TCSP Toyama Prefectural Police Cyber Security Personnel
# サイバーセキュリティの置き薬
2020年 第24号

## インターネットバンキングの不正送金等の被害につながるメールに注意

現在、インターネットバンキングマルウェア「DreamBot」等の感染拡大を目的としているメールが日本を標的として大量に送信されています。

また、2020年２月上旬以降、「Emotet」の攻撃メールが観測されない状態が続いていましたが、７月中旬から「Emotet」の攻撃メール活動も再び観測されています。

### DreamBot（ドリームボット）

Amazonや楽天等といった企業を騙った不審なメールが確認されています。

不審なメールの添付ファイルを開いたり、本文中のリンクをクリックすることにより、マルウェア（DreamBot等）への感染等につながり、インターネットバンキングの不正送金などの犯罪被害にあうおそれがあります。

また中には、本文中に記載されているリンクからフィッシングサイトに誘導され、クレジットカード情報等の情報が窃取され、不正使用の被害にあうケースもあります。

### Emotet（エモテット）

Emotetは、情報の窃取に加え、更に他のウイルスへの感染のために悪用されるウイルスです。

Emotetへの感染を狙う攻撃メールの中には、正規のメールへの返信を装う手口が使われている場合があります。Emotetへの感染被害による情報窃取が、他者に対する新たな攻撃メールの材料とされてしまうおそれがあります。


### 不審なメールは開かない 添付ファイル、URLリンクに注意する マクロ動作を有効にしない

身に覚えのないメールの**添付ファイルは開かず**、メール本文中の**URLリンクはクリックしない**でください。

OSやアプリケーション、セキュリティソフトを常に**最新の状態**にしましょう。

信頼できないメールに添付されたWord文書やExcelファイルを開いたときに、マクロやセキュリティに関する警告が表示された場合**「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない**でください。

参考：JC3：不正送金等の犯罪被害につながるメールに注意（https://www.jc3.or.jp/topics/virusmail.html）

IPA独立行政法人情報処理推進機構：「Emotet」と呼ばれるウイルスへの感染を狙うメールについて（https://www.ipa.go.jp/security/announce/20191202.html）