「役員」や「社長」になりすました詐欺メールにご注意ください

法人・企業の「役員」や「社長」になりすました詐欺メールを送信し、従業員に「お金を振り込ませる」「SNS のグループを作成させる」「機密情報を送らせる」などの指示を行う詐欺（いわゆる CEO 詐欺※）が全国で確認されています。　（本会にも同様のメールを確認しております）

役員や社長になりすました詐欺メールは、法人・企業や従業員のみでなく、関係者に対しても送信されていることが確認されています。不審なメールを受け取った場合は、開封したり返信したりせず、送信元が正しいか必ずご確認ください。

※社長など最高経営責任者である「チーフ・エグゼクティブ・オフィサー（Chief Executive Officer）」になりすまして、従業員や取引先を騙し、金銭や機密情報を詐取する詐欺手口

１．詐欺メールに使われる手口

・ 理事長や経営者、上司になりすまし、「急ぎで対応してほしい」と振込や情報提供を求める。
・ 本物に似たメールアドレスを悪用して、正規の連絡に見せかける。
・ LINE グループの作成など、外部サービスへの誘導を行う。

【事例①（振込を指示する詐欺）】

件名：至急振込してください
差出人：理事長を装った偽アドレス
内容例：　商談に必要なため、至急振込をお願いします。
　　手続きは後回しで構いません。戻ったら説明します。
振込先：〇〇株式会社
金額：〇0,000,000 円
⇒　「至急」「会社に戻ったら説明する」などは、詐欺メールでよく使われる言い回しです。

【事例②（LINE グループ作成を依頼する詐欺）】

件名：法人名を記載した偽メール
差出人：理事長を装った偽アカウント
内容例：　お疲れ様です。
　　業務利用のため、新しい LINE グループを作成してください。
　　完了したら招待 QR コードを返信願います。
理事長（or 代表取締役社長）　〇〇
⇒ 会社では通常使用しない外部 SNS への誘導は、要注意ポイントです。

２．不審なメールを受け取った場合

・ 差出人のメールアドレスを必ず確認する。
・ 内容に不自然な点があれば、正当な相手（役員等）に直接電話で確認する。
・ リンクを開かない、添付ファイルをダウンロードしない。
・ 個人情報を送らない。