マイナンバーへの対応を急げ！（第5回）

マイナンバー前夜に相次ぐサイバー攻撃被害

2015.10.21

マイナンバーをきっかけに、本格的に情報漏えい対策に取り組み始めた企業も多いことと思います。どの企業でも、特定個人情報以外にもさまざまな情報を保持しています。これらの情報を守り、顧客や取引先に迷惑を掛けないために、情報漏えい対策は不可欠です。

しかしマイナンバー前夜にサイバー攻撃被害が相次いでいます。情報漏えい事件といえば、5月に起きた日本年金機構の事件がまだ記憶に新しいでしょう。125万件もの個人情報を流出させてしまったきっかけは、職員宛てに送られた「標的型攻撃メール」といわれています。

「標的型攻撃メール」という名前には、ものものしい印象がありますが、実は非常に身近な話題を偽装した、添付ファイル付きのメール。例えば「健康診断のお知らせ」とか「セキュリティ対策について」など、誰しもうっかり、もしくは忙しさに紛れてつい、よく確認せずに開いてしまいそうなシロモノ。これを開いたことがきっかけでパソコンがウイルスに感染し、それが職場のネットワークから情報が盗まれるきっかけになるのです。

ハッカーは、そんな身近な、誰にでも可能性のありそうなミスを誘って、大切な情報を狙います。「こんなメールは不特定多数にばらまかれているだろうから、私ぐらいが開いてもどうってことない」などと侮っていると、実は計画的に仕組まれていて、あなたや同僚、職場のパソコンの利用者など、ターゲットを絞って送られて来ているものだったりします。職場内の誰かの、ちょっとしたダブルクリック1つで、大変な事態が引き起こされてしまいます。

マイナンバー対策をきっかけに、情報漏えい対策の必要性が多く語られているにもかかわらず、相変わらずさまざまな機関でのサイバー攻撃被害が報告されています。全国健康保険協会（協会けんぽ）、東京商工会議所、石油連盟、国立精神・神経医療研究センター、早稲田大学などが挙げられます。

中でも大規模なのは長野県上田市です。上田市に至っては6月に起きた事件以降、サイト上で「標的型サイバー攻撃を受けたため上田市役所では現在インターネットを遮断しています」と告知し、約3カ月もの間インターネットから遮断された状態でした。

これらのサイバー攻撃被害も、きっかけのほとんどが標的型攻撃メールでした。上田市の場合も、職員に送られたメールに添付されてきた書類は「医療費通知」というファイルだったといわれています。

「分散管理で安全」といわれているが…… 続きを読む