information Exchange between Systems—Near Field Communication—NFCIP-1 等。この国際標準では、上位レイヤー（内部ファイル構造・セキュリティ機能等）に関する実装上の想定はない。

14 コンタクトレス IC カードの技術的特徴については補論 1 で補足する。

15 コンタクトレス IC カードとその隣接技術に関する標準化の動向については補論 2 に概要を紹介する。

16 コンタクトレス IC カードへの電池内蔵は不可能ではないが、キャッシュカードあるいはクレジットカードと同一の形状・寸法を前提にする場合、外部から電力を供給する方式が実用化されている。

(3) コンタクトレス IC カードの消費電力

カードに内蔵された IC の消費電力は実装される回路の増大や複雑化・内部動作の高速化に伴い増大するが、いずれの場合もカードとしては端末等から供給されるエネルギー（電力）の範囲内で動作しなければならない。この条件は、半導体技術の進展に伴って IC の動作に必要な電力が低減していくなかにあっても、搭載可能な暗号アルゴリズムや関連するセキュリティ機能を限定するなどの実装上の制約につながる。カードに求められる機能と処理速度を実現するために、例えば、実装する暗号アルゴリズムの処理に適した専用回路を加えると、その回路の追加によって消費電力が増加する。一方、処理時間の短縮が求められる場合、内部動作の高速化が必要になり、それによって消費電力が増加する。

コンタクトレス IC カードでは、上記のような消費電力の増加の割振りをその利用目的と利用可能な電力に応じて定める必要があり、そのために実装する機能あるいは処理速度を個別に最適化する。例えば、アプリケーション上の要求に基づいて短い処理時間が求められる場合には、必要な処理速度を実現するために内部動作の高速化を優先するとともに可能な範囲での専用回路の追加等が検討される。具体例としては、当初、交通サービスを目的にスタートした国内の交通系電子マネーでは、利便性の観点から特に高速処理を重視する必要があった。国内の交通システムではラッシュ時における改札ゲートでの連続した利用者の通過に対応するため、海外の同種のサービスよりも非常に高速な 0.1 秒の処理時間が求められている。このため、要求された高速処理に伴う消費電力の増加が供給可能な電力を超えない範囲で最大限のセキュリティ機能を搭載した製品が使用されている。

一方、ATM 取引等においては、より高いセキュリティ機能の搭載によって取引システム全体としてのビジネスリスクを抑えることが重視されるため、より暗号強度を高められる RSA 用追加回路等を実装した IC カード（端子付き）が用いられている。

4. 国内外の取引環境・運用方針の相違

(1) 取引の種類と取引金額等の範囲

リテール取引において取引可能な金額の範囲は、取引システムが提供するサービスの種類に応じて設定されている場合が多い。例えば、キャッシュカードでは、金融機関によって口座別に定めた 1 回当たりの引出し限度額や、一定期間内の総引出し額の上限が定められているのが普通である。ただし、いずれの場合も原則として口座残高の範囲内である[17]。キャッシュカードでは、他の取引形態とは異なり基本的に全件オンライン承認を想定しているため、取引金額によってビジネスリスク管

17 自動融資サービスがついている場合は残高を超える引出しが可能である。

理の条件（例えば、オンライン承認かオフライン承認か）が変化することは想定されていない。ただし、IC キャッシュカードの導入や生体認証の追加等、なりすましの困難さのレベルに応じて、MS キャッシュカードでの取引時とは異なる上限額を設定するなどの運用を行っている。

クレジットカードでは、信用照会の条件に取引金額が含まれ、他のビジネスリスク管理の条件とあわせてオンライン承認かオフライン承認かが決定されるとともに、一定期間内の与信限度が設定されている。

これらに対して、電子マネーでは、個々の電子マネー・システムによって取引ごとの上限額が定められることが多いが、国内ではカード内残高いっぱいまでの取引を可としている。

一方、海外では、クレジットカード > デビットカード > 電子マネーの順に取引金額の上限が低くなるように設定されている。個々の取引システムによって具体的な取引金額の範囲は異なっている。

(2) 小額取引のイメージに関する国内外の相違

イ．相対的に高額取引が可能なわが国の実情

本節(1)において取引の種類によって取引金額の範囲に差があることを示したが、これはビジネスリスク管理上、取引の真正性確認のためのプロセスや使用する設備環境等にかけられるコストの差を背景としている。通常、ビジネスリスク管理のための設備投資とその運用に伴う処理費用は、事業として提供するサービスのなかで吸収することが必要になる。そのため、高度なセキュリティ機能を前提にした設備と運用による処理を行う場合は、その処理料金が高額となる結果、小額取引には利用されないこととなる。一方、高額の取引を想定したサービスについては、その取引が真正であることを高いセキュリティ・レベルで確認し、ビジネスリスクの増大を抑えることが求められる。高いセキュリティ・レベルでの確認がコスト的に困難な場合、取引を小額の範囲に制限して取引ごとのビジネスリスクを抑えることが考えられる。このような背景から、取引の種類やそれに適用されるセキュリティ管理の内容に応じて取引金額の範囲を制御することが求められる。

海外における小額取引の上限金額は、日本円換算で 2,000～3,000 円程度が世界の共通認識であるとみられる。具体的には、汎用目的の電子マネー、デビットカードに関しては、25 米ドル、25 カナダドル、15 ユーロ、10 ポンドが小額取引の上限金額として設定されている。特定用途に限定した場合や会員制により利用者の特定が容易な場合等は、個々のビジネスケースとして上記の金額例を超えた取引を認めるサービスも存在している。

これに対して、わが国の場合、汎用目的でオープンな取引システムにおいて上記の金額例を遥かに超える数万円程度の取引が可能となっている。これは、わが国の社会が安全であることを示すものとして評価することができる反面、海外からの攻

撃者にとっては、攻撃成功による見返りが相対的に大きいという意味で魅力的な攻撃対象とみられてしまう危険がある。

以下では、英国と米国・カナダにおける小額取引の運用事例を紹介する。

ロ. 英国の Barclaycard における事例

前述のとおり、クレジットカードやデビットカードのシステムは MS カードをベースに構築され、後に IC カード（端子付き）への対応が加えられたほか、オプションとしてコンタクトレス IC カードの追加が行われている。そのため、コンタクトレス IC カードを使用した場合も、基本的には IC カード（端子付き）を使用した場合と同様のリスク管理が行われるが、その内容は国際クレジットカード・デビットカードの業界標準である EMV 仕様に基づいている。

こうした状況下、英国の Barclaycard は、ロンドンにおいて 3-in-1 Card のサービスを提供している[18]。3-in-1 Card は、1 枚の IC カードに IC カード（端子付き）とコンタクトレス IC カードを実装し、IC クレジットカード、コンタクトレス IC デビットカード、交通専用コンタクトレス IC カードの 3 機能を提供するものである。IC クレジットカード機能は、EMV 仕様に準拠した IC カード（端子付き）で実現されている。PIN（暗証番号）入力による本人確認を行い、後述の小額取引以外をサービス対象とする、全世界で共通利用が可能なクレジットカード機能を提供している。コンタクトレス IC デビットカード機能は、EMV 仕様のオプションであるコンタクトレス IC カード（ISO/IEC 14443 シリーズ準拠）による小額取引に限定したサービスを提供する。PIN の入力やサインを求めることなしに取引が可能であるものの、英国発行の IC カードに限定されている。ここで小額取引とは、10 ポンドを上限と定め、“Sandwich for lunch” あるいは “Pint of beer” のためのサービスとして紹介されている。交通専用コンタクトレス IC カードについては、ロンドンの地下鉄と一部の郊外電車とバスの利用に特化した交通用途限定のコンタクトレス IC カードであり、日本国内のように交通系電子マネーが一般の店舗等でも利用可能な環境は提供されていない。

このように、取引金額に応じたサービスと認証方法の切替えによってビジネスリスクを制御している。

ハ. 米国・カナダにおける Visa Operating Regulations の事例

Visa USA と Visa Canada が定める Visa Operating Regulations のなかには、コンタクトレス IC デビットカードについて次のような運用例がある（Visa U.S.A. Inc. [2008]、Visa Canada Inc. [2008]）。すなわち、オプションとして認められている非接触インタフェース経由の取引において、取引の金額が米国では 25 米ドル、カナダでは 25 カナダドルを上限として定めている。

18 本サービスについては、Barclaycard の関連サイト（http://www.barclaycard.co.uk/personal-home/cards/one-pulse/index.html）等において紹介されている。

ただし、オフラインでの取引承認のため、指定された仕様に従った取引ごとの暗号化情報生成とその確認を必須としており、その前提のもとに、PIN 入力またはサインを求めないこと、レシートの発行を省略可とすることを認めるとしている。これは、小額取引までを含めてオンライン取引承認を行う場合のコストとビジネスリスクとのバランスに基づき設定された条件であると考えられる。

5. 非接触インタフェース経由取引の環境変化とリスク管理上の課題

(1) ビジネスリスクにかかわる取引環境の変化

本節では、前節で紹介した海外のビジネスリスク管理の事例を踏まえつつ、リテール取引の環境変化に伴うリスク管理上の課題を検討する。ビジネスリスクにかかわる取引システムの環境変化の例としては、

- ➢ サービス内容の変更
- ➢ サービス提供範囲の拡大
- ➢ 関係機関・関係者の変化
- ➢ 利用技術・関連技術の進展
- ➢ 法制度等を含む社会環境の変化

などがある。これらの変化は意図して生じさせる場合と意図されずに生じてくる場合があるが、特にサービスの内容や提供範囲が変化する場合は使用する利用技術・関連技術も変化する可能性があること、それらの技術を取り巻く環境は常に変化を続けていること、システムを運用する側とシステムを攻撃する側との技術的バランスも変化を続けるものであることを理解したうえで、適切なリスク管理を図っていく必要がある。

非接触インタフェースの利用は利便性を変化させるが、それ自体が上記環境変化の大きな要因の 1 つであると考えられる。

非接触インタフェース経由取引の利便性が高いことは共通の認識になっていると考えられるが、その利便性は「電子媒体を取り出して端末等に挿入する必要がない」「PIN 入力やサインを求めない」「オンラインの取引承認を行わない」「特に必要な場合以外はレシート（取引記録）を出力しない」ことなどによって発生していると考えられる。

一方、非接触インタフェース技術を利用しない取引環境では、「電子媒体を取り出し端末等に挿入する」「PIN 入力またはサインを求める」「必要に応じてオンラインの取引承認を行う」「レシートを出力する」ことなどを前提にしたシステム構築が行われている。これらは、「利用者が取引の意思を表示する」「正当な利用者であるこ

とを確認する」「イシュア（またはその代行者）が取引の可否を決定する」「利用者に対してレシートを発行する」ことなどによって、当該取引の正当性確認や取引にかかわる疑義発生時の詳細な検証を可能にしている。

こうした処理は、リテール取引システムにおける既存の事例・事故に基づき、リスク管理の必要性から実装されているとみられる。上記機能の一部や全部を省略する場合、利便性の向上と当該機能の運用にかかわるコストの軽減が可能になる反面、省略された機能によって従来対策されていた事故等の発生防止が困難になる場合がある。こうした機能の省略による利便性の向上と損害発生のリスクの増大をどのようにバランスさせるかは、個々のシステムごとに異なる。

例えば、IC カード（端子付き）を前提とする取引システムにおいて、利便性の向上を意図してコンタクトレス IC カードを導入すると上記のリスク管理上の処理の一部が機能しなくなるという環境変化をもたらすことに注意が必要である。

(2) サービスの変化・拡大と環境の変化

どのような取引システムであっても、当該システムが当初計画されたときの環境に長期間とどまっていることは稀である。本節(1)の冒頭に示したように、技術的条件が変化する場合や、ビジネスの拡大を意図してサービスの範囲や内容を積極的に変化させ拡大しようとする場合が考えられるほか、資金決済法等の法令改正に伴って変化を求められる場合も想定される。そのような状況の例として、以下が挙げられる。

- キャッシュカード：ATM 専用カードへのデビットカード機能の追加
- クレジットカード／デビットカード：ハウスカードから国内カード、国際カードへ
- 交通系電子マネー：交通用途限定から駅ナカ交通用途外利用、街ナカ汎用へ

これらの環境変化は、事業者（イシュア）の管理下にある環境でのみの利用から、イシュアの管理外の部分を含む環境での利用への拡大を意味している。イシュアの直接管理下にない利用環境を含む例としては、インターネット・バンキングや EC／インターネット・コマースがある。これらは、直接管理下にある端末や一般の加盟店が保有する端末等の管理とは大きく異なり、その利用環境の管理状況の確認は物理的にも困難であると考えられる。

(3) 意図された環境変化への対応

サービス範囲の拡大は、一般にビジネス上歓迎される一方で、ビジネスリスクを変化させる可能性があることに留意する必要がある。イシュア自らの意思によってサービス拡大を行う場合は拡大後の環境について分析・考察を行う必要がある。安

易に拡大後の環境も拡大前と同一であるとした場合には、潜在する新たなリスクへの対策が講じられない状態になる危険がある。

具体的には、サービス提供範囲の拡大が取引システムに含まれる利用環境を変化させ、例えば、管理者が単一機関から複数機関になる状況や、場合によっては管理者不在の状況に至るケースがある。例えば、キャッシュカードが銀行の ATM でのみ利用される場合、ATM の管理状況の把握を当該銀行は確実に行うことができるであろう。しかし、同じカードがデビットカードとして使われる場面では、その利用環境について ATM と全く同じレベルの確認を行うことは困難である。用途限定の電子マネーが汎用化する場合も同様であろう。

前節で紹介した英国の 3-in-1 Card では小額取引をサービスに追加することによって利便性を拡大しているが、通常の IC クレジットカード取引では必須の本人確認を行わない代わりに、用途と取引金額を限定することで異なる取引環境におけるビジネスリスクを管理している。

重要なポイントは、当初想定した利用環境（システムの計画時・開発時の想定環境）と現実の利用環境、あるいは、サービス拡大後の利用環境との間にリスク管理上の条件について整合性が維持できているか否かを確認することである。例えば、サービスの拡大によって、取引の正当性確認に必要な処理、顧客の利用の意思の確認に必要な処理、関係者の権限と責任の範囲等に変化を生じることが考えられる。こうした変化を読み取ってリスク管理を適切に実施できない、あるいは、制御できない場合には、取引システム自体の破綻やビジネス自体に対する評価・信頼の低下を招く可能性が高まる。

想定される追加リスクがビジネス上重大なインパクトをもたらす可能性がある場合には、システムの機能を改善しリスクを回避できるようにするか、軽微なリスクに抑えるように運用条件等を調整しなければならない。

(4) 意図せざる環境変化への対応

リテール取引システムでは、サービスの拡大を全く意図していない場合においても、情報技術や社会の動向によってシステムを取り巻く環境が変化していくことがある。例えば、コンピュータの性能向上が結果として攻撃者に有利な環境を提供することになり、暗号機能の強度が相対的に低下していく場合がある（例、「暗号アルゴリズムの 2010 年問題」）。

このような問題については、提供しているシステムの定常的な運用以外に、社会環境の変化やそこに使われているセキュリティ関連技術の研究動向・実用化動向等をモニターし、システムのリスク管理にどのような影響が生じうるかのレビューを行う必要がある。そうしたモニタリングやレビューを個々のイシュアが単独で行うことは困難な場合が多いが、業界としての取組みが行われている場合はそれに従うという方法がある。

例えば、前述の EMV 仕様では、暗号アルゴリズムとして 2-key Triple DES と RSA を使用している。これらの暗号アルゴリズムの危殆化に対しては既に後継の暗号アルゴリズムが検討されているが、EMV 仕様に基づく IC クレジットカード・IC デビットカードは全世界での相互利用を前提にしているため、具体的な移行の時期等について引き続き検討が進められている。EMV 仕様は、その初版から、暗号アルゴリズムやその利用方法について、識別情報等を用いて必要な切替えを可能とするように構成されているほか、サービスを中断することなく安全な鍵長への移行を可能にするため、異なる鍵長を用いて発行された IC カードを同一の端末で利用可能とするように端末内部では複数の鍵長をサポートし、その世代管理を行っている。既に利用中の RSA については利用する鍵長の安全性について鍵長ごとの利用可能期間が定められ、毎年の定期レビューによってその見直しが行われている。

最近では、IC カード（端子付き）の利用を基本とする EMV 仕様に、オプションとしてのコンタクトレス IC カードの利用を追加している。ただし、前述のようにコンタクトレス IC カードでは実装可能なセキュリティ機能に制約を生じる場合があるため、全体システム中のカード以外の部分による管理あるいはサービス提供範囲の管理等による対応[19]を行いつつ、長期的には実装するセキュリティ機能を強化した後に国際レベルの共通利用を進めることが計画されている。このように非接触インタフェースの活用に際しては危殆化への対応をより慎重に行う必要があると考えられる。

(5) 環境変化への対応メカニズム

固定的な構造のみでシステムが構築されている場合は、最悪のケースでは新しく高度化したシステムの構築を強いられて既存システムから移行しなければならない（既存システムを放棄せざるを得ない）場合も生じる。そのような残念な結果となった事例は国内外に存在する。

その一方で、リスク管理機能の向上を見込んだシステム構築が行われたケースにおいては、システムの全面入替え等を行うことなしに、より高度なリスク管理を行いつつシステムの運用を継続できた事例も多く存在している。以下では、環境変化へのシステム対応について、イ. ではシステムの入替えをせずに済んだ事例、ロ. とハ. ではシステムの入替えが必要になった事例を紹介する。これらの事例は環境変化への対応メカニズムの重要性を示している。

イ. ドイツの ATM における暗号方式一斉切替えの事例

古い事例ではあるが、1997 年頃にシステムの入替えなしにレベルアップを実現した事例である。ドイツでは国内の ATM で当初は Single DES を暗号機能として用い

19 カード以外の部分による管理としては取引記録の分析による異常取引の検出とブラックリストへの反映等、サービス提供範囲の管理としては用途の限定等がある。

ていたが、暗号アルゴリズムとしての安全性低下に対応して 2-key Triple DES への移行が必要となった。その際に、国内の ATM とそのネットワークに用意されていたプログラムのダウンロード機能を活用して、各 ATM 内の暗号機能を Single DES から 2-key Triple DES にきわめて短期間に移行することができた。

ロ．オランダのコンタクトレス IC カードに対する攻撃の事例

システムの入替えを計画せざるを得なくなった事例も存在する。2008 年に、オランダのナイメーヘン・ラートボウト大学（Radboud University Nijmegen）の研究グループ等が同国内で使用されている交通系コンタクトレス IC カードの内部構造を解析し、そこに実装されていた暗号アルゴリズム（仕様非公開）を解読したほか、実験的に偽造カードの作成が比較的容易に実行可能であることを実証した（Gans, Hoepman, and Garcia [2008]）。これを受けて、オランダの鉄道では、同コンタクトレス IC カードのシステムをより安全性の高い暗号アルゴリズムを搭載したシステムに置き換える方針を決定している。

ハ．フランスの CB カードの事例

リスク管理に加えて国際的な互換性を高めるためにシステム全体を入れ替えた事例としてフランスの CB カード[20]とその利用環境がある。フランス国内では 2006 年末までに移行が行われた。これは 1992 年に導入されたフランス独自の IC カード国内仕様から国際 IC クレジットカード・IC デビットカードの業界標準である EMV 仕様への全面切替えを行ったものであるが、独自の国内仕様のセキュリティ機能が十分ではなくなったことが移行の大きな原因となっている。

(6) 非接触インタフェースの得失を考慮した活用

取引システムが安全に稼働するためには、その構成要素としての電子媒体をも含めて、必要とするリスク管理のための機能がシステム中の各部に適切に実装され処理されなければならない。非接触インタフェース機能を有する電子媒体はその利便性の高さから利用場面が広がっている。しかし、取引システムのなかで電子媒体は最も実装上の制約を考慮する必要のある部分でもある。特に取引処理を高速化する必要があるケースにおいては、電力供給上の制約を背景に、工業製品として低価格（低コスト）での高度なセキュリティ機能の実装が接触インタフェースに比べて困難な場合があり、暗号アルゴリズムの安全性低下をはじめとする利用技術・関連技術の進展の影響を相対的に強く受ける可能性がある点に留意する必要がある。

非接触インタフェースを有する電子媒体に期待するセキュリティ機能が実装困難な場合、電子媒体に実装可能な範囲のセキュリティ機能を前提に電子媒体以外の部

20 CB カードは、フランスの Groupement des Cartes Bancaires による銀行カードの統一ブランドである。

分のセキュリティ機能の強化や運用管理等によりシステム全体として必要なセキュリティ・レベルを実現しなければならない。そのようなシステム全体としての対策を講じることによってビジネス上のメリットを提供できリスクも管理可能であればよいが、そうでない場合は提供する利便性の範囲を制限することによって必要なリスク管理を行う必要があると考えられる。

具体的な考え方を示すシステム例として、EMV 仕様に基づく IC クレジットカード・IC デビットカードのシステムがある。EMV 仕様の取引システムではイシュア―アクワイアラ間で定めた金額に基づきオンライン取引承認の要否を制御している。非接触インタフェース経由で利用者の本人確認を行わない取引の場合等は、上記の金額を別の値（接触インタフェース経由時よりも低い値）に設定している。

また、同システムでは、実装可能な範囲でセキュリティ機能を搭載した IC カードを前提に初期のシステム構築を行う一方、その後の技術進歩によって搭載可能になるセキュリティ機能と増大するリスクとを考慮し、システム全体としてのセキュリティ機能のレベルアップを図るためのメカニズムを用意している。具体的には、IC カードの発行時に Application Interchange Profile と呼ばれるアプリケーション機能を示す情報が IC カード内に記録される。IC カード使用時にこの情報が読み出されて端末側の機能との対応関係が確認され、IC カードと端末が共通に利用可能なセキュリティ機能を決定する[21]。本節(4)で紹介した EMV 仕様における環境変化への対応では、このメカニズムによって、運用されている暗号アルゴリズムやセキュリティ機能を識別できるため、必要に応じてより高度な暗号アルゴリズムやセキュリティ機能への移行が可能になる。

このような移行のメカニズムによってセキュリティ機能を高いレベルに維持してリスク管理を行うことが可能であり、この考え方は非接触インタフェースにも拡大されていく。2009 年 11 月に EMVCo が発表した「EMVCo Common Contactless Terminal Roadmap」（EMVCo [2009]）では、既存のコンタクトレス IC カード利用システムの存在を認めつつ、今後の国際共通システムとしてオンライン取引承認専用の仕様を定め、その後、楕円暗号等の利用によってセキュリティを向上させたうえでオフライン取引承認も可能とするシナリオが示されている。

前述の非接触インタフェースの利便性とビジネスリスク管理の関係、コンタクトレス IC カードの技術的特徴とその課題（制約）等を考慮した取引システムの構築とその環境変化に対する継続的な対応が重要である。

21 Application Interchange Profile には Issuer Public Key Certificate Index があり、この Index から Issuer Public Key Certificate と Algorithm Identifier を確認することによって使用すべきアルゴリズムが特定され対応する処理が可能になる。

6. おわりに

本稿においては、リテール取引システムにおける非接触インタフェースの利用について、その利便性とビジネスリスクのバランスに関する検討を行った。

まず、非接触インタフェースの利用箇所を特定し、非接触インタフェースに利用されている各種技術とそれらの標準化動向を紹介した。非接触で外部からの電力供給を利用するコンタクトレスICカード等の場合には、供給可能電力の制約から実装可能なセキュリティ機能にも一定の限界が存在する可能性があり、運用条件等とどのように整合させるかが重要であることを説明した。また、そうした運用条件が非接触インタフェースによるリテール取引においてどのように考慮されているかについて海外の事例を紹介し、取引金額の上限を相対的に低く設定するなど、ビジネスリスク管理上の配慮がなされている点を説明した。

こうしたビジネスリスクの適切な管理は当該システムが社会に広く受け入れられる条件の1つであるが、現実には利便性優先のシステムとセキュリティ優先のシステムが存在しており、システムが置かれている環境によって利便性とセキュリティのどちらを優先するかが選択されていると考えられる。ビジネスリスク上の問題がない場合、あるいは、バックオフィス機能の活用や運用上の対策が可能な場合には、非接触インタフェースの利便性を活用することができる。

ただし、中長期的には、システムとして提供するサービス自体が変化するばかりでなくシステムが置かれている環境も変化するため、常にバランスが維持されうるかについてビジネスリスク管理上の見直しが必要である。コンタクトレスICカード等の非接触インタフェースの活用に当たっては、ICカード（端子付き）の場合に比べて制約された電力供給を前提にしたセキュリティ機能の実装等が行われることから、セキュリティ対策の陳腐化が進みやすい面がある点に留意する必要がある。そうした陳腐化への対応に関して、本稿で説明したように、既存の技術の研究動向をフォローするとともに、より高度なセキュリティ技術に移行しやすいシステムの構築や環境の整備を検討することが重要である。

今後、本稿で述べたようなビジネスリスクに対する配慮が十分に行われ、ユーザーのニーズに見合った非接触インタフェース経由でのリテール取引サービスが提供されるようになり、ひいては、長期的にも安全で効率的なリテール取引における決済手段の1つに成長することを期待したい。

参考文献

金融庁、『資金決済に関する法律（資金決済法）』、金融庁、2009 年

日本銀行決済機構局、「最近の電子マネーの動向について（2008 年度）」、『BOJ Reports & Research Papers』、日本銀行、2009 年 7 月（http://www.boj.or.jp/type/ronbun/ron/research07）

EMVCo, “EMV Specifications” (http://www.emvco.com/specifications.aspx).

EMVCo, “EMVCo Common Contactless Terminal Roadmap,” *Genaral Bulletin*, 43, EMVCo, November 1, 2009 (http://www.emvco.com/news.aspx?id=46).

Gans, Gerhard de Koning, Jaap-Henk Hoepman, and Flavio D. Gracia, “A Practical Attack on the MIFARE Classic,” 8th Smart Card Research and Advanced Application Conference (CARDIS 2008), March 15, 2008 (http://aps.arxiv.org/abs/0803.2285).

GSM Association, *Mobile NFC Technical Guidelines Version 2.0,* GSM Association, November, 2007.

ISO/IEC 7816 Identification Cards—Integrated Circuit(s) Cards シリーズ.

ISO/IEC 14443 Identification Cards—Contactless Integrated Circuit(s) Cards シリーズ.

ISO/IEC 18092 Telecommunications and Information Exchange between Systems—Near Field Communication—NFCIP-1.

ISO/IEC 21481 Telecommunications and Information Exchange between Systems—Near Field Communication—NFCIP-2.

Visa Canada Inc., *Visa Regional Operating Regulations CANADA*, November 15, 2008 (http://www.corporate.visa.com/pd/rules/main.jsp).

Visa U.S.A. Inc., *Operating Regulations Volume I—General Rules*, November 15, 2008.

補論 1. 非接触インタフェースの技術的特徴

(1) IC カード、コンタクトレス IC カードとその隣接技術

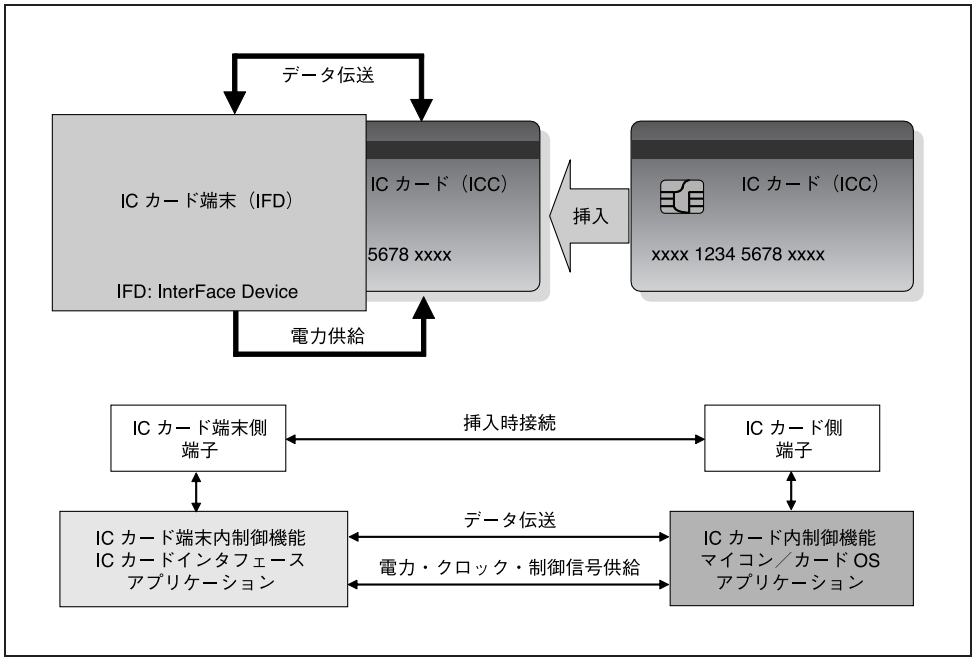
3 節でコンタクトレス IC カードおよびその隣接技術に基づく製品には、その動作に必要なエネルギー供給上の制約があることを示した。ここでは、その制約の背景を純技術的要因と特定のニーズに基づく製品化に伴う実装上の要因の両面からレビューする。さらに、その制約が IC カードの機能・性能にどのような影響を与えるかを概観する。

IC カード（端子付き）は、ワンチップのマイクロコンピュータをカードに内蔵し、それに接続されたカード表面の端子を通じて電力や制御信号の供給を受けるとともに、端子を通じて情報の入出力を行っている（図 A-1 参照）。

コンタクトレス IC カードは、マイクロコンピュータをカードに内蔵し、それに接続されたカード内のアンテナを通じてカード外からのエネルギー供給を受けて動作するとともに、情報の入出力を行っている（図 A-2 参照）。

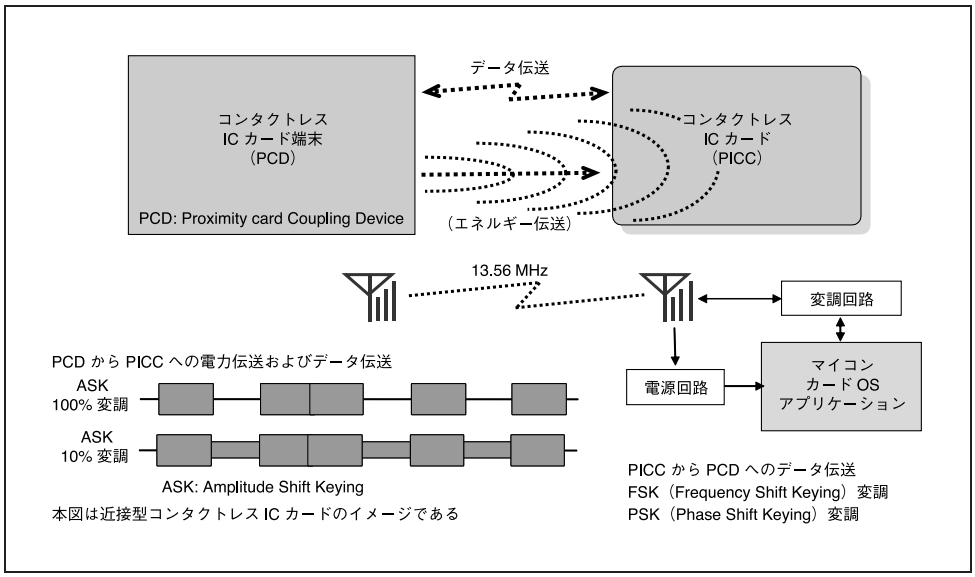
IC カード（端子付き）は、端末等から端子経由で電力の供給を受けるため、高機能化のための回路追加[22]や演算処理の高速化に必要な電力供給に大きな問題はない

図 A-1　IC カード（端子付き）の内部構造イメージ



22 高機能化のための追加回路としては、公開鍵暗号アルゴリズム RSA 用演算回路等があり、IC カード（端子付き）では既に実用に供されている。

図 A-2　コンタクトレス IC カードの内部構造イメージ



と考えられる。

一方、コンタクトレス IC カードは、端末等が作る磁場（磁界）をカードに内蔵されたアンテナ経由で電力に変換しており、内蔵されたマイクロコンピュータの動作環境に電力供給上の制約が生じ、高機能化のための回路追加や演算処理の高速化に制約が生じる場合がある。

コンタクトレス IC カードに隣接する非接触インタフェース技術として、NFC（Near Field Communication、近距離無線通信）がある。この技術はコンタクトレス IC カードと基本的に同じ磁場を前提にした通信方式であり、コンタクトレス IC カードに相当する動作モード（Passive Mode）と端末等に相当する動作モード（Active Mode）がある。一般にカード形状の場合は Passive Mode を、端末等の場合は Passive Mode と Active Mode を選択的に使用することができる。電源を内蔵していない場合[23]には上記コンタクトレス IC カードと同様の電力供給の制約に関する課題がある。

(2) コンタクトレス IC カード等の内部構造

イ. 主要な構成要素

コンタクトレス IC カード内の主要構成要素は、アンテナ、電源回路（IC）、変調回路（IC）、マイクロコンピュータ（IC）等である。これらは単一のチップに集積されているものが多い。アンテナは、端末等から供給される磁場のエネルギーを電源

23 一般にカード形状の場合には電源を内蔵していない。

回路に伝えるとともに、変調回路による端末等とカード間のデータ伝送のための信号授受に用いられる。電源回路（IC）は、アンテナで受けた磁場のエネルギーを変換して、マイクロコンピュータ（IC）の動作に必要な電圧や制御信号を生成し供給する。また、変調回路（IC）はマイクロコンピュータとアンテナを接続し端末等との間の通信を制御する。カード形状の Passive Mode の NFC も同様の要素で構成されている。コンタクトレス IC カード内のマイクロコンピュータは、通常の IC カード（端子付き）と同様に IC カードとしてのデータ管理やセキュリティ管理に必要な処理を行う。

ロ．コンタクトレス IC カードと端末等の通信

コンタクトレス IC カードと端末等との間の通信は、磁場に変調を加える（送信する信号に応じて波形等を変化させる）ことによって行われる。端末等からコンタクトレス IC カードに信号を送る場合は ASK（Amplitude Shift Keying）と呼ばれる変調方式が採用されているほか、その逆方向に信号を送る場合は FSK（Frequency Shift Keying）、PSK（Phase Shift Keying）と呼ばれる変調方式が採用されている。信号の伝送方向によって変調方式が異なることから、必要な場合は全二重通信も可能である。上記の変調方式に加えて符号化方式やビットの送出順序（最下位ビットから送出／最上位ビットから送出）にも複数の方式がある。これらの技術的条件については、国際標準が定められているほかに、業界団体の標準仕様も存在している。

コンタクトレス IC カードは、その所持者が世界各地に旅行する場合にも動作可能である必要から、各国の電波法上の制約を考慮し全世界で共通に利用可能な ISM Band（Industrial, Scientific and Medical radio bands）のうち 13.56 MHz 帯を使用している。この周波数は、コンタクトレス IC カードのほかに NFC と RFID タグの一部でも使われている。

（3）コンタクトレス IC カード等に期待される処理能力

前述のように、コンタクトレス IC カード（あるいは Passive Mode の NFC、以下同様）は端末等が供給する磁場から電力供給を得て動作しており、自ら動作環境をコントロールできないことによる実装上の制約が存在する。

コンタクトレス IC カード内のマイクロコンピュータは、その利用システムが要求するデータ管理およびセキュリティ管理等の処理を一定の時間内に完了させる必要がある。例えば、高度なセキュリティ機能を意図して複雑な処理を組み込む場合や、運用上定められた時間内に処理を完了させなければならない場合には、カード内部の動作速度を上げる必要があるが、その際に消費電力も増加することになる。こうした消費電力の増加を考慮しつつ、利用可能なエネルギー（供給可能電力）の範囲内で実装可能な回路規模と動作速度の制約のもとでコンタクトレス IC カードを製品

化しなければならない[24]。このように、利用可能なエネルギーの制約によって、IC カード（端子付き）の場合に実現可能である要件がコンタクトレス IC カードでは実現可能とはならない場合があることに注意が必要である。

システム全体からみれば、コンタクトレス IC カードと端末等との間の最大処理時間はシステムとしての運用条件によって決められる一方、コンタクトレス IC カードが分担すべきセキュリティ機能はシステム全体のなかでの機能分担に基づいて決定される。こうして決定されたセキュリティ機能を最大処理時間内に実現するように実装した場合、マイクロコンピュータの全消費電力が供給可能電力の範囲内に収まる場合は問題が生じないと考えられる。そうでない場合、例えば、次の対応が考えられる。

- ➢ 運用方法を再検討し、コンタクトレス IC カード内での処理のための最大時間を長くする。
- ➢ コンタクトレス IC カードに分担させるセキュリティ機能等を軽減する。
- ➢ 上記の両方を調整する。

ただし、これらの対応はシステム全体としての処理効率やビジネス上のリスク管理の考え方に影響を与えるという点に留意する必要があり、利用可能な非接触インタフェースの機能・性能がビジネスリスク管理上必要なセキュリティ機能を満足するか否かを確認することが重要である。

(4) コンタクトレス IC カード等におけるセキュリティ機能実装上の課題

コンタクトレス IC カードと NFC は共通の周波数を前提に動作するが、当初の国際標準化時に想定された利用目的は同一ではない。コンタクトレス IC カードは IC カード（端子付き）に非接触インタフェースを加えるものとして検討された。一方、NFC は IC カードとは異なる利用場面を想定して検討された[25]。

しかし、非接触インタフェースにかかわる実装上の技術的課題は共通である。すなわち、非接触インタフェースには内蔵されたマイクロコンピュータに対する動作電力供給に制約があることから、ビジネスリスク管理上必要なセキュリティ機能の実装や高速処理が困難な場合がある。

ここで、より重要なポイントは、IC カード（端子付き）、コンタクトレス IC カード、NFC が共通に使用できるか否かは、アプリケーションが実現すべきビジネスリ

24 高度なセキュリティ機能を意図して公開鍵暗号アルゴリズム等を実装する場合、処理を高速化するために専用の演算回路（Co-processor）をチップ内に搭載する方法が考えられるが、同回路の搭載によって増加する消費電力を含めたチップの全消費電力が供給可能電力の範囲内に収まることが必要になる。

25 想定する利用場面の違いにより無線インタフェース、伝送プロトコル等の下位レイヤーにおいて細かい相違が存在するほか、上位レイヤーにも相違が存在する。すなわち、コンタクトレス IC カードでは IC カード（端子付き）と共通の内部ファイル構造とアクセス管理を含むセキュリティ構造を用いるのに対し、NFC 規格には上位レイヤーの定めがないため異なる内部ファイル構造とセキュリティ構造が用いられている。

スク管理上の要件に対応できるか否かによって決定されるという点である。一般に、IC カード（端子付き）とコンタクトレス IC カードのセキュリティ機能は同等とのイメージがあるが、本人確認やオンライン承認の要否等を含めたシステム運用上の相違があることから、すべての利用システムにおいて同等であるとはいえない。IC カードまたはコンタクトレス IC カード（含、NFC カード）に求められるセキュリティ機能と、実際に実装され提供されるセキュリティ機能との間に不整合がある場合、利用システム全体としてのビジネスリスク管理が実現できないことになる。運用条件を含め、IC カード（端子付き）やコンタクトレス IC カードとそれら以外のシステムの各部分とが分担すべきセキュリティ機能を調整することで上記の不整合を解消することができれば、利用目的に沿った利用が可能になる。仮に、不整合のままでシステムを稼働させた場合は、それによって生じるセキュリティ上の問題がビジネス上の損害につながる可能性を意識しておかなければならない。

補論 2. 非接触インタフェースにかかわる標準化の動向

(1) 国際標準・業界標準

非接触インタフェースにかかわる標準化は、国際標準と業界標準の両面から推進されている。IC カード（端子付き）とコンタクトレス IC カードについては ISO/IEC JTC 1/SC 17[26]において国際標準化が行われている。IC カード（端子付き）については、端子の位置・寸法、電気特性、初期応答シーケンス、伝送プロトコル等が ISO/IEC 7816 シリーズで標準化されている。同シリーズはコンタクトレス IC カードにも共通な内部ファイル構造、セキュリティ構造、共通コマンド、共通データ要素等を標準化している。

コンタクトレス IC カードには、密着型・近接型・近傍型があるが、ここではリテール取引に使用されている近接型についての国際標準 ISO/IEC 14443 シリーズを紹介する。同国際標準は端末側からコンタクトレス IC カードに供給する磁場の特性、初期化シーケンス、同一の磁場内に複数のコンタクトレス IC カードが存在する場合の衝突回避制御、伝送プロトコル等を規定している（内部ファイル構造、セキュリティ構造、共通コマンド、共通データ要素等については上記の ISO/IEC 7816 シリーズを適用する）。ISO/IEC 14443 シリーズで規定された方式は、IC 旅券（電子パスポート）、IC 運転免許証、住基カード等に採用されている。

これらのほか、ECMA[27]が規格化した後に、ISO/IEC 18092 および 21481 として制定された国際標準がある。これらはカードに関する規格ではなく NFC（近距離無線通信）に関する規格であるが、カード（カード形状の Passive Mode の NFC）とその対応端末間のインタフェースにも利用されている。

なお、携帯電話（非接触インタフェース対応機能付き）では、携帯電話網を経由する通信によって処理を行う場合と、端末等との間で上記の ISO/IEC 14443 シリーズまたは NFC シリーズの非接触インタフェースに基づく通信によって処理を行う場合とがあるが、本稿における検討は後者のみを対象にしている。

コンタクトレス IC カードと NFC の当初の利用目的は同一ではなかったが、利用システムの立場から両者を同等に扱いたい、あるいは、共存させたいとの要望に基づき、13.56 MHz 帯における動作条件の共通化が必要との認識が出てきている。これについて関係する国際標準化委員会間での検討が開始されているが、現在は検討の段階といえる[28]。非接触インタフェースにおいて下位レイヤーの共通化ができた

26 ISO/IEC JTC 1/SC 17 は、カードおよび個人識別を対象とし、各種カードの要素技術から利用システム（クレジットカード・IC 旅券・運転免許証等）までを含む国際互換性に関する標準化と登録管理を担当する国際標準化委員会である。

27 ECMA 規格は、欧州における計算機メーカーの業界団体である Ecma International（旧、European Computer Manufacturers Association）によって策定された業界標準である。

28 国内で普及している交通系カードに採用されている符号化方式やビットの送出順序は NFC の一部に規定されているが、コンタクトレス IC カードの国際標準である ISO/IEC 14443 シリーズ（タイプ A、タイ

場合、従来のコンタクトレスICカード利用システムとNFC利用システムがそのまま相互乗入れ可能になると期待する見方があるが、上位レイヤーの概念やビジネスリスク管理面から整合性の検討が必要である。

一方、業界標準として普及が進んでいる標準仕様がある。これらは上記のカードと端末間の基本的インタフェースにかかわる国際標準を参照または引用しつつ、個々の業界における応用面の機能までを含めて標準仕様としたものである。代表的なものとしてICクレジットカード・ICデビットカードの業界標準仕様としてのEMV仕様[29]、欧州の携帯電話（GSM）標準仕様とガイドライン、国内の全銀協仕様等がある。

(2) 電子媒体の形態と国際標準

ここでは、非接触インタフェースに注目する立場から、物理的な形状としてのカードには限定せずに検討を行う。非接触インタフェースを提供する代表的な電子媒体として、以下の(a)～(d)が挙げられる。

(a) カード形状の電子媒体にISO/IEC 14443シリーズの非接触インタフェースが搭載されているもの。
(b) SIM（あるいはUIM）[30]にISO/IEC 14443シリーズの非接触インタフェース機能を加えたチップが携帯電話に内蔵され、携帯電話内のアンテナと接続されて非接触インタフェースを構成するもの。
(c) ISO/IEC 14443シリーズの代わりにNFCシリーズの規格を上記の(a)に適用したもの。
(d) ISO/IEC 14443シリーズの代わりにNFCシリーズの規格を上記の(b)に適用したもの。

図A-3は上記の機能を実装した電子媒体の各種形態イメージであり、最上段左からMSカード・ICカード・コンタクトレスICカード（上記の(a)に対応）・NFCカード（上記の(c)に対応）を、最下段左からSIM（ICカード）、SIM（ISO/IEC 14443対応、上記の(b)に対応）、SIM（NFC対応、上記の(d)に対応）のイメージを示す。

通常の利用場面では、これらの電子媒体がどの標準に準拠しているかが意識されることはないが、電子媒体の形状が同一であっても準拠している標準が異なる場合には伝送手順やデータ伝送形式等に異なる部分があるため互換性が保証されない。このような状況は、おのおのの標準がその制定時に意図していた環境とは異なる条件下でも広く利用されるようになり、利用場面が重複するようになった結果でもある。

プB）で定められた条件とは異なっている。両方式の相互乗入れを可能にするための条件については今後の検討課題と考えられている。

29 EMV仕様においては、ISO/IEC 7816シリーズおよびISO/IEC 14443シリーズが採用されている。

30 SIM（Subscriber Identity Module）あるいはUIM（User Identity Module）は、携帯電話への内蔵を前提とした、電話番号を特定するためのID情報を記録したICカードである。

図 A-3　電子媒体の各種形態イメージ