

2025年10月19日

フィッシング（詐欺）メールにご注意

IT サロン 玉上 佳彦

最近のインターネット上の詐欺メールをフィッシング（phishing）メールといいますが、あたかも正規の発信元を偽装したメールによる被害が頻発しているようです。

実在する会社・団体からのフィッシングメールは、大量に皆さんのメールアドレス宛に送られている可能性があります。以下の点につき、ご注意下さい。

- 最近特に目立って多くなっているフィッシングメールは、以下の会社を偽装したものが多くあるようです。

通販会社：Amazon、楽天市場、Yahoo、ベルーナ、メルカリなど

銀行：みずほ、JA バンク、イオン銀行など

カード会社：JCB、VISA、マスターカード、AMEX、ジャックスなど

証券会社：野村證券、SBI 証券、楽天証券、マネックス証券、大和証券など

役所関係：総務省、税務署、国勢調査関係、東京電力、東京ガス、日本郵便など

運送業者：佐川急便、ヤマト運輸、DHL など

その他： JAL、ANA、Apple、ETC、エキネット、ニンテンドーなど

● 【対策】

- ・メールを開く前に、送信元のアドレスを確認し、不自然なアドレスの場合はすぐ削除する。フィッシングメールの送信元アドレスは、正規の発信元メールではない無関係のアドレスの場合が多く、気がつきやすいです。
- ・もし、メールを開いてしまった場合は、メール本文中の出ている URL を絶対にクリックしない。
- ・パスワードの入力やクレジット番号などを要求される場合には、特に注意する。
- ・上記の URL をクリックして怪しげなページが出てきた場合には、すぐに PC をシャットダウンして、正規のアドレス元に連絡し、対処方法を相談して下さい。

たいへん恥ずかしい話ですが、私は先日取引のある証券会社のページの送信元アドレスを確認せずに、パスワードを入力してしまいました。持っていた株が売却され、知らない会社の株を買付けされました。即日に気がついたので、証券会社に連絡し、取引制限をかけて、改めて2種のパスワードを再設定することで解決できました。僅かですが 10万円ほどの損失を被ってしまいました。取引のある証券会社だからといって、送信元のアドレスを確認せずに、メールを開いて、パスワードを入力しないようにお気をつけ下さい。