知って納得！
覚えて安心！

個人情報保護法の１～１０まで

この春、あるニュースにより個人情報保護やセキュリティ関係者のみならず、産業界全体に衝撃が走りました。みなさんも報道で見聞きされたことと思いますが、ソニーの米国関連会社からの大量の個人情報の流出です。ハッカーによるサーバーへの不正アクセスが原因で、その攻撃対象は１社にとどまらず、合計１億人超というかつてない規模の個人情報の流出につながりました。流出した個人情報の中には、クレジットカードの情報も含まれていたために悪用されるのではないかとの憶測も一時流れ、訴訟の動きも報じられるなどソニー全体のブランドと信用を大きく失墜させる事態となってしまいました。

この事件には、ある著名ハッカーとソニーの対立という独特の背景もあるようで、「自分たちにはここまでのことは起こらないだろう」という見方もできます。しかし、今回ソニーへの非難の声が高まった原因は、個人情報の流出そのものだけでなく「この事態を招いた根本原因」と「事故発覚後の対応」にありました。この部分は、企業規模に関わらず学ぶべき点があるようです。

■認識している危険を放置しない

今回のハッカーによる攻撃は、専門家によれば事前に防ぐことができたそうです。サーバーに組み込まれたソフトウェアの弱点を突かれてデータ流出につながったのですが、この弱点は既に知られたものだったようです。その弱点への対応を怠ったことで、サーバーへの不正侵入を許してしまい、大規模な個人情報流出という結果を招きました。これは、サーバーやソフトウェアだけの問題ではありません。日々の業務で、個人情報をはじめとする機密情報の管理に不安な点はありませんか？パソコンやネットワーク上に限ったことではありません。オフィスやキャビネットの施錠や鍵の管理、重要データを複製する際の承認から廃棄にいたる手順、外部とのデータのやり取り、ＦＡＸ送信時のダイヤルミスの防止、退職者のデータ持ち去りについての確認、伝票やデータの廃棄の手順など「このやり方で大丈夫なのかな？」とふとよぎる不安や疑問に、個人情報の流出を防ぐヒントはあります。そして、こういった小さな点を見逃すことが大きな事故につながりかねないのです。情報管理において「危険」を察知するアラームを敏感に機能させ、察知したらその場で解決していくことが大切です。

■事故公表のタイミングをはずさない

ソニーが大きな批判を浴びることになったもう１つの要因が事故の発表の遅さです。サーバーへの不正アクセスに気づいてから公表まで６日経過しました。ソニー側は、事実関係をきちんと把握するためにはこれだけの日数が必要だったとしていますが、その発表の方法が記者会見などではなくブログの記事だったことも含めて、消費者を軽視した対応だという厳しい声が寄せられています。確かに事故が発覚した場合、事実関係を明らかにし正しい状況を報告することは大切です。しかし、それと同じかそれ以上にスピードも重要です。関係者におよぶかもしれない不具合を考えれば、まずは事故発生を知らせ、注意を喚起するべきだったでしょう。事故発生時の対応では、迅速さと誠実さが重要です。そのために、個人情報の流出などの事故が発生した際の体制を事前に決めておき、対応手順のシミュレーションをして、万一の事態に備えておくことも必要でしょう。

■セキュリティのチェックシートも活用を

最後に「自社のネットワーク環境のセキュリティに不備はないか」という視点も重要です。インターネット上でもセキュリティに関する確認事項やチェックシートが公開されています。「経済産業省　セキュリティチェックシート」や「ＮＰＯ法人日本ネットワークセキュリティ協会　セキュリティチェックシート」といったキーワードで検索してみてください。各機関が提供しているチェックシートや利用方法が紹介されているページがあります。

以上となりますが、上記に掲げた点を踏まえ、万全な体制で日々の業務に取り組みたいですね。