14　システムのセキュリティー

昨今のインターネット事情としまして、巷では、いわゆるコンピューターウイルス、スパイウェア等の様々な脅威であふれています。どのようなモノがあるのか、まずは敵を知り、自分とお客様を守るための準備をしましょう。万が一　情報が流出して、それがニュースにでもなったら、たったの一度でも、すべての信頼を失う恐れがあります。まさかじぶんが・・・と必ず皆さん口をそろえて言いますが本当に大丈夫でしょうか？

●システムのセキュリティー

ネットショップでは、お客様からインターネットを経由して個人情報をいただき、その情報をネットワークでつながったパソコン上で管理する。そのため、Web サーバー、ネットワーク、作業用 PC といったシステムのセキュリティーが非常に重要になる。2010 年度を振り返ってみると、ガンブラーウイルスを利用したアカウント情報の窃取等の、悪意のある活動は引き続き国内外に大きな被害をもたらした。G　Data　Software のレポートによると、2010 年の一年間に約 200 万の新種マルウェアが発生したとされている。また、ＯＳや定番ソフトウェアの脆弱性を狙った攻撃も多く、特に発見時期の古い脆弱性を悪用する攻撃が多発した。まずはこれらの脅威をタイプ別に理解したい。

※ガンブラーウイルス…ホームページを改ざんし、そのホームページを閲覧した人のパソコンをウイルス感染させる攻撃手法

※マルウェア…ウイルス、スパイウェア、ボット等悪意のあるソフトウェアの総称

●コンピューターウイルス

コンピューターウイルスとは、電子メールやＷｅｂサイト閲覧、ＯＳやアプリケーションの脆弱性経由で利用者のコンピューターに侵入する悪意のあるプログラムである。コンピューターウイルスは、作業用のパソコンのシステムを破壊するだけではなく、中にはメールソフトのアドレス帳や受信箱を利用して、ウイルス付きのメールをばら撒くといった行動をとるものもある。このようなウイルスに感染すると、お客様にウイルスをばらまくことになり、広範囲に重大な被害をもたらすことも考えられる。ウイルスをばらまいたネットショップは、被害者ではなく加害者とみなされ、ショップの信頼が大きく下がることになる。またガンブラーウイルス等、Ｗｅｂサーバーを攻撃対象としたウイルスに感染すると、ネットショップのサイトが改ざんされて、お客様が悪意あるサイトに誘導され、そこで個人情報等を入力してしまう等、大きな被害が出る可能性がある。

14　システムのセキュリティー

●スパイウェア

スパイウェアとは、利用者の意図に反してコンピューターにインストールされ、個人情報やアクセス履歴等の情報を収集し、外部に送信する悪意あるプログラムのことをいう。スパイウェアに侵入されると、お客様の個人情報やネットショップの機密情報が外部に流失する可能性がある。

●ボット

悪意のあるプログラムの中で、コンピューターに無断侵入し、コンピューターを遠隔操作することを目的としたものをボットと呼ぶ。作業用パソコン、Ｗｅｂサーバーともにボットに侵入されると、スパムメールの大量配信や特定サイトへの攻撃加担、個人情報やアクセス履歴等の情報を収集し外部に送信するなど、深刻な被害をもたらす。コンピューターウイルスへの感染拡大と同様に、スパムメールの大量配信や特定サイトへの攻撃加担を行ったネットショップは、被害者ではなく加害者とみなされるため、十分に注意をする必要がある。

●そのほかの攻撃

上記に挙げたマルウェア以外にも、データベースの脆弱性を攻撃するＳＱＬインジェクション、踏み台とされた複数のコンピューターが、標的を攻撃するＤＯＳ攻撃といったＷｅｂサーバーを標的とした脅威や、社内ネットワークの不正侵入、無線ＬＡＮ不正利用や盗聴等、様々な脅威が存在する。

★これらの脅威からお客様とショップを守る代表的な対策★

●作業用パソコンにおける主なシステム対策（一般スタッフ向け）

・アンチウイルスソフトウェア、アンチスパイウェアの導入
・アンチウイルスソフトウェア、アンチスパイウェアの定期的な定義ファイルの更新およびスキャン
・コンピューターのＯＳやアプリケーションを常に最新にする
・メールの添付ファイルに仕込まれたウイルス等への注意
・便利なツールに見せかけたスパイウェアへの注意
・ウイルスやスパイウェア混入の可能性がある、怪しいサイトにはアクセスしない
・不正アクセス防止の為パーソナルファイアーウォールの利用
・ブラウザ等のセキュリティーオプションの利用

14　システムのセキュリティー

●社内ネットワークにおけるシステム対策（システム管理者やマネージャー向け）
・ルーターの正しい設定
・ファイアーウォールの設定
・無線ＬＡＮのセキュリティー設定

●Ｗｅｂサーバーにおける主なシステム対策（システム管理者やマネージャー向け）
・個人情報をお客様より取得する場合は必ずＳＳＬを利用して通信を暗号化する。
・ＯＳや利用アプリケーションに適切なセキュリティー対策用の更新プログラムを適応する。
・迷惑メール対策サービスの利用
・ネットショップの管理画面への適切なアクセス制限
・通信の暗号化および認証
・データの保護とＷｅｂサーバーのバックアップ
・アンチウイルスソフトウェアおよびファイアーウォールの利用

※参考文献「ネットショップ検定　公式テキスト」より一部抜粋

過剰に心配する必要はありませんが、パソコンで使用しているソフト・ＯＳ等を常に最新バージョンにアップデートしておくことは非常に重要です。
なにはなくとも、最低限、アップデートは必ず行うようにしましょう。可能であれば、プライベート用のパソコンと、ネットショップ用のパソコンを別にして、リスクを減らすようにしてください。それだけで、相当量の危機を回避することが出来ます。逆にいえば、それだけプライベートでの使用環境が危険にさらされているという事になります。しっかりと上記の対策を行っておけばそんなに恐れることはないのですが、ここは私の方で脅かしておいて、本気で対策をしていただきたいところです。