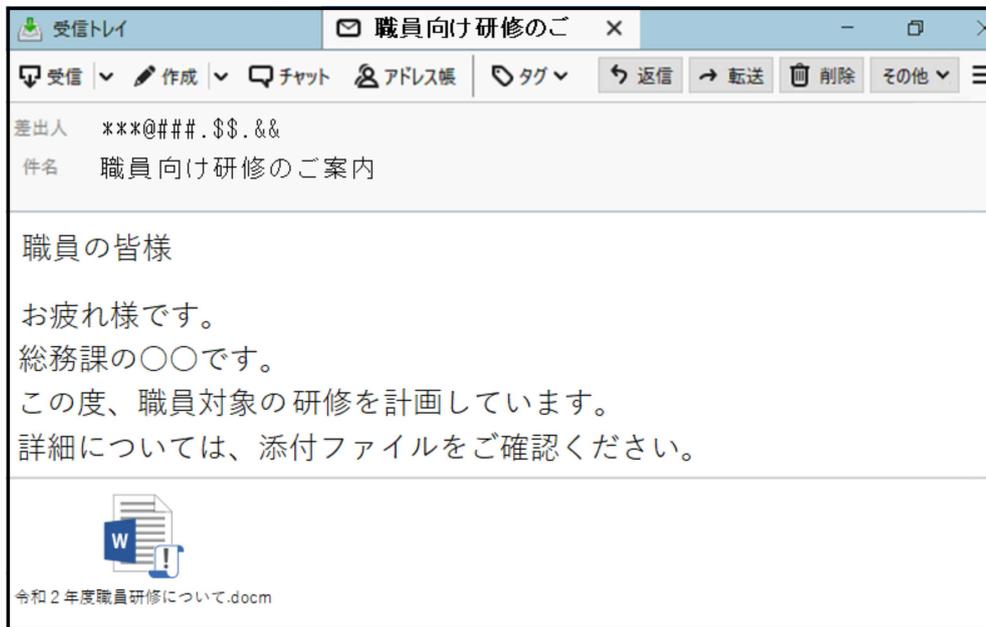




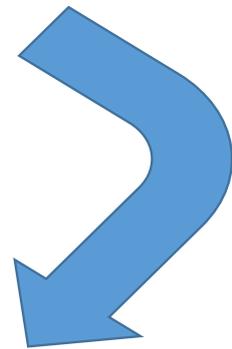
## 訓練用ファイルによるEmotet感染体験訓練を実施しました！

長崎県警察本部サイバー犯罪対策課では、Emotetの脅威を体験するため、Emotetと同じような動作をするマクロを含むWordファイルを作成し、感染体験訓練を実施しました。このWordファイルは、社員教育用などに使用していただくため、提供することが可能です。社内訓練用に作り替えるアドバイスも行いますので、お気軽にお問合せください。

< 画像はイメージです >



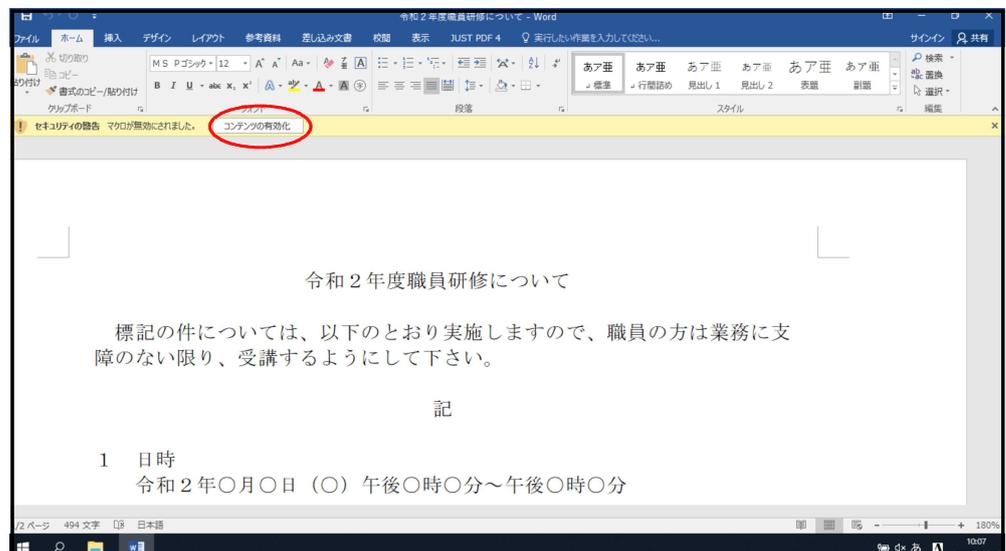
ある日、このようなメールが届きました。添付ファイルも普通のワードファイルのようです。



内容を確認してみると、本当に社員研修の案内でした。

よく見ると、何か表示があります。よくわかりませんが有効化しました。

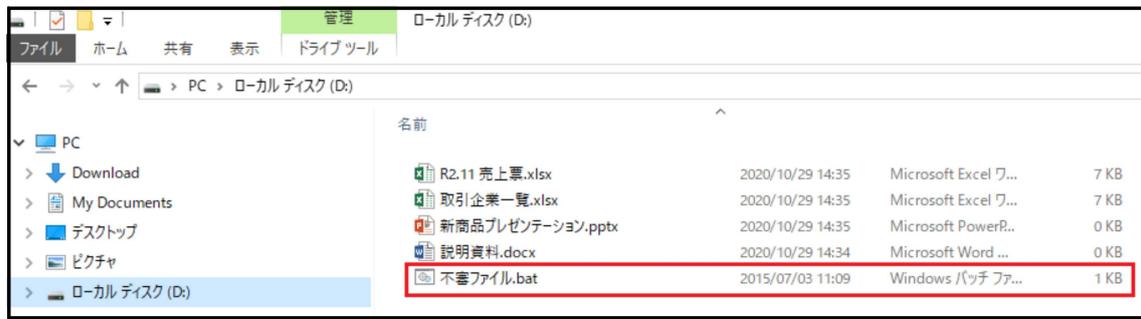
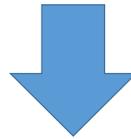
有効化しても、画面上には特に変化もありません。



でも実は、、



< マクロ実行前 >



< マクロ実行後 >

ご覧のとおり、気づかないうちに不審なファイルがダウンロードされていました。

この訓練では、パソコン内のフォルダに不審ファイルをダウンロードさせましたが、実際の被害を見てみると、普段は開かないような場所にあるフォルダや、スタートアップなどの起動するだけでファイルが実行される場所に保存されるなど、感染がわかりにくいように偽装されています。

もし、この不審ファイルが、情報流出を引き起こすマルウェアや、ランサムウェアなどの悪意のあるファイルの場合、知らないうちにダウンロード・実行されることにより、機密情報の漏えいや、パソコンが暗号化されてしまい、使用できなくなるなどの被害に遭うおそれがあります。

長崎県警察本部サイバー犯罪対策課  
095-820-0110 (3451・3452)  
メールアドレス e103108@police.pref.nagasaki.jp

サイバー犯罪対策課 LINE ID : @387ojopi

公式LINEアカウントで

情報配信中!

友だち登録をお願いします!

