# サイバー瓦版

岡山県警察本部
サイバー犯罪対策課発行
086(234)0110
pcyber@pref.okayama.lg.jp

# 2022、ネット界で「大泥棒」が暗躍！

## この特徴にピン！ときたら、ウイルスチェ～ック!!

### WANTED・手配書

| | Emotet（エモテット） | ランサムウェア |
|---|---|---|
| 侵入方法 | 知り合いの名前を使ったメール | ①VPN機器の脆弱性<br>②脆弱なアカウントから入手したリモートデスクトップの認証情報 |
| 盗むもの | ①メールアカウントの認証情報<br>②メール本文<br>③メールソフトのアドレス帳 | ①認証情報<br>②機密情報 |
| その他の悪行 | ①ランサムウェアなど他の不正プログラムを呼び込む<br>②侵入した端末を感染拡大メールの踏み台にする<br>③増殖して同じネットワーク内に感染を広げる | ①端末やネットワーク内に保存された情報を暗号化<br>②復号化と引き換えに高額な身代金を暗号資産で要求<br>③盗んだ情報をリークサイトに掲載 |
| | 情報泥棒、運び屋 | 情報泥棒、脅迫<br>身代金目的誘拐 |


いまだ世界中で新型コロナウイルスへの感染が収まらず、みなさん、感染防止に気の抜けない毎日を過ごされていると思います。そんな中、インターネットの世界でもコンピュータウイルスへの感染が拡大していることをご存じでしょうか。なかでも「エモテット」と「ランサムウェア」による被害が急拡大しています。両方とも、上の手配書のとおり、大切な情報を盗む「大泥棒」なのです。

### ■「エモテット」はメールでやってくる…

「エモテット」はあなたが過去にメールの送受信をした相手の名前を使い、添付ファイル付きメールを送り付けてきます。知り合いからのメールと信じて添付ファイルを開き不正指令が実行されると、エモテットに感染してしまいます。感染に気づかず何の対策もとらなかった場合、ネットワークを通じてどんどん感染が広がっていきます。

### ■身代金を要求！「ランサムウェア」

「ランサムウェア」はもっと凶悪です。ネットワークのセキュリティーが弱い部分を探し出すなどして侵入してきます。データを暗号化し、暗号解除と引き換えに高額な身代金を要求してきたり、盗んだ情報を暴露サイトに掲載すると脅し、二重の支払いを要求することもあります。さらに、データの暗号化により会社の業務が停止することで営業利益等に悪影響を及ぼすなど被害甚大です。

この両者を比較すると、一見、エモテットの被害が小さいように見えますが、実は、エモテットはランサムウェアを呼び込むことで知られています。

**ポイント　感染しないために気を付けること**

① 知り合いから添付ファイル付きメールが届いたら必ず送信元メールアドレスを確認。
いつもと同じメールアドレスですか？
② メール本文内のＵＲＬにはアクセスしない
③ ＯＳやソフトは常に最新にアップデートしておく

**重要！　感染したかも？その時は**

① ネットワークから端末を遮断
② ウイルススキャンなどで感染確認
③ 社員、その他関係者へすぐに連絡
④ 警察、セキュリティ会社への相談

### ■やっぱり大切、感染防止対策

新型コロナ感染防止対策と同様、私たちが今すぐできる対策を確実に行うことが、自分の身を守るだけではなく、社会全体の被害を減らすことにもつながります。

もし、感染してしまったら、決して放置せず、警察やセキュリティ会社に相談してください。

### 課長のつぶやき

知人の名前を使ってメールするエモテットや暗号解除と引き換えに身代金を要求するランサムウェア等、サイバー空間における犯罪は巧妙化しています。

私たちが生活する実空間でも、犯罪者は悪知恵を働かせており、特殊詐欺等でもみられるように手口は進化しています。

しかし、サイバー空間での犯罪は、実空間と異なり、国境を越え、24時間、非接触・非対面で行われるため、被害に遭うリスクは一層高く、インターネットを利用する全ての人が被害に遭う可能性があります。

被害を防止するため、最小限にするため、実空間と同様、一人一人が対策を行うとともに、被害発生時は警察等に相談して社会全体で対応しましょう。