テロ対策ネットワーク藤枝
～テロを許さない社会づくり～

令和4年　第5号

〔発行〕
藤枝警察署　警備課
TEL
代表　054-641-0110
（内線　内線461・462）

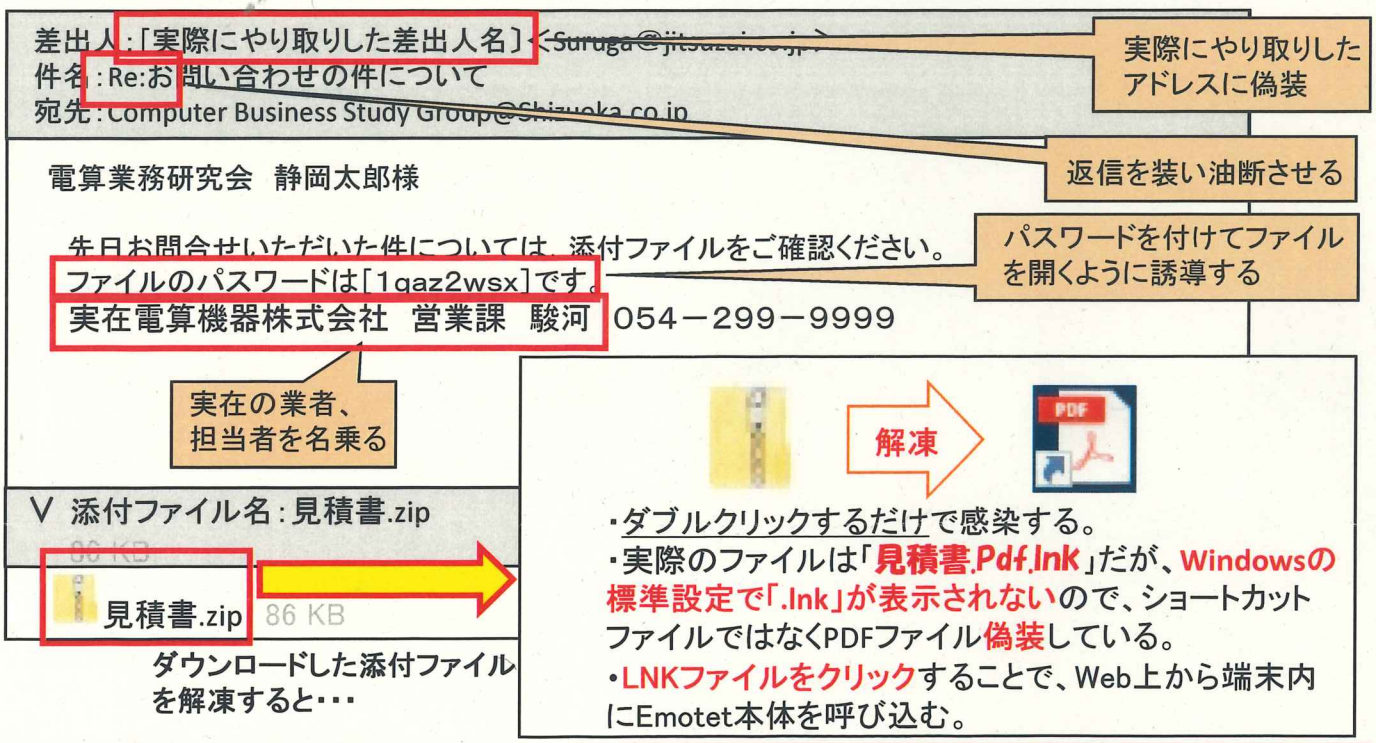
マルウェア「Emotet」の新しい手口

Emotet（エモテット）は、情報の窃取に加え、更に他のウィルスへの感染のために悪用させる不正プログラムです。特に注意を要するのは**「正規のメールへの返信を装う手口」**です。

正規に送信したメールの内容が丸ごと引用され、返信されてきたかのように見える内容で、これまでは、不正プログラムをダウンロードさせるため、ファイル又はリンクを添付する手口が使われていたことから、「添付ファイルのマクロの自動実行の無効化」、「不審なリンクをクリックしない」といった対策が可能でした。

しかし、４月以降、**ショートカットファイル（拡張子「.lnk」）やZIPで圧縮されたショートカットファイルを添付する手口**が見られるようになり、この場合、添付されたショートカットファイルを**ダブルクリックするだけで不正プログラムに感染**します。

ショートカットファイルは、アイコンが文書ファイルのように偽装されていることや、Windowsの標準設定では拡張子が表示されないといった特徴から、見分けにくい点に注意してください。



～　新たなEmotetの手口に対する対策　～

○ 不審メールを受信した場合は、システム管理部門へ連絡する等、情報を共有して組織的に対応する。

○ メールでショートカットファイルを授受するような業務要件がない場合は、Emotetに限らず、同等の攻撃への対策となるため、メールサーバ等で
- ショートカットファイル（拡張子.lnk）が添付されたメールをブロックする。
- ZIPファイルに格納されたファイルの拡張子をチェック可能であれば、ショートカットファイル（拡張子.lnk）が含まれているZIPファイルが添付されたメールをブロックする。

等の対策を検討する。