意外と知らない？！

クレジットカードのセキュリティコードとは？

インターネットショッピングなどでクレジットカードを利用する際に「セキュリティコード」を求められることがあります。セキュリティ強化のためであろうことはわかりますが、どのような効果があり、どんな時に役立つのでしょうか。今回は意外と知られていないのでは？と思われるクレジットカードの「セキュリティコード」について確認したいと思います。

クレジットカードのセキュリティコードとは？

セキュリティコードとは、クレジットカードの安全性を高めるためにカード番号や有効期限とは別に、カードごとに決められた番号のことです。セキュリティコードを定めておくことで、仮にカード番号が知られた場合でも不正利用されにくくなると言われています。（※日本国内全てのクレジットカード発行会社が、セキュリティコード対策を施しているわけではないです）
セキュリティコードは、クレジットカードの種類によって位置と桁数が異なります。
国際ブランドが Mastercard、Visa、JCB、DinersClub の場合は、カード裏面に記載されている 3 桁の番号がセキュリティコードになります。クレジットカードによっては 3 桁以上の数字が印字されている場合がありますが、この場合は末尾 3 桁がセキュリティコードに該当します。国際ブランドが American Express の場合は、カード表面のカード番号右上に 4 桁で記載されています。クレジットカードの有効期限が間近になり新しいカードが発行される際、変更事項がなければカード番号は変わらないことがほとんどですが、セキュリティコードは必ず変更になります。この点が、カード番号とセキュリティコードの大きな違いです。

クレジットカード使用時の安全を守るセキュリティコードの効果

セキュリティコードは、暗証番号やサインと同様にクレジットカードをもつ本人のみが知ることができるため、クレジットカードのセキュリティを高める効果があります。具体的にどのような場面で効果があるか見ていきたいと思います。

不正利用のリスクを軽減できる

お店などでクレジットカードを利用する際、4 桁の暗証番号やサインが求められます。また、実際にクレジットカードが手元にないと決済できないため、不正利用をある程度抑えることが可能だそうです。
しかし、インターネットでクレジットカードを利用する際は、暗証番号やサインを求められることはありません。そのため、何らかの理由でカードに記載されている情報が流出した場合、不正利用されるリスクが高くなります。
そのリスクを抑えられるのが、セキュリティコードです。カード番号などの情報が流出した場合でも、カードが手元になければセキュリティコードはわかりません。暗証番号と同様、カードの所有者にしかわからない数字であるため、セキュリティコードを盗まれない限りは、インターネット取引での不正利用のリスクは軽減されます。

スキミング詐欺への対策

クレジットカードの磁気や IC チップには、クレジットカードの情報が盛り込まれています。これらの情報をスキマーと呼ばれる機械を使って抜き取る手口をスキミングと言います。スキミングで抜き取った情報から偽造カードを作成し、不正利用されるケースが多いですが、スキミングではセキュリティコードを抜き取れないため、スキミング詐欺のリスクを抑えることができます。

セキュリティコードは万全な対策ではない！

不正利用を抑制できるセキュリティコードも万全な対策ではないです。

⚠セキュリティコードの入力が不要なインターネットサイトもある

⚠フィッシング詐欺（*1）にあう可能性がある

（*1）フィッシング詐欺・・・金融機関を装ってメールを送り、メールに記載されている偽サイトにアクセスさせてカード番号や暗証番号などを盗む詐欺

⚠カード自体を紛失すれば、セキュリティコードも流出してしまう可能性がある

セキュリティコードを流出させないことが重要！

例え、セキュリティコードが流出してもそれだけではクレジットカードを不正利用することは不可能です。しかし、セキュリティコードが流出した時は、他のカード情報も流出している可能性が高いため、不正利用されるリスクが高まるそうです。セキュリティコードを流出させないために、いくつか対策を見ていきます。

セキュリティ対策がされたサイトで買い物をする

インターネットサイトで買い物をする際、表示されている URL を確認したことがあるでしょうか。URL には大きく「http://」と「https://」の 2 種類に分かれており、「s」は SSL（暗号化通信）を表しています。よってこの「s」が付いているサイトは付いていないサイトに比べ、セキュリティ対策が強いことを意味しているそうです。

怪しいメールを開いたり、URL にアクセスしない

カード会社や銀行、郵便局などの金融機関を装って送られてきたメールの URL にアクセスすると個人情報が抜き取られるフィッシング詐欺は、よくある犯罪のひとつと言われています。詐欺サイトと知らずにカード情報やセキュリティコードを入力してしまうことがあるため、怪しいメールを開いたり、そこに掲載されている URL にはアクセスしないよう注意しましょう。

クレジットカードを保有しすぎない

クレジットカードを多く保有すると紛失するリスクが高まるだけではなく、紛失したことや不正利用に気付きにくい、というデメリットがあります。クレジットカードは、必要最低限の枚数を保有することもセキュリティコードやカード情報の流出対策になりそうです。

※※万が一、クレジットカード情報が流出した場合はカード会社に速やかに連絡をし、番号を即変更してもらいましょう。カード会社が番号流出を認定すると早急に変更手続きが可能となります。

クレジットカードには、セキュリティコードがあることによって不正利用のリスクが抑えられますが、一方で万全ではありません。カードは自分自身で管理できる枚数を保有し、セキュリティに対する意識をきちんと持つことが大切です。
近年キャッシュレス化が進み、現金ではなくクレジットカードで支払う機会も以前に増して多くなったように感じます。クレジットカードと上手に付き合っていくためにも基礎知識として理解しておきたいですね。