

©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

「迷惑メールはどこから?」

私のところには、一日に数百通の迷惑メールが届きます。最近ではさらに増えているように感じ、お客様からも「迷惑メールをどうにかできないか?」という問い合わせが多く寄せられます。

対策として、Gmailなどのクラウドサービスを利用すれば迷惑メールのフィルタリングが強化されますが、独自ドメインでクラウドサービスを使うのは手間がかかります。また、ホームページ用のサーバーとメールサーバーを分けるには、新たなコストが発生する場合があります。

さて、迷惑メールはどこから来るのか? 多くの迷惑メールは海外から送信されますが、一部は国内のサーバー経由で届くものもあります。迷惑メールの送信者は、自分のサーバーから直接送ることはありません。多くは、第三者のサーバーのメールアドレスとパスワードを奪取し、そのサーバーを利用して一度に数万件ものメールを大量送信します。

このように悪用されたサーバーは、迷惑メールの送信元とみなされ、インターネット上でブラックリストに登録されます。送信しても、経由するサーバーや受信先のサーバーが「このサーバーからのメールは迷惑メールの送信元だ」と判断し、受信や中継を拒否するため、結果的に送信できなくなります。復旧には状況にもよりますが、数日から数週間かかることもあります。

最も基本的な防御策は、メールのパスワードを複雑にすることです。私が設定権限を持っている場合、

パスワードは10桁程度に設定しています。過去に、パスワードが奪取された事例をみると、お客様側の設定パスワードが短かったり、簡単な組み合わせだったケースが見られました。パスワードは、文字の組み合わせが増えるほど解読されにくくなります。例えば、英数字(記号は含めず)だけで考えた場合、英大文字26種類、英小文字26種類、数字10で62種類になります。6桁の場合、 $62 \times 62 \times 62 \times 62 \times 62 \times 62$ は約56億通りになります。7桁にすると、さらに62を掛けるので、約3兆通り、8桁にすると、なんと218兆通りです。6桁から8桁にするだけで、3844倍になるそうです。

攻撃者は時間をかけて攻撃を試みるため、パスワードを強化しても100%安全とは言えません。しかし、最低限の対策として、パスワードの複雑化は必須だと思います。

迷惑メールの多くは、第三者のサーバーが悪用されていて、私自身も、いつ被害者の一人になってしまうかわかりません。また、最近の迷惑メールは見た目や内容も巧妙化しており、一見すると本物のメールと区別がつかないものも増えています。迷惑メールの送信者として悪用されないよう、しっかりとパスワードを管理し、受信側としては少しでも怪しいと思ったら、そのメール内のURLをクリックしないことが重要です。特に、通販サイトやネットバンクなどへのログインは注意です。

ご案内

それほど高機能ではなく、
更新したいページを簡単に更新できる

簡単更新くん

「つながりたい」をサポートする

簡単らいんちゃん

【この件に関するお問合せ】
ラップ東京株式会社
(担当：田島)
TEL:042-349-3535

ラップニュース バックナンバーはホームページからご覧いただけます。

アンケートがありますのでよろしかったら、ご意見をお聞かせください。 <https://www.raptokyo.co.jp/>

