



産経新聞

カードの規則性悪用

クレジットカードマスター「防ぎようない」

インターネット決済とクレジットカード番号の規則性を悪用した新たなカード犯罪の一端が明らかになった。警視庁が7日に窃盗容疑などで逮捕状を取る大阪市の男らは、カード番号と有効期限だけで簡単に決済できるネットの通販サイトに着目。「クレジットカード」と呼ばれる手口で、他人になりすまし購入を繰り返していた。

カード番号の仕組み自体を悪用しているため、カード会社なども番号流出の防止に打つ手がないのが実情だ。専門家は「ネット決済に暗証番号の項目を追加するなどの対策が急務」としている。

カード会社関係者によると、これまでカード犯罪で、スキマーと呼ばれる機械を使ってカードの磁気情報を盗み取る「スキミング」や、偽のウェブサイトのURLを張りつけたメールを送りつけ、カード情報を登録させる「フィッシング」と呼ばれる手口の被害が目立っていた。

特殊な機械や技術が必要なら、これらの手口に比べ、クレジットカードは元になるカードがあれば、あとは計算を繰り返すだけの比較的単純なものだ。男らは、

通販業者のサイトで次々と番号を打ち込んでいくことで、実在する他人のカード番号に行き着いていた。

NPO法人「日本情報安全管理協会」(東京都)は、「クレジットカード番号を知られることは防ぎようがない。ネット上で不正利用するため、犯人にとってリスクの低い手口」とする。

複数のカード会社によれば、クレジットカードの被害報告は約10年前から寄せられているという。日本クレジットカード協会の調査では、今年1～3月までのスキミングやフィッシングな

ど不正行為による被害額は25億9000万円。クレジットカードマスターによる被害件数もこの中に含まれるとみられるが、カード会社が詳細を公表しないため、実際の被害は不明だ。

カード会社関係者は「サイト上でより多くのカード情報や個人情報を入力するシステムにするなど、業界で統一ルールを作る必要がある。ある程度、ネット利用者には手間をかけてもらうしかない」と指摘する。

ただ、業者にとってはハドルが低い方が客を呼び込みやすいという本音もある。

ある通販業者は「打ち込む情報が少ない方が買い物が便利」と、ネット決済の煩雑化には及び腰だ。

日本情報安全管理協会は「決済はカード会社の問題と考えられており、販売側にとつてひとごとなのではないか」としている。

カード番号に計算施し他人の番号割り出す

カード番号に特殊な計算を施し、ほかのカード番号を割り出す「クレジットカードマスター」という手口を使って、不正にインターネットで商品を購入していたとして、警視庁は6日、窃盗の疑いなどで大阪市内の無職の男(45)の逮捕状を7日に取る方針を固めた。捜査関係者によると、クレジットカードマスターによるカード犯罪の摘発は全国初だという。こうした手口はカード会社などで問題となっており、被害防止に向けて抜本的な対策を迫られそうだ。

カード会社関係者や捜査関係者によると、クレジットカードマスターは、実際のカード番号に複雑な計算を加え他人のカード番号を割り出す手口。ネットにはカード番号と有効期限を登録すれば買い物ができる通販サイトがあり、この手口で不正に入手した番号を打ち込むと、実在のカード番号に当たる可能性がある。有効期限は元のカードの期限がそのまま該当する場合がある。

中野署の調べによると、男はクレジットカード会社の手帳を盗み、総額1千万円分以上を購入していたという。オークションサイトなどで転売し利益を得ていたとみられる。

男の知人で共犯の無職、旭千鶴被告(20)＝大阪市＝は、窃盗と電磁的記録不正作出、供用の罪で既に起訴されている。(27面に関連記事)

警視庁きょう男に逮捕状

クレジットカード 16けたのクレジットカード番号のうち複数のけたに、決まった数字を足し引きしていくと、特定の回数で元の番号に戻る。その過程で出てきた番号は、他人が使用しているものに該当する可能性があるという。カード番号の並びの規則性を悪用した方法。こうした計算を瞬時に自動ソフトも出回っているとされる。カード業界の関係者などによると、10年ほど前から被害が確認されているが、具体的な防止策は見つかっていない。

クレジットカードマスター 初摘発

カード会社関係者や捜査関係者によると、クレジットカードマスターは、実際のカード番号に複雑な計算を加え他人のカード番号を割り出す手口。ネットにはカード番号と有効期限を登録すれば買い物ができる通販サイトがあり、この手口で不正に入手した番号を打ち込むと、実在のカード番号に当たる可能性がある。有効期限は元のカードの期限がそのまま該当する場合がある。