講座

Web広告

村山　哲治

サイトの運用における「個人情報管理」大丈夫ですか？

■簡単に入手できるようになった「個人情報」

10月８日，Googleが提供するＳＮＳサービス「グーグルプラス」が2018月８月で終了するという発表がありました。驚くべきことに，そこで50万人分の個人情報が流出した恐れがあるといいます。しかし，実際にはそうした状況をもっと早く察知していたにもかかわらず，その公表が遅れたことで，これは今後いろいろな形で波紋を広げそうです。

こうした個人情報に関するトラブルは，もう慣れっこになってしまうほど年に何度も発生しています。その背景には，個人でも情報サービスやＥＣサイトを運営するようになり，簡単に個人情報の収集，加工，利用ができるようになった反面，情報管理の脆弱性などからデータが漏洩したり，世界中に拡散されたりといったことに関する危機管理の認識や知識が追いついていないことがあります。グーグルのような大企業でさえもこうしたことが発生してしまうのですから，そのセキュリティ技術や管理体制も高度なものになっています。では一般のサイトを運用する我々にとっては，個人情報の保護について最低限どのようなことを知っておかなければならないかを解説してみたいと思います。

■2017年５月に改正された「個人情報保護法」のポイント

「個人情報保護法」は2005年に施行されて10年以上経過し，2017年５月にネット環境の変化によりその内容が一部改正されました。そのポイントをいくつか拾ってみます。

●「個人情報」の保護範囲が広がる

これまで「個人情報」とされていた範囲は個人の属性（氏名・年齢・職業・家族構成・勤務先など）が中心ですが，それに加えて最近の技術や制度で生まれたデータが含まれるようになりました。

＜改正によって追加されたもの＞

- 指紋データや遺伝子データのような身体の一部をデータ化した情報
- マイナンバーのように個人に割り振られる個人識別番号
- 移動履歴や購買履歴などの情報

●個人情報の取扱量が撤廃される

これまでは個人情報の取扱事業者は「5,000人分以上の個人情報」が対象となっていましたが，その取扱量に関係なくほぼ全事業者が対象になりました。

●ビッグデータの情報が活用できる

個人情報を利用する場合，その個人から同意を得られた範囲内でした。しかし，産業競争力に欠かせなくなったビッグデータやＤＭＰを早く誰もが活用できるようにするためには，一人ひとりから同意を得ることは不可能であり，「個人情報」に該当しないようにデータを加工して「匿名化」することで，活用できるようになりました。

●個人情報のトレーサビリティ

個人データをどこから取得したのか，適正に取得された情報かどうかを確認することが義務付けられるようになりました。また情報の入手経路や手段，それをいつどこへどのよ

うに渡したかといった記録も必要となりました。

この他にも改正内容は多々あります。それに伴って一度作ったきりになっているWebサイトの情報管理対策などを見直してみてはいかがでしょうか。

■サイト運営における情報マネジメント

サイト運営者の多くは「個人情報」「セキュリティ」の対策は必要だし慎重に行わなければならないと感じつつも，システム任せであったり，外部のアウトソーシング先の運用任せになっていたりしないでしょうか。

例えばＥＣサイト運営において，顧客ニーズを満たす要素は，商品スペックや価格だけではありません。その前提に「安心して買い物ができる」ことが重要です。最近のWebマーケティングの主流であるＭＡ（マーケティングオートメーション）を行っているサイトにしても然りです。ホワイトペーパーをダウンロードするにしても安心感がなければ，なかなか詳細の情報まで記述する気にはなれないと思います。この安心とは，セキュリティ面での不安や個人情報漏えいのリスクに対して，しっかりとした管理がなされているかという点がポイントとなります。

そのためには，他社の「プライバシーポリシー」をコピペして体裁を整えるだけではなく，改正された「個人情報保護法」の概要くらいは理解して，サイトの情報マネジメントのポリシーをしっかり構築しておく必要があります。

あなたの会社ではセキュリティ管理の不備から顧客の個人情報が漏えいした場合の対処まで考えているでしょうか。まず漏洩した情報は回収することはできません。漏洩した顧客情報はその後，スパムメールやセールスの勧誘，犯罪に使用される可能性もあります。

それによって，企業イメージ低下や信用失墜，株価下落，売り上げ減少，訴訟や損害賠償請求と，負の連鎖はとどまることなく会社にダメージを与えることになるでしょう。

情報漏えいを防げるのは，あくまで運営者側であるということを忘れてはいけません。

■運営者側で行うべきセキュリティ対策

このようなリスクに対して運営側の行うべき対策は大きく「内部対策」と「外部対策」の二つがあります。一般的なイメージとしては，外部からのハッキングやウイルス攻撃，なりすましといった外部からのリスクが非常に大きいと思われがちですが，実際には運営者側の内部の不注意やミス，犯行によるものが多いのです。

内部犯行の代表的な対策として「顧客情報の社外持ち出し禁止」の徹底が挙げられます。

仕事を家でも行おうと，ＵＳＢメモリーや業務用ＰＣを自宅に持ち帰るというケースが多いようですが，そこで紛失や流出することが多いため，アルバイトやパートも含めて雇用時に顧客の個人情報持ち出し禁止を認識させ，同意書を得る必要があります。

では外部対策として「ウイルス感染」に対処するにはどうしたらよいでしょうか。まず感染させない対策と，感染してしまった時に被害を最小限に留める対策と，被害が出てしまった時の対応策の３段階をあらかじめ立てておくことが必要です。

こうした運用を実践するためには，まず個人情報にアクセス出来るスタッフを定め，利用範囲を明確にしておくこと。そして個人情報取り扱いの責任者を決め，問題が発生した時の対応フローと体制を決めておくことが大切です。それに加えて，そうした関係者には定期的な情報管理教育が必要となります。

（東京ドアーズ／人間力教育センター代表）