会社名や個人名を装った「なりすましメール」に注意

昨今、実在する会社名や個人名を名乗り、一瞬「自分に関係があるかも？」
と思わせる巧妙な迷惑メール（なりすましメール）が全国的に急増しています。
会社の情報を守るため、取引先へ被害を広げないため、一人一人が注意徹底しましょう！

1 どこで「感染・被害」が起きるのか？

迷惑メールの被害の多くは、
<u>添付ファイルの開封やURLのクリックをきっかけに発生</u>します。
以下の「3つの操作をしない」ことを社内で周知し、徹底しましょう！

返信する

やり取りの中で
ダマされる可能性が高まります

添付ファイルを開く

ウイルス感染の
原因になります

本文のURLをクリックする

偽サイトへ誘導され、
情報を盗まれます

2 「怪しい」と見抜くチェックポイント

少しでも「あれ？」と思ったら、以下の点を確認してください。

「知っている名前」でも、まずは疑う

犯人は信頼させるために
実名や具体名を使用します。
「知っている名前＝安全」
ではありません。

メールアドレスが不自然ではないか？

送信者名は偽装できます。
必ずメールアドレスそのものを
確認してください。

不自然 ＝ フリーメール
一文字違いのドメイン など

日本語が不自然ではないか？

「てにをは」がおかしい、
日本で使わない漢字
が混じっている
場合は要注意です。

3 迷ったら、「開かず、検索・確認」！

知らない電話番号からの着信を無視して、後で番号を調べるのと同じです。
少しでもおかしいメールは、**<u>開かず・返信せず・そのまま削除</u>**してください。
判断に迷う場合は、相手先の**<u>公式サイトや以前から使用している名刺等の連絡先</u>**など、別の手段で確認することをおすすめします。
誤って開封・クリックした場合は、社内の担当者にスグに連絡しましょう。

長岡商工会議所