クレジットカード取引における セキュリティ対策

第 4 回

ICカードのセキュリティ対策(1)

山本 正行 Yamamoto Masayuki **山本国際コンサルタンツ代表**
関東学院大学経済学部経営学科講師、決済サービス事業の企画、戦略立案を専門とするコンサルタント。消費生活相談員を対象とした研修も実施。講演、執筆多数。

今号から2回にわたってICカードのセキュリティについて解説します。

割賦販売法の改正によってクレジットカード会社や加盟店などに「IC化対応」が義務づけられることになりました。IC化対応とは、クレジットカードを磁気カードからICカードに更新し、カードを受け入れる店舗(加盟店)の決済端末装置をICカード対応にすることを意味します。

ICカード方式の違い

ICカードにはいくつかの方式があります。例えば、クレジットカードで用いられる「接触型」、交通乗車券や電子マネーなどで用いられる「非接触型」、などがその代表例です。

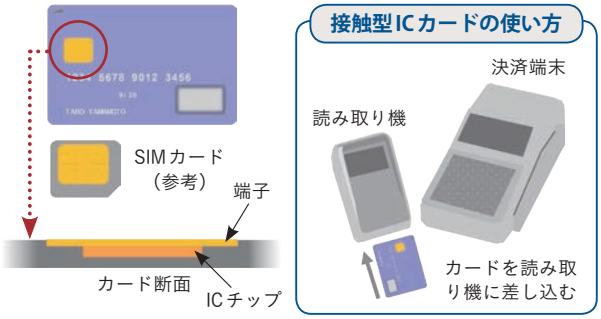
●接触型ICカード

接触型は専用のICカード読み取り機にカードを差し込んで使用します(図1)。クレジットカードの場合は、店舗の決済端末などにICカード読み取り機が付いており、そこにカードを差し込みます。接触型のICカードの表面には端子と呼ばれる部品が見えており、この下にICチップが埋め込まれています。端子部分が読み取り機に刺さってICチップが動作します。同じ接触型のICチップは通信会社のSIMカードにも採用されています。

●非接触型ICカード

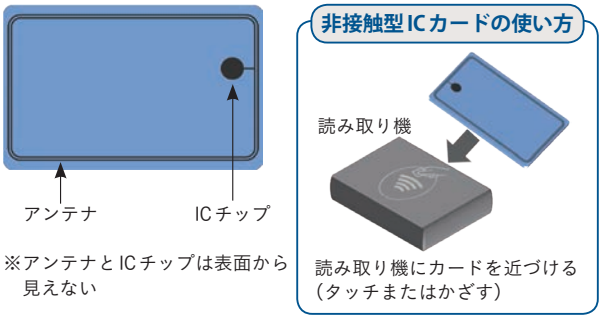
非接触型に端子はなく、外見はただのカードにしか見えませんが、カードの中にICチップとアンテナが組み込まれています(図2)。非接触方式の読み取り機が発する電磁波にアンテナが反応し、ICチップが動作するしくみです。日本で普及する非接触型のICカードはソニーが開発したフェリカと呼ばれるICチップを使用しており、交通乗車券、ICカード型電子マネーなどで利用されています。海外ではフェリカに代わり国際標準機関のISOが定めるタイプA／タイプBという規格のICチップが用いられており、交通乗車券、IDカードなどで広く普及しています。

図1 接触型ICカード



用途：クレジットカード、国際デビットカードなど

図2 非接触型ICカード



※アンテナとICチップは表面から見えない

用途：交通乗車券、電子マネーなど

接触型と非接触型の両方を備える「多機能カード」

通常ICカードは接触型または非接触型のどちらかの方式を取りますが、最近は１枚に接触型と非接触型の２つの方式を備える「多機能カード」も増えています。

日本では、接触型のクレジットカードと、非接触型のフェリカを使用した電子マネーの２つの方式を備えた多機能カードが増えています。海外には日本で普及しているような電子マネーは少なく、それに代わって、接触型と非接触型（タイプA／タイプB）のどちらでもクレジットカードやデビットカードが使える多機能カードが増えています。

クレジットカード用ICカードの仕様

クレジットカードに用いられるICカードは、ビザ、マスターカード、JCBなどの国際決済ブランドが策定した標準仕様（EMV仕様＊1）に準拠しています。接触型が必須となっており、前述した多機能カードに限りタイプA／タイプBの非接触型にも対応できます。

EMV仕様はクレジット、デビット、プリペイドのすべての決済手段に対応しており、そのためクレジットカードだけでなく国際デビットカード、国際プリペイドカードもICカードに対応することが可能です。実際に日本で発行が進む国際デビットカードのほとんどのものがクレジットカードと同じEMV仕様のICカードとなっています（以下、EMV仕様に準拠したICカードを単にICカードと記します）。

ICカードによるセキュリティ対策

まず、ICカードの効果は店舗でカードを提示して支払う場合に有効です。インターネット決済ではカード番号やセキュリティコードを入力して支払うため、せっかくのICカードも意味がありません。インターネット決済では、認証サービスなどICカードとは異なる対策が必要です。

店舗での支払いに限定されるとはいえ、ICカードは従来の磁気カードとは比べものにならないほど高いセキュリティ機能をもたらします。先行してIC化対応を終わらせたイギリスでは、対応後、偽造カード被害額が70%、盗難・紛失カードによる被害額が60%も減少するという効果がありました＊2。

ICカードのセキュリティ機能の主なポイントをまとめると次のとおりです。

①スキミングが極めて困難

磁気カードの情報はスキマーで簡単に読み取ることができますが、ICチップの情報を読み取るには専用の読み取り機が必要です。ICカードには読まれてもよい一般情報と秘匿情報が別々の領域に格納されており、秘匿情報の内容は読み取ることができないようになっています。ICカードを偽造するには秘匿情報を再現する必要があるうえに、高価な発行設備も必要です。実質的にICカードの偽造は不可能といえるでしょう。

しかし、ICカードは磁気カードも兼ねるため、磁気カードの情報をスキマーで読み取られ、磁気の偽造カードが作られてしまう可能性が残ります。磁気の偽造カード悪用を防ぐためにも、加盟店の決済端末のすべてがICカードに対応することが強く望まれます。

②認証のしくみを高度化

カードを利用する際に、まずICカードのデータが変造されていないことをチェックする認証機能が働きます。データ変造が検出されると取引を中止するなどして不正使用を防ぎます。次にイシュアー＊3による利用承認（オーソリゼー

＊1　ビザ、マスターカードなどの国際決済ブランド組織が策定した決済用ICカードの仕様。EMVとはEuropay、MasterCard、Visaの３つの決済ブランドの頭文字をとった名称。現在EuropeyはMasterCardと合併したことにより消滅。

＊2　イギリスの金融機関による業界団体“Payments UK”の統計データから分析。

＊3　クレジットカード会社、銀行、前払式支払手段発行者。

ション）の際に、取引ごとに個別に暗号化した情報を用いてイシュアーとICカードが相互に認証しています。このしくみを破って不正取引を行うことは極めて困難です。従来の磁気カードは、イシュアーが取引の承認・否認の回答を決済端末に返すだけの単純なしくみですので、決済端末に仕掛けを施して全取引を承認してしまう、という不正が発生したこともあります。

③通信機能がない環境でも安全

例えば機内販売では、決済端末に外部との通信機能がないため利用承認をイシュアーに求めることができません。ICカードは、このような取引でもIC チップ内のプログラムが取引の安全性を評価して自ら取引を承認・否認することができます。その機能を生かすために、イシュアーはカード発行時にさまざまなパラメーター（指示事項）をICカードに設定します。

④暗証番号による本人確認に対応

本質的な機能とは異なりますが、ほとんどのICカードには暗証番号が格納され、支払いの際には決済端末に付随するPINパッドに暗証番号を打ち込む必要があります。暗証番号で利用者本人の確認を行うことで、盗難・紛失カードの悪用を抑制します。

磁気カードでは、ATM でのキャッシングなどを除き、原則として署名（サイン）で本人確認を行っています。日本では、店員がカード裏面とレシートのサインを照合することは少なく、盗難・紛失カードが第三者によって簡単に利用されやすい状況であることが指摘されています。

ICカードが残す課題

ICカード化は、とても優れたセキュリティ対策ですが、人の手による運用やしくみが抱える問題までは解消できません。例えば暗証番号に関する運用や、ICカードに対応する決済端末の導入に時間がかかることなどは、ICカード導入の際の悩ましい課題です。

●暗証番号の課題

日本では2002年ごろにICカードへの移行が始まりましたが、当時はクレジットカードの暗証番号がまだ一般的でなく、利用者が暗証番号を認識していない問題点が指摘されました。そのため、救済策としてICカードで支払う際に暗証番号を知らない人はサインでよいとする運用が行われました。現在多くの店舗が暗証番号を求める運用に変えていますが、一部にICカードでの支払いでもサインを認める店舗が残っています。

前号＊4でも紹介したとおり、海外のATMやチケット券売機などで暗証番号が盗まれる被害が発生しています。この被害を防止するために、海外旅行の際に専用の国際プリペイドカードを持参するのは効果的な対策の１つです。帰国した際に暗証番号を変更することもよい対策です。現在まだ一部ですが、コンビニのATM で簡単に暗証番号を変更できるICカードもあります。該当カードを持つ人は頻繁に暗証番号を変更するのが最も有効な対策でしょう。

●加盟店での課題

IC化対応は、イシュアーによるカードのICカードへの更新と、店舗の決済端末のIC対応の両輪で成り立ちます。両方が一斉に対応をすませればその効果は最大となりますが、残念なことにその足並みはなかなかそろいません。カードは更新時にあらかたICカードに置き換えられると考えられますが、店舗の決済端末の置き換えが思うように進まない問題が指摘されています。せっかくのICカードも、店舗の決済端末が磁気専用の場合は磁気カードとして処理されてしまい、その効果が発揮されません。

このように事業者が絡む課題や、政府が推進する実行計画の内容については次号で詳しく解説します。

＊4　ウェブ版「国民生活」2017年８月号「クレジットカード取引におけるセキュリティ対策」第３回「カード情報の悪用」
http://www.kokusen.go.jp/wko/pdf/wko-201708_10.pdf