滋賀県警からのサイバーセキュリティに関するお知らせ

県内で標的型メール攻撃が発生しています。
実在する人物を装ったメールからのウイルス感染に注意

最近、県内で標的型メール攻撃によるウイルス感染事案が確認されています。

標的型メール攻撃は、近年、非常に巧妙化しており、見破ることが難しくなっています。

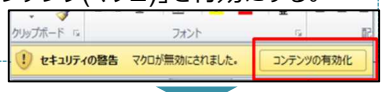
しかしながら、ウイルスに感染するとパソコンが使用できなくなったり、他の企業や組織に影響を及ぼしたりするなど事業活動が停滞してしまいます。

メールの添付ファイルを開くときは、ウイルス感染の可能性があることを念頭に慎重にお願いします。

県内で発生した事例

メール受信
取引業者の担当者から「請求書」（Word ファイル）が送付される。

Word ファイル「請求書」を開封
「コンテンツ(マクロ)」を有効にする。

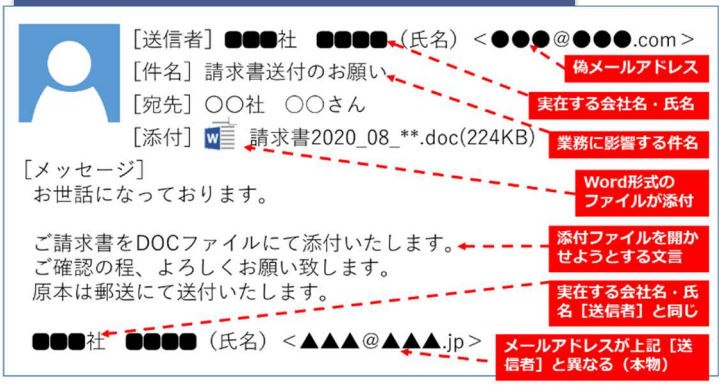


ウイルスがダウンロードされ、送受信メールが流出する

攻撃者が盗み取ったメールを利用して、ウイルス付きメールを第三者に送信

取引先から問合せが殺到
「変なメールが来た」「以前のメールが来た」「ファイルを開いたが白紙だ」等

実際に送られたメール（一部編集しています。）



「Emotet（エモテット）」に注意

Emotet は、情報の窃取に加え、更に、他のウイルス感染のために悪用されるウイルスです。

Emotet は、主にメールに添付された「Word ファイル」を開いたうえ、「コンテンツの有効化」又は「編集を有効にする」ボタンを押すことで、マクロプログラムが実行され、外部サーバからプログラム（Emotet）がダウンロードされます。

Emotet に感染すると、PC に保存されている送受信メールの情報が盗まれるため、実在する人物の氏名やメールアドレスを使用することが可能となり、正規のメールへの返信を装って、別の人（取引先等）へ、標的型メールが送られます。

特に、最近では、パスワード付きの ZIP ファイルを添付する新しい手口が確認されています。

パスワードはメール本文に記されており、ZIP ファイルを開くと Word ファイルが入っているというものです。添付ファイルが暗号化されているため、メール配送経路上でセキュリティ製品の検知・検疫をすり抜ける可能性が高いので注意が必要です。

標的型メール攻撃の対策

・身に覚えのないメールの添付ファイルは開かない。
・メール本文中の URL リンクをクリックしない。
・自分が送ったメールの返信でも不自然な点があれば添付ファイルは開かない。
・「Word」や「Excel」ファイルを開いたときに、マクロやセキュリティに関する警告が表示された場合、「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に連絡する。

参照：IPA「Emotet 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

［お知らせ］ 不正送金事案が発生しています。フィッシングによる ID・パスワードの流出に注意してください。

滋賀県警察本部サイバー犯罪対策課 （代表）077-522-1231