

第3回：可視化されない価格の妥当性 - 医療費にも似たIT投資



掲載日：2004年6月30日

執筆者：株式会社スクウェイブ

代表取締役社長

黒須 豊

・さて、今回は現実に私が被った個人情報漏洩問題について書いてみたいと思う。それは、クレジットカードの被害である。これを読めば、もはやカード被害は他人事ではないことがお分かりになるだろう。

・皆さんのまわりには、クレジットカードの被害に遭われた人はいるだろうか。ニュースでは良く耳にする話だが、現実に身の回りで起きているかどうかは、実際に体験してみないとわからないことが多い。実は、つい最近、私のクレジットカード情報が漏洩し、結果として身に覚えのない売買が私のクレジットカード番号によって行われたのである。今回はその詳細を紹介しよう。

・2004年5月某日深夜、私は仕事で遅くなり家路についた。帰宅すると、私は習慣的に留守録の有無を確認するようにしている。この日は1件入っていた。着信記録には電話番号が残っていたが、知らない番号からのものであった。単なるセールスか何かだろうと思いつつ再生してみることにした。

『こちらは、三井住友 VISA カードの△△△ですが、至急折り返し電話を頂きたく……』

用件は今ひとつ明確ではなかった。ちなみに私は用件が明確ではなく、とにかく折り返し電話をくれという趣旨の留守電が大嫌いである。人に折り返し電話を依頼しておきながら要件を明確に伝えない人は無礼だと思っている。少しだけ頭にきた私は、このことが翌朝自分を慌てさせることになろうとは夢にも思わず、ベッドに入って寝てしまった。

・翌朝は、とあるマスコミとのインタビューが朝一で予定されていたため、私はいつもより少しだけ早起きして着替えを始めた。その時、昨夜の留守電のことを思い出した。用件が明確でない留守電で頭には来ていたが、時間が少しあったので、私はコールバックす

ることした。

『ル ル ル ル ガチャ』

担当者が出た。単刀直入に私は聞いた。

『昨夜、お電話を頂いた者なのですが、ご用件は何ですか？』

『実は、お客様が利用したことがある店舗でスキミング被害が発生し、もしかすると、お客様のカードも不正に使われた可能性があります・・・』

担当者の言葉を私の耳は素直に聞き入れなかった。一瞬絶句していると、担当者は慣れた口調で言葉を続けた。

『今からご記憶のない取引を確認させて頂きたいと思います。5月xx日に、インターネットで\$140の買い物をされた記憶がございますか？』

そんな明確な記憶はなかった。しかし、ハーバードビジネススクールのケース資料など、インターネット上でドルでの買い物を行うことは私にとっては珍しいことではない。ただし、取引内容で明示された文言に記憶がないだけでなく、買い物したとされる日付が直近のことであったため、それは私が行った取引ではないことは明らかだった。このようなやりとりを経て、結果として私のカード番号は直ちに登録が抹消された。また、身に覚えのない最後の取引は無かったことにしてもらえ、代わりに新しいカードが1週間以内に発行されるとのことで少しだけホッとした。

しかし、問題はまだある。携帯電話や雑誌購読などをカード決済にしている場合に、切り替えの手間が発生することがあるのである。カードが自動で変更できるものと、そうでないものが存在するのである。さらに、一体何をクレジットカード決済にしていたかを全て記憶しているわけでもない。

私は、時間切れになり、インタビューに間に合わせるため家を後にした。全くとんだ朝を迎えてしまったものである。精神的なダメージもあったが、純粋な手間だけを考えても、これらの時間は言うまでもなく機会損失である。犯人が捕まったら民事上の損害賠償も求めたいくらいである。

・ところで、一体どこの店でスキミング被害が発生したのか。日頃からニュースで騒がれているのに、このような被害を出すとは、その店は怠慢であり、その店は何処なのか教えて欲しいと思うのは人情である。

しかし、三井住友 VISA カードとしては回答できないと言う。まあ、事情はわからない

わけではない。一番悪いのは犯人である。お店としては、それが理由で客足が減っては困る。客足が減ると結果としてカードの売り上げも減るので、カード会社も困る。

・一般的な磁気カードにはカード情報が厳密に暗号化されない状態で記録されている。さらに、問題なのは、認証として事実上機能を果たしていないサイン制度と、サインもパスワードも無しで購入手続きが完了するオンラインショッピングの致命的な運用制度にある。

サイン認証はカード裏面のサインと似ていさえすれば良いわけで、カードが偽造されれば、偽造した犯人が自分のサインを書き込むことができる。

・インターネットなどの取引では、カード番号、カード記載氏名、カード有効期限の情報さえあれば、通常何の認証も必要としない。

これらは正規のユーザーが購入する上で負担の少ない運用制度と言えるが、泥棒にとっても好都合な制度なのである。

・私は、カード会社に是非とも抜本的な情報漏洩対策の確立を急いでもらいたい。スキミングにはカード情報の暗号化を、購入に際しては、店舗でもオンラインでもパスワード入力を必須にしてもらいたい。たったこれだけで、当被害の大半は防ぐことが可能である。

・最後に、企業内の通常業務における情報漏洩に関する質問を良く受けるが、ポイントは、どうやって漏洩を避けるかよりも、仮に生のデータが漏洩しても、そのままでは機密がいかに見えないようにするかに力点を置いた対策を練るべきである。

・また、承認の厳格化は当たり前の話であり、今の時代に現在のクレジットカードの運用体制は論外であるが皆さんの会社では大丈夫だろうか。今一度、各領域の運用体制を見直されてみることをお勧めしたい。