

サイバーだより



令和4年11月22日第12号

長野県警察本部
サイバー犯罪捜査課
026-233-0110

Emotet (エモテット) 感染警報

個人・機密情報の流出?!

Emotet(エモテット)は、主にメールを感染経路としたマルウェア(不正プログラム)です。

ランサムウェアに感染?!

Emotet(エモテット)は、取引先業者などに以前送信したメールの返信や転送を装い、添付されたエクセルファイルなどを実行させてマルウェアに感染させるものです。メール内のURLや添付のショートカットファイルからの感染も確認されています。

【感染すると・・・】

- ① 電子メールが漏えいするほか、メールソフトの連絡先に、Emotet(エモテット)付きのメールが送信され、**マルウェアが拡散**される。
- ② 自らランサムウェア等の**他のマルウェアを呼び込み、感染**する。
- ③ Webブラウザに保存された**クレジットカード等の情報が流出**する。



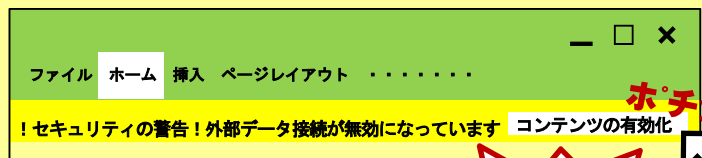
Emotet(エモテット)付きメールの一例です!

・返信 (Re:) や転送 (Fw:) を偽装

件名	Re: ●●の御依頼
添付ファイル	XXXXXXXX.xls

件名	Fw: 御確認ください
添付ファイル	P2022C.zip

・添付ファイルのエクセルファイルを実行すると「コンテンツの有効化」が表示される



ホチッ!

- ◎ 添付ファイルがあるメールには注意! 送信元に直接電話して確認しましょう!
- ◎ EmoCheckで感染しているか確認できます!
入手先: <https://github.com/JPCERTCC/EmoCheck/releases/>
- ◎ 被害が確認されたら、システム管理の委託業者に連絡するとともに、警察にも通報してください。



感染!

絶対に
押さないで!



サイバー犯罪対策アドバイザーのコラム

長野県警察サイバー犯罪対策アドバイザー
公立諏訪東京理科大学杉田誠准教授からの寄稿

静岡県沼津市、大阪市の医療機関がランサムウェアによるサイバー攻撃の被害を受けました。ランサムウェアとは感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する不正プログラムです。医療機関においてIT導入の遅れのためセキュリティ対策が不十分なケースが多くあり、可能ならば補助金等を利用して優先的なITの導入をよろしくお願いいたします。

～お知らせ～

長野県警察サイバーボランティアの学校法人松商学園松商学園高等学校ビジネス情報技術部の皆さんに、サイバーセキュリティに関する動画を作成していただきました。自社ホームページへのリンク掲載や、自社メディアでの放映を希望される場合は、サイバー犯罪捜査課まで御連絡ください。
URL: <https://www.pref.nagano.lg.jp/police/anshin/cyber/cyber-volunteer.html>

