特集

情報を盗みとられないために ～ソーシャルエンジニアリング対策～

昨今の洋菓子業界の老舗における品質表示偽装は、内部告発による企業不祥事の摘発であった。内部告発を通じて明るみにでた経営姿勢の問題により、社会的責任の追及を受けるのはやむを得ないことだ。しかし、内部から盗み取られた情報が風評となって企業イメージを貶めることもある。また、顧客情報や個人情報、企業ノウハウの外部流出は企業存亡に関わる事態を引き起こす。

ソーシャルエンジニアリング

ソーシャルエンジニアリングということばをご存知だろうか。直訳すれば「社会工学」であるが、情報セキュリティ用語としては、心理的な虚をついた巧みな話術や身なりなどで不正に情報を入手する犯罪行為をさす。不正に入手された情報はネットワーク犯罪に利用されたり、情報が売買されるヤミ市場に流出していくことになる。

一般に情報セキュリティといえば、コンピュータウイルス、ネットワーク不正侵入など外部からの攻撃についてのイメージが大きく、様々な防御策が講じられている。しかし、もう一方、社内の人に起因する情報漏洩リスクに対する防御策はまだまだ体系化されていないようである。情報漏洩は社内の人間の不注意が原因となることもあるが、悪意の第三者によって引き起こされる危険性も高い。

ソーシャルエンジニアリングの手口

ソーシャルエンジニアリングの手口を大きく分類すれば次の三つになる。

①**なりすまし**：公共機関やISPなどを装った電話等により、不正アクセスに必要なセキュリティ重要情報を盗み出すこと。本人や上司になりすますケースもある。消防署員に変装して消火器を売る詐欺事件などに見られるように、私たちは既存の知識や権威などを安易に信用してしまうことが多い。

②**ショルダーハッキング**：社内で企業情報を盗み見ること。肩越しに盗み見るという意味である。業者や訪問者が機密情報のあるオフィスに立ち入る場合に注意が必要である。デスク上のメモや不要文書を裏紙として使用している場合に危険性が増す。顧客名簿や名刺なども外部の眼にふれると危ない。

③**トラッシング**：廃棄された書類等から情報を読みとること。いわゆるゴミ箱あさりのことである。清掃員として侵入し情報を盗み取る者もいる。廃棄文書のシュレッダー処分は一般化しているが、シュレッダーで廃棄された紙クズを組み合わせて情報を再生するプロがいる。再生できなくするにはミリ単位での粉砕が必要だがというが難しいところである。

ソーシャルエンジニアリングの対策

ソーシャルエンジニアリングの対策としては以下の項目が考えられる。

①離席時にはディスプレーを消しておく。文書は裏返しにする。
②ノートパソコンが持ち去られないようにチェーン等でつなぐ。
③来訪者をオフィスに入れない（応接室等での対応）
④廃棄する文書はすべてシュレッダーをかけ、複数のポリ袋に入れて捨てる。
⑤外部からの質問に対応する専門の担当者を設定する。

要は、「人を見たら情報泥棒と思え！」という位のリスク感覚を持つことである。疑心暗鬼になりすぎるのも問題ではあるが、情報セキュリティのためには石橋を叩いて渡るくらいの慎重さは必要である。

テクノ経営総合研究所では、経営コンサルティング事業における社会的責任を果たすため、自社の情報セキュリティマネジメントシステムの構築を進めてまいりました。このたびISO認証取得を契機として、貴社の情報セキュリティマネジメントシステム構築のお手伝いができればと考えております。

ISMSに関するお問合せは、下記までお気軽にご連絡ください。

㈱テクノ経営総合研究所　IS事務局　06-6910-6797（担当：池野まで）