新型コロナウイルスに関する

「標的型メール」に要注意！！

標的型メールは、差出人が実在する組織名や個人名を使用し、みなさんの仕事に関係する内容の本文や件名にして、ウイルスが添付されたメール、悪質なWEBサイトのURLが記載されているメールを送り、メールを開かせて、ウイルスをダウンロードさせようとします。
ウイルスに感染すれば、パソコン内のメールアドレス情報やメール本文が盗まれて、その情報が新たな標的型メールを送信するために利用されるおそれがありますので、注意してください！！

メールの例

ファイル　メッセージ

差出人：〇〇保健所福祉室（〇〇@□□.jp）
宛先：△△（株）××課
件名：　通知　2020　Jan 29

メッセージ　instruction Jan 29 29292 .doc

〇〇　様

お世話になっております。

新型コロナウィルス関連肺炎については、中国武感市を中心に患者が報告されているところであり、

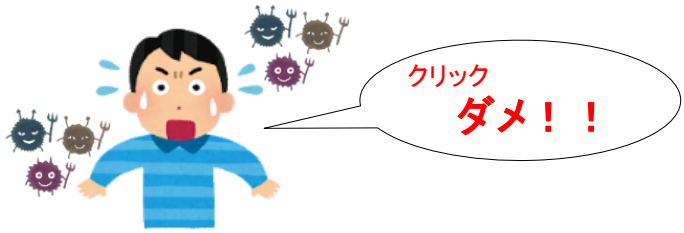
つきましては、別添通知をご確認いただき、
感染予防対策についてよろしくお願いいたします。
なお、並行して〇〇ページへの掲載準備をしております。

****
〇〇保健所福祉室（担当：□）
〒〇〇
電話：□□　FAX：△△
****

ここを注意！！

ファイルを開けば、プログラム（マクロ）の実行等を許可させようとする
「コンテンツの有効化」ボタン
が表示されます。
ボタンをクリックすることで、ウイルスに感染するおそれがあります。

表示される「コンテンツの有効化」ボタン



対　策　方　法

◎　差出人、件名を確認して、普段やり取りをしない差出人、自分の仕事内容とは関係ないメールは、添付ファイル、メール本文中のURLリンクを不用意にクリックしない

◎　件名の日本語が不自然であったり、【緊急】【重要】等のキーワードが誇張されているメールは、不用意に開かず、差出人に確認する

◎　パソコンのOS、ウィルス対策ソフトを常に最新のものに更新

◎　「Word」のセキュリティ設定で「警告を表示して、すべてのマクロを無効にする」を選択して、マクロの自動実行を無効化にしておく

設定方法　ファイル ➡ オプション ➡セキュリティセンター➡☑警告を表示してすべてのマクロを無効にする

◎　会社内での注意喚起を徹底する

参考：IPA 独立行政法人 情報処理推進機構（URL:https://www.ipa.go.jp/security/announce/20191202.html）
：厚生労働省（URL:https://www.mhlw.go.jp/stf/newpage_09393.html）

島根県警察本部 生活安全部 生活環境課 サイバー対策室　**TEL.0852-26-0110**