Weekly コラム

平成 27 年 12 月 1 日

〒541-0055　大阪市中央区船場中央 2-1
船場ｾﾝﾀｰﾋﾞﾙ 4 号館 4 階

船場経済倶楽部
(NPO 法人 SKC 企業振興連盟協議会)

Tel　06-6261-8000
Fax　06-6261-6539

人の輪・衆智・繁栄

senBa

活動方針

当団体は、異なる業種の経営者が相集い、　力を合わせ、自らの研鑽と親睦を通じて、斬新な経営感覚と新たな販売促進を創造して、メンバー同士でより健全な事業所とその事業所のイメージアップを図り、地域社会に貢献できる事業所となることを目的とする。

インターネット不正送金で変わるセキュリティのあり方

インターネットバンキングの不正送金の被害が目立っています。警察庁によると、今年上半期(1～6月)の被害額は、昨年の下期に比べ約 46%増加、15 億 4,400 万円にも及びました。不正送金の受け取り口座の名義人は、国籍別でいうと日本人は 3 割程度、中国が最も多く全体の半数を超えます。

1件の平均被害額は約 155 万円で、2013 年の約 107 万円から 45%も大きくなりました。その理由は、被害の内訳に法人口座が増えたことがあります。個人よりも法人のほうが扱う金額が大きく、犯人にとっては一度に多額の金額を盗みだせるため、あえて法人口座を狙うようになったといいます。企業にとって、銀行口座の不正送金は対岸の火事とはいえない状況になっています。

どのようにして、被害に遭うのでしょうか。手口のなかでも多いのは、ウイルスに感染させ、インターネットバンキングのIDやパスワードを盗みとるやり方です。犯人は企業の従業員になりすまし、盗み出したパスワードを利用して、会社の口座から自分の口座へ送金します。最近では、法人口座を狙う、専用のウイルスも開発されているといいます。

また、電子証明書といって、インターネット上の実印のような役割をするものが狙われるケースもあります。電子証明書はインターネットバンキングを利用するときに、自分のパソコンが不正なものではないことを証明する「身分証明書」のようなものです。

電子証明書を発行しておくと、電子証明書のないパソコンからは送金ができないので、不正送金を防げるといわれていました。ところが、最近では、電子証明書を窃取するケースも出ており、簡易な対策では不十分という状況になっています。

不正送金の被害を防ぐには、自社のパソコン全部を対象にセキュリティシステムを強化し、ウイルスに感染しないようにすることが第一です。ただ、セキュリティ業界としても、ユーザー任せではなく、金融機関自ら、対策強化に乗り出しています。メガバンクや地方銀行は、「ワンタイムパスワード」といって、取引ごとにパスワードを発行するシステムを導入し、不正を未然に防止しています。

また、抜本的な対策として、金融機関はNTTデータと連携し、インターネットバンキングの不正送金を見破るシステムを開発しています。どのようにして見破るかというと、これまで起こった不正の被害情報を集約し、まずはブラックリストを作成します。そして、リストに掲載された犯罪者が取引しようとすると、自動的に遮断するというものです。

NTTデータの取り組みは、セキュリティ強化の新たな手段というだけではなく、業界のビジネスそのものを変える意味合いもあります。

従来ですと、セキュリティ業界は、セミナーやソフトウェア販売といった形のビジネスが主流でした。NTTデータの取り組みは、金融機関が送金を遮断するという抜本的な対策となります。

セキュリティは、被害に巻き込まれないよう、個々の利用者が対策するものから、犯人が犯罪を起こせないよう、金融機関などのおおもとで対策するという形が、新たな柱として出てきたことになります。

今後も犯人側が手を緩めることはなく、それに対してセキュリティ業界の企業がどのように対策を打ち出すのか、自社が被害に遭わないためにも注目しておきたいところです。

記事の内容に関するお問い合わせは事務局までご連絡ください。

ウィークリーはメールでの配信も行っております。お手数ですが、「メール希望」・「配信停止希望」と件名にご入力の上、
skc-soudan@skc.ne.jp まで空メールをご送信ください。また、FAX ご不要の際は、その旨をお電話にてお申しつけください。