CyberCrime Control Project

令和４年３月

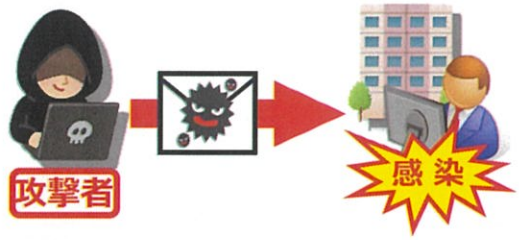
広島県警察本部
サイバー犯罪対策課
082-228-0110
（内線：705-586）

マルウェア「Emotet（エモテット）」の感染が再び拡大中！

先月、県内の企業でEmotetの感染事例が複数確認されました。

Emotetは、メールソフトからメールアドレス、メール本文やパスワードを盗み取り、その情報を悪用して他人へなりすましメールを送信したり、新たなウイルスに感染させたりするマルウェアです。

EUROPOL（欧州刑事警察機構）等の停止措置により活動を停止していましたが、2021年11月中旬ころから活動を再開しています。



（例）　メールに添付されたExcel・Word形式のファイルを開いて、「コンテンツの有効化」や「マクロを有効にする」を許可すると、不正なマクロが実行されて感染します。（開封しただけでは感染しません。）

Emotetが仕込まれたメールの特徴

- ○ Excel・Wordファイルが添付されている
- ○ メール本文にファイルをダウンロードするリンクが記載されている
- ○ 添付されたPDFファイル内にExcel・Wordファイルをダウンロードするリンクが記載されている
- ○ 過去にやりとりしたメールへの返信を装い、添付ファイルの開封を促す

Emotetに感染しないためには・・・

巧妙に偽装され見分けるのが困難なメールが増えているため、メールに添付された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、［コンテンツの有効化］はしないようにしてください。　有効化する場合はセキュリティ担当者に確認するか、送信者に直接電話、メールなどで問題ないことを確認してから有効化してください。

Emotet感染していませんか？

JPCERT/CCが公開している「EmoCheck」で確認できます。
https://github.com/JPCERTCC/Emocheck

① 「EmoCheck v2.0」をダウンロード
② 「EmoCheck」を実行
③ Emotetのプロセスが見つかりました

※　感染していた場合は、大至急セキュリティ担当者または警察に連絡して対応してください。

「減らそう犯罪」第５期
ひろしまアクション・プラン
令和3(2021)年～令和7(2025)年

運動目標　住む人 来る人 誰もが
日本一の安全安心を実感できる広島県の実現

重点項目
- 不安に感じる犯罪の抑止
- 特殊詐欺被害の抑止
- 子供・女性・高齢者等の安全確保
- インターネット利用犯罪被害の防止