当法人職員を装った不審メール(なりすましメール)にご注意ください

令和４年３月３日から、当法人職員を装った不審メール（なりすましメール）が複数の当法人職員に送信されていることを確認いたしました。

不審なメールには解凍（zip）ファイルが添付されており、中のファイルを開きますと、マルウェア「 Emotet（エモテット)」感染や不正アクセス等の恐れがあります。

３月３日現在、当法人において当該マルウェアに感染したパソコン等は発見されておりませんが、当法人職員及び事業所を装った不審メールが社外の方へも送信されている可能性があります。これらは当法人職員および事業所になりすました不正なメールであり、当法人から送信されたものではありません。

当法人を装った不審なメールや心当たりのないメールを受信した際は、ウイルス感染や不正アクセスなどの危険がありますので、メールに添付されているファイルを開かず、メールごと削除していただきますようお願い申し上げます。

現在、当法人で把握している不審メールの内容は以下のとおりです。

【不審メール例】

差出人：〇〇〇(当法人職員又は事業所名)＜当法人とは異なるドメインのメールアドレス＞

件　名：***UNCHECKED***　　RE: 〇〇〇(当法人職員又は事業所名)

添付ファイル：解凍（zip）ファイルまたはエクセルファイル（xlsm）

本文例：（１）以下メールの添付ファイルの解凍パスワードをお知らせします。

添付ファイル名:〇〇〇（添付された zip ファイル名）

解凍パスワード: 53516（記載されるパスワードは異なります）

（２）ご確認をお願いします。

宜しく御願い致します。

〇〇〇（事業所名）〇〇（職員名）

〇〇〇（実在するメールアドレス）

なお、なりすましメールの特徴として、以下のような特徴があります。

・市外局番「044」から始まる電話番号、FAX 番号が記載されている場合がある

・「090」から始まる携帯電話番号が記載されている場合がある

・メール本文に挨拶や前置きがない

・メールに解凍（zip）ファイルやエクセル（xlsm）ファイルが添付されている

・メール本文に ZIP 圧縮ファイルのパスワードが記載され、開封を促している

これらのメールを受信した場合、絶対に添付ファイルを開かないでください。

また、送信名ではなく、送信元アドレスを必ずご確認ください。

何卒ご理解、ご協力を賜りますようお願い申し上げます。