

ウィルス感染を狙った不審メールに注意！

先日、注意喚起させていただいたビジネスメール詐欺を逆手にとり、経営者をかたってメールを送り、

メールに添付したファイルをダウンロードさせ、パソコンをマルウェア（コンピュータウィルス的一种）に感染させる

手口が確認されました。

マルウェア感染を狙った手口

- ① 企業のメールアドレスに経営者をかたる者から、不審メールの対策と称して、添付ファイル『メール遮断ツール』をダウンロードするよう指示される。
- ② ファイルをダウンロードすると、パソコン等がマルウェア感染

【企業・団体の代表者・社長をかたる偽メールの例（詳細は裏面へ）】



【件名】メールブロックツール

【内容】私の名前を名乗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、経済的損失を防いでください。

【内容】お疲れ様です。今、会社にいますか。

今後の業務プロジェクトに対応するため、

添付ファイルを確認のうえ、必要事項を入力してください。

【添付ファイル】XXX.zip

マルウェアに感染するとどうなるの？（過去の例）

総務省ホームページ参照

顧客情報など個人情報流出

コンピュータシステムの破壊

遠隔操作され、サイバー攻撃の踏み台に

データを暗号化され、身代金要求

警察からのお願い

マルウェア（ウィルス）に感染すると、金銭的被害だけでなく、顧客情報の流出やシステム障害等に発展し、企業の社会的信用低下や最悪の場合、業務停止につながる可能性があります。

以下の注意点について、従業員の皆様に早急に周知願います。

- ◆不審なメールの添付ファイルやURLをダウンロード(クリック)しない
- ◆経営者をかたる者からメール等で口座情報を聞かれたり、添付ファイルをダウンロードするよう指示されたら、連絡事実を確認する
- ◆組織内で情報共有し、自分だけで判断せず、上司やシステム管理者に報告する

同様のメールを受信した場合は、最寄りの警察署又は警察相談専用電話 #9110に相談してください。



山形県警察

不審メールの例

けいさつ商事株式会社

フリーメールアドレスが使われている場合があります。
普段から経営者が使用しているメールアドレスか要確認！

差出人: nisesyachop@saginomail.com
送信日時: 2026年1月28日水曜日 18:42
宛先: けいさつ商事株式会社
件名: 業務連絡
添付ファイル: 9374j198325622p.zip

おつかれさまです
今、会社にありますか

添付ファイルに
マルウェア（ウィルス）が
含まれている可能性がある

今後の業務プロジェクトに対応するため、添付ファイルを
確認のうえ、必要事項を入力してください

URLを記載して
マルウェアのダウンロードサイトに
誘導する場合もある

社長 詐欺山

↑ 法人の経営者などを名乗る

※実例を元に構成したものです

- ◆ フリーメールアドレスからのメールに添付されたファイルやURLは要注意
- ◆ 最新の手口を常に確認