サイバーセキュリティだより

発行：愛媛県警察本部生活安全部サイバー犯罪対策課

令和2年
2月25日
Vol.39

新型コロナウイルスに乗じたサイバー犯罪に注意

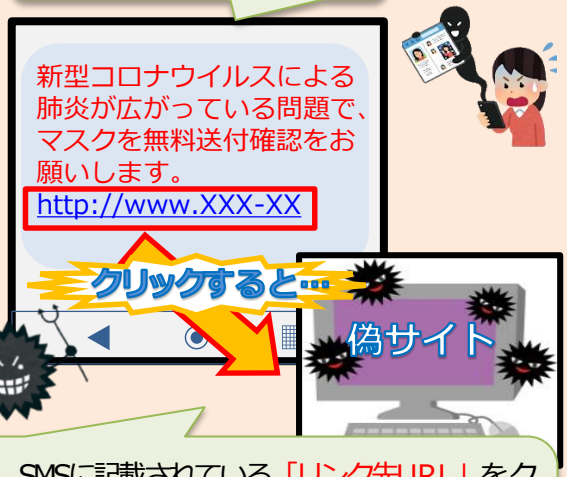
【現状】

世界的な感染予防対策が求められている「新型コロナウイルス（COVID19）」ですが、それに便乗したサイバー犯罪が発生しています。

手口については、ＳＭＳ（ショートメッセージサービス）を悪用した「スミッシング」や、不正メールにより「Emotet（エモテット）」と呼ばれるマルウエアへの感染を狙ったものなどが確認されています。

【手口1】

①偽SMSが送信される！



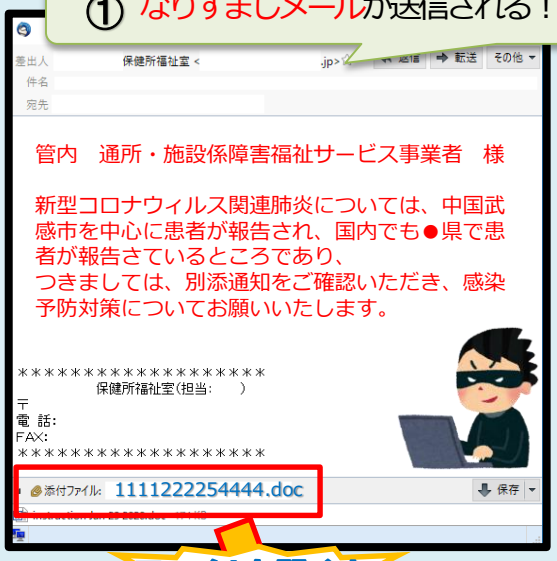
② SMSに記載されている「リンク先URL」をクリックすると偽サイトに接続され、個人情報等の入力を求められたり、不正アプリをインストールさせられたりする！

～対策～

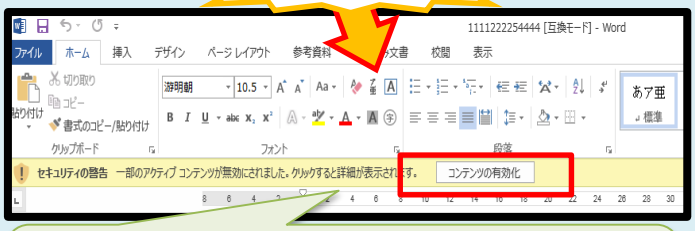
- ○ 記載されたURLには、絶対にアクセスしない。
- ○ サイトが表示されてもタップしない。
- ○ 提供元不明のアプリをインストールしない。
- ○ IDやパスワード等の個人情報は入力しない。

【手口2】

① なりすましメールが送信される！



ファイルを開くと…



② メールに添付されている「word形式のオフィスファイル」を開き、「コンテンツの有効化」をクリックするとウイルスに感染する！

～対策～

- ○ 身に覚えのないメールを開かないことに加え、自分が送信したメール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。
- ○ メールや添付ファイルを閲覧中、警告ウインドウが表示された際、警告の意味が分からない場合も操作を中断する。
- ○ 添付されたWord等のオフィスファイルを開いた際に、マクロ等の警告が表示された場合「コンテンツの有効化」のボタンはクリックしない。
- ○ Windows等、OSの定期的に配布されるセキュリティパッチを適用する。
- ○ 常にセキュリティ対策ソフトを最新状態に更新し、パソコンを保護する。

参照元：IPA(https://www.ipa.go.jp/security/announce/20191202.html#L12)
JC3(https://www.jc3.or.jp/topics/newmodel_coronavirus.html)

相談窓口

愛媛県警察本部サイバー犯罪対策課　TEL089-934-0110(代)