サイバーセキュリティニュース
C S ー N E W S

三重県警察本部
サイバー犯罪対策課
059ー222ー0110

不正プログラム「Emotet（エモテット）」に注意

～ 県外で警察組織を装った不審なメールが確認されています ～

1　概要

窃取した情報を悪用し、感染拡大が目的のメールを送信します

- ◇ **Emotetは**、主にメールの添付ファイルを感染経路とした**不正プログラムです。**
- ◇ 過去にやり取りしたメールへの返信を装ったメールを送信し、添付ファイルの開封を促します。
- ◇ **Emotetに感染したパソコンから**メールアカウント、パスワード、メール本文等の**情報を窃取します。**

2　感染経路

Emotetの主な感染経路は、メールの添付ファイルです

- ◇ メールにはパスワード付きZIP形式で圧縮された文書ファイルが添付されており、パスワードはメールの本文に記載されています。
- ◇ 文書ファイルを開くと、ファイルに埋め込まれたマクロの実行を促す内容が表示され、実行するとEmotetに感染します。
- ◇ 過去には、メール本文に記載されたURLリンクや、メールに添付された圧縮されていない状態の文書ファイル等からEmotetに感染する事例も確認されています。
- ◇ 従来使われていた文書ファイルに替わり、メールショートカットファイルが添付される事例も確認されています。

3　Emotetに感染すると・・・以下のような影響があります

- ◇ メールソフトやブラウザに記録したパスワード等が窃取されます。
- ◇ 過去にやり取りしたメールの本文、メールアドレス等が窃取されます。
- ◆ **感染拡大を目的としたメールを送信するのに、窃取されたメール関連の情報が悪用されます。**
- ◇ ネットワーク内の他のパソコンに感染が拡大します。
- ◇ 他の不正プログラムに感染します。

実在する機関、企業等や、そのやり取りを装って、マルウェアに感染させるためのメールを送信します

4　被害防止のため、一般的なセキュリティ対策に加え、次のような対策を検討してください。

- ◆ 不審なメールだけでなく、自分が送信したメールへの返信に見えるメールであっても、不自然な点があれば添付ファイルは開かない、メール本文中のURLリンクはクリックしない
- ◆ メールに添付された文書ファイルを開いた時に、マクロやセキュリティに関する警告が表示された場合には、マクロを有効にしたり、セキュリティ警告を無視するような操作をしない