

MasterCard カード会員の皆様へ

『フィッシング』詐欺にご注意ください

最近、実在のカード会社や金融機関の名前を使って、悪意を持った e メールを送り付けて、個人情報を取得・悪用しようとする事件が多発しています。e メールにはもっともらしい偽装サイトにリンクが張っており、偽装サイトに誘導して、カード番号、住所、ID、パスワードなどの個人情報を入力させて盗み取る手口で、『フィッシング』e メールとも呼ばれています。

当社やカード発行会社が、e メールでカード会員の皆様の個人情報を入力するよう求めることはありません。

- ・ ID やパスワード、カード番号等の個人情報を要求する e メールには、**絶対に返信したり、リンクの張ってある Web サイトも開かないで下さい。**
- ・ そのような e メールを受け取ったときには、その送り主の会社に電話で問い合わせをしてください。(なお、送り主がお手持ちのカード発行元の場合、ご自身のカード裏面に記載されているカード発行会社の電話番号をお使いください。)
- ・ または、新しくインターネット・ブラウザを開き、その金融機関の正しいウェブアドレスを入力して、サイトの真偽を判断してください。

すでにフィッシング e メールに返信してしまい、偽装ウェブサイトに個人情報を入力してしまった場合は、

- ・ **直ちにカード発行会社に連絡してください。**

カード会社からの請求書が届いたら直ちに請求内容を確認してください。

- ・ **もし心当たりのない請求があった場合には発行カード会社に、電話で問い合わせてください。**

未然に被害を防止するために

『フィッシング』e メールは、米国で 2003 年に現れ、主に個人情報窃取の常套手段として猛威を振るってきました。現在では米国のみならず全世界で『フィッシング』e メールが横行し、特に世界的な規模で展開している金融機関のウェブサイト似せて罠のサイトが作られています。

マスターカード・インタナショナル (MasterCard International) では、このような『フィッシング』詐欺から MasterCard カード会員を守るために、米国のソフトウェア会社であるネームプロテクト社 (<http://www.nameprotect.com/>) (英文のみ) と提携して、偽装ウェブサイトの摘発に協力しています。フィッシング詐欺の温床となる偽装ウェブサイトやカード情報取引サイトを特定・検知して、各国の警察等、法執行機関に情報提供を行い、このような偽装ウェブサイトが閉鎖されるよう働きかけています。

カード会員の皆様にも、以上記載した防止手段を講じられるようお願い申し上げます。

MasterCard では、会員の皆様に快適で安全なカード生活を引き続き享受していただくため、今後も努力してまいります。

以上