**情報漏えい**

今月の事例から学ぼう！は、「情報漏えい」についてです。

次の事例を読んで、問題点を考えてみましょう。

保険会社のT社は外回りの営業担当者が多く、週に一度しか事務所に顔を出さないという担当者も多くいます。もちろん、社内掲示板や勤怠入力システムなどの環境は整備されており、社外からでもユーザーIDとパスワードで社内システムにアクセスできるようなっています。

最近になり、保険の契約者から「T社と契約してからというもの、勧誘の電話が急増した。ほかに心当たりもないので、そちらから情報が漏れてるのではないか」という問い合わせが入るようになりました。

T社の情報システム部では緊急対策チームを結成し、社内調査を実施したところ、漏えいしているのは「保険契約者リスト」のデータで、深夜にそのデータにアクセスしているログがあることが判明しました。ログを解析してみると、利用者は営業部のAさんのものでした。Aさんに確認したところ、深夜にアクセスした覚えはないとのことでした。ただ、一週間ほど前に情報システム部と名乗る人からAさんに次のような電話がかかってきたということでした。

**B「情報システム部のBです。Webuシステムのメンテナンス中でユーザーIDとパスワードを再登録しています。確認させてもらえますか？」**

**A「はい。ユーザーIDは『88686』でパスワードは『AN701005』です。」**

実際には、情報システム部にはBという担当者はおらず、部外者による「なりすまし」でした。さらに「保険契約者リスト」以外にも漏えいしているﾃﾞｰﾀがあることが判明しました。

**事例05**

**確認しよう**

**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」とは、巧みな話術・盗み見・盗み聞きなどの方法を駆使して、不正アクセスのための情報を収集することです。

具体的な方法としては、なりすましやのぞき見、トラッシングなどが考えられます。

**対策案**

ユーザーIDやﾊﾟｽﾜｰﾄﾞはどんな状況でも他人には教えない。

代行処理などでやむを得ず教えた場合は速やかにパスワードを変更する。