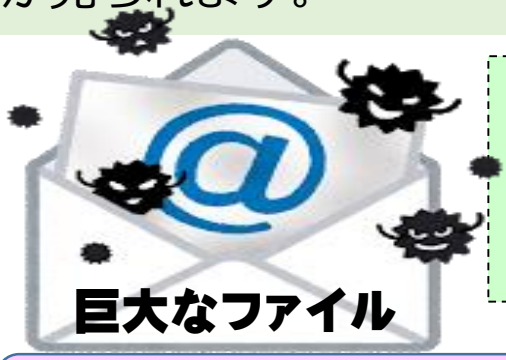
新たなEMOTETが確認されました

**３月、新たなEmotetの活動が確認されました。
道内の企業にも、Emotetウイルス添付型のメールが送付されてきています。**

今回新たに確認されたEmotetウイルスは、メールに添付されたzip圧縮ファイルを解凍すると、ファイルのサイズが500メガバイトを超えるワードファイル（.doc）が展開されるなどの変化が見られます。



解凍前は１メガバイトにも満たない添付ファイルですが、解凍（展開）すると、500メガバイトを超える巨大なファイルになります。
これは、アンチウイルスソフトによる検知の回避を図っているものと思われます。

Emotetとは･･･
感染端末の情報を盗み出す事に加え、他のウイルス感染のために悪用されるウイルスで、日々凶悪化し続けています。
主に添付ファイル付きのメールを用いて感染拡大し、正規のメールへの返信メールを装う手口が多く使われています。

今回のウイルスも、添付ファイルを開いて
「マクロを有効化する」と感染します。

- **不用意にメールの添付ファイルを開かない**
- **マクロは絶対に実行させない**
- **違和感を感じたら、送信元に電話等で確認する**

などし、ウイルスに感染しないように注意してください。

※本資料は一般社団法人JPCERTコーディネーションセンターの公開資料を参考に作成しております。
URL:https://www.jpcert.or.jp/at/2022/at220006.html

北海道警察サイバーセキュリティ対策本部