



業務メールを装った サポート詐欺が急増中！！

要注意

現在、業務メールを装った「人事評価について」や「セキュリティ確認」などと偽り、偽の警告画面を表示させたうえ、サポート窓口へ電話するように仕向け、金銭を詐取するサポート詐欺が**急増**しています。

焦ってURLをクリックしたり、**絶対に**電話をしないようにしてください！

1 サポート詐欺の流れ

【メール文の例】※実際のメールを元に作成しています。

1. 基本的な人事評価確認を装った例

件名例:
【人事部】2026年度 人事評価結果のお知らせ / 【重要】貴方の評価結果が確定しました
本文例:

text
株式会社oo 人事部です。
全社員各位
2026年度上半期の人事評価が完了いたしました。
以下のリンクより、ご自身の評価結果およびフィードバックをご確認ください。

【評価確認リンク】
[https://\[redacted\].jp/\[redacted\]2026-result?emp=XXXXXX](https://[redacted].jp/[redacted]2026-result?emp=XXXXXX)

ログイン後、確認ボタンを押していただきますようお願いいたします。
※確認期限：2026年6月10日まで
対応がない場合、次回昇給に影響する可能性があります。

人事部 評価担当

3. 社内メール（会社・業務）を装った例（BEC風・内部偽装）

件名例:
【緊急】社内システムメンテナンスのお知らせ / 【総務部】セキュリティ確認のお願い
本文例:

text
株式会社oo 総務部です。
全社員各位
現在、社内メールサーバーのセキュリティ更新を行っております。
一部の社員でメール受信に不具合が発生しているため、以下のリンクより本人確認をお願いします。

【確認URL】
[https://co\[redacted\].jp/\[redacted\]](https://co[redacted].jp/[redacted])

ログイン後、簡単な確認作業を行っていただきます。
対応が遅れるとアカウントがロックされますのでご注意ください。

情報システム課

URLをクリックすると・・・

焦って電話すると・・・



大音量の警告音

**サポート名目の
金銭の要求！**

**遠隔操作ソフトの
インストール指示！
→意図に反する操作**

2 不審・見覚えのないメールが来た場合

お客様のコンピューターで深刻なウイルス感染が確認されました。
このままでは個人情報流出の危険性があります。

すぐに以下のリンクからサポートページにアクセスし、問題を解決して

▶ [https://\[redacted\]support-security.com/\[redacted\]](https://[redacted]support-security.com/[redacted])

または、下記電話番号でも対応可能です。
0120-XXX-XXX

24時間以内に連絡がない場合、アカウントがロックされます。
Microsoftサポート

- ・安易にクリックしない!
- ・送信元アドレスを確認!
- ・焦らず公式サイトURLを確認!

3 クリックしてしまった場合(警告表示のみ)



- ・まず社内で相談・情報共有!
- ・絶対に連絡をしない!
- ・ウィンドウを強制終了!
(ALT+CTRL+DEL)
または、PCの強制終了!
(電源ボタンの長押し)
- ・ウイルス対策ソフトでの感染有無のチェック!

4 相手に連絡をした場合



- ・怪しいと思ったらすぐに電話を切る!
(片言の日本語、AI音声等)
- ・サポートのためのソフトといわれてもインストールは絶対しない!
- ・金銭要求、カード番号の要求は詐欺!

詐欺に気付いたら110番!!

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク (通称:F-CSNET) とは、県内中小事業者のサイバー犯罪被害の未然防止・拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手法や対策などを、X (旧Twitter) やホームページに掲載していますので、ぜひご覧ください。

[X] (旧Twitter) [ホームページ]

