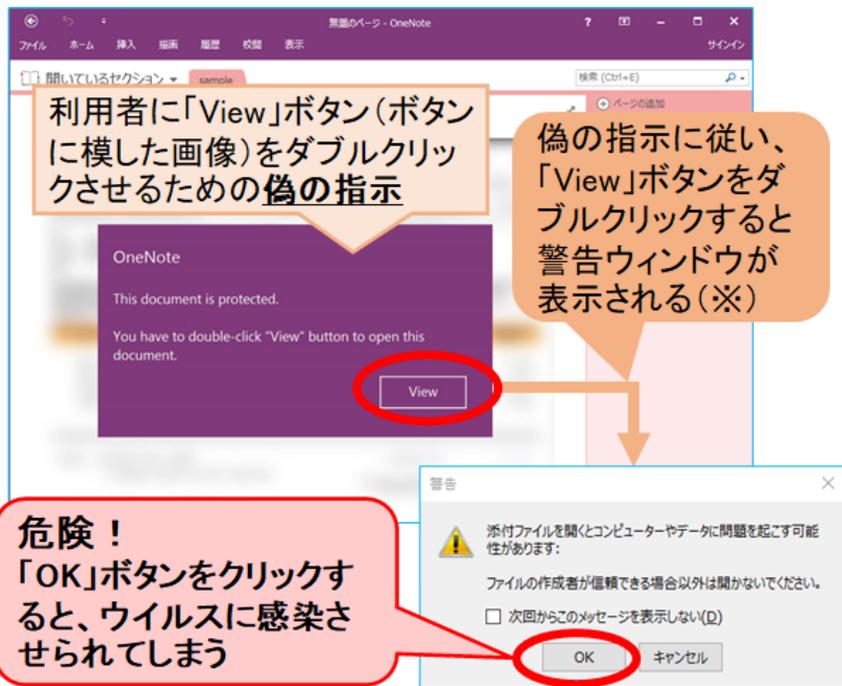


Emotetの新たな手口に注意！

Microsoft OneNote形式のファイル(.one) を悪用してEmotetへ感染させる新たな手口が確認されました。

攻撃メールに添付されたMicrosoft OneNote形式のファイルを開き、ファイル内に書かれた偽の指示に従って操作すると、Emotetに感染する恐れがあるため、注意が必要です。



左の図は新たな手口の一例です。攻撃メールの文面はこれまでと大きな違いはありません。

引き続き以下の対策をとっていただくようお願いいたします。



対策

- ・ 身に覚えのないメールの添付ファイルは開かない。本文中のURLリンクはクリックしない。
- ・ 自分が送信したメールへの返信と思われるメールでも、文面や添付ファイルの存在等少しでも不自然な点があれば、添付ファイルは開かない。
- ・ 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する。
- ・ 添付ファイルを開いた際、マクロやセキュリティに関する警告が表示された場合、「マクロを有効化する」「コンテンツの有効化」というボタンはクリックしない。
- ・ 身に覚えのないメールや添付ファイルを開いてしまった場合は、すぐにシステム管理部門等に連絡する。

引用元
Emotet(エモテット)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>

