

◎ラップ東京では、皆様のお役に立てるような様々な内容のコラムを発信しています。バックナンバーは www.raptokyo.co.jp から

「しつかり者」

先日、普段お世話になっているサーバ専門会社、いわゆるサーバのプロ集団の方と情報交換をしました。何度かラップニュースでも書きましたが、フィッシング詐欺や情報漏洩のきっかけは、メールであることが多いのです。そこで、こんな話を伺いました。

ある大手の建設会社と、その子会社であるシステム会社が、社内のセキュリティ意識向上のため、フィッシング対策の「訓練メール」を送ったそうです。受信しても開封してはいけない「訓練メール」です。結果はというと、システム会社では開封率が1%未満だったのに対し、建設会社では約65%の人が開封していたとのことでした。最初は一通のメールから、次第に社内、取引先などにも広がっていき、中枢部に侵入される。この話を伺って、日頃から注意を払うことの重要性を改めて感じました。

私たちは、メールは「送信できれば受信できるもの」、つまり双方向でやり取りできるのが当たり前だと考えがちです。しかし、実際にはその前提が少しずつ変わり始めています。例えば、自社のメールサーバが適切に判断できる「しつかり者」だった場合、送信側（例えばお客様）のメールサーバに何らかの問題があると判断されれば、自社ではそのメールを受信しません。「お客様からのメールが届きません」と連絡しても、お客様側からは「何度も送っていますよ」と言われてしまうこととなります。実際には、自社側の「しつかり者」が安全のために遮断しているのですが、そのお客様も、なぜメールが届かないのか

理解できずにトラブルになる可能性があります。

メールに関しては、今後、双方が正しい認識を持っていないと、予期せぬ事態が起こり得るということを理解しておくことが重要だと思います。

これまでインターネットは、ある意味「性善説」で成り立っていました。しかし、あまりにもインターネット、特にメールをきっかけとした犯罪が増えてしまいました。そのため、サーバ受信時にウイルスを駆除するという考えから、そもそも、怪しいメールを受信しないという流れになってきています。

私は工作上、Gmailを利用していますが、最近Gmailに届くメールの数が少ないと感じます。GmailやMicrosoftなどが提供しているメールサービスは「しつかり者」のひとつです。フィッシングメールを防ぐだけでなく、送信元が正しく送信しているか、そのメールは偽造されていないかどうかとも判断し、不要なメールはユーザーに届く前に破棄します。そのため、私の使っているGmailも余計なメールを受信せず、数が少なくなっていたというわけです。

メールのセキュリティは、日進月歩で進化しています。メールは便利なツールですが、その仕組みや変化を正しく理解して使うことが、これまでに以上に重要になってきています。メールサーバの移転はかなり大変な作業ですが、今後検討が必要だと考えています。

ご案内

ホームページの更新、変更（文章や写真の変更）などお気軽にご相談ください。

LINEからどうぞ。

ラップ東京公式
LINE



@750evjfo

【お問合せ】
ラップ東京株式会社
TEL:042-349-3535

