サイバーセキュリティパートナーシップだより

R8-2

社長をかたる詐欺メールの新手口！
マルウェア感染をねらう攻撃メールに注意

昨年12月頃から、会社の社長などをかたり、業務命令を装って、LINEグループの作成を要求した上で、指定の口座に送金させる「ビジネスメール詐欺」が確認されていましたが、類似事案として新たに、社長などをかたって添付ファイルのダウンロードを指示し、マルウェア感染に誘導する手口が確認されています。端末の感染被害につながるおそれがあるため、会社内の注意喚起をお願いいたします。

新たに確認された社長をかたるメール

注）画像は情報処理推進機構（IPA）公式Ｘから引用

① 差出人は実在の社長名などだが、メールアドレスが普段と異なる

文例１

株式会社［　　］

差出人　［　　］<［　　］@gmail.com>　←①

日付　2026/01/27 (火)

宛先　［　　］

1 個の添付ファイル (15 KB)　←②

今日の予定.pdf;

添付ファイルにマルウェアが仕込まれている可能性あり

オフィスにいますか？ ルーチンワークの詳細を添付しました。確認しておいてください

② 添付ファイルの形式：PDF、docx等

※件名や文面、ファイル名などは今後他のパターンの出現が予想されます。

文例２

宛先　［　　］　01/23 (金)　←①

ツール.docx
26 KB　←②

私の名前を騙って LINE グループを作成するメールが頻繁に届いています。絶対に信用しないでください。添付ファイルはメール遮断ツールです。直ちにダウンロードし、対策を講じて会社の経済的損失を防いでください。

③ 偽ツールをダウンロードするよう指示
（URLを記載してマルウェアのダウンロードサイトに誘導する場合もあります。）

【　被害にあわないための対策　】

- ◆ **社長などをかたった不審メールの手口について従業員等に注意喚起**
  同様のメールを受信しても**絶対に添付ファイルやＵＲＬを開かない**こと
- ◆ 社長の名前であっても、メールアドレス、添付ファイル、ＵＲＬなどをよく確認
- ◆ 不審メールを受信した場合には、メール以外の確実な手段で差出人に確認
- ◆ 万が一、ダウンロードしてしまった場合は、端末をネットから切り離し、会社のシステム担当等に報告するとともに、警察や関係機関に相談

サイバー犯罪相談事例
対処法と対策・相談窓口

山口県警察サイバー課ＬＩＮＥ友だち募集中！
サイバー犯罪に関する防犯情報を配信中です

山口県警察本部　サイバー犯罪対策課