

世界中で猛威を振るっているランサムウェアに注意

1 ランサムウェアの猛威

今年5月14日には、アップデートのされていないWindowsのパソコンを狙って、ランサムウェアによる被害が世界150ヶ国、約20万件発生した等と報道され、大分県内でも、被害が確認されています。一度感染すると、復旧はできませんので、注意して下さい。



ランサムウェア画面①



ランサムウェア画面②

2 ランサムウェアとは

ランサムウェアとは、「Ransom(身代金)」と「Software(ソフトウェア)」を組み合わせた造語です。パソコンの内部に保存されている特定のファイル(文書ファイル、表計算ファイル、画像や写真データ等)に勝手に暗号化処理を行い、読み取れない状態にしてしまう不正プログラムです。パスワード等が分からないため、復号(暗号化を解除)することができません。そこで、犯人はファイルの復号と引き換えに金銭を要求するのです。



3 標的型メールとは

業務に関連した正当なものであるかのように装いつつ、不正プログラムを添付した電子メールを送信し、これを受信したコンピュータを不正プログラムに感染させることによって情報を盗み取るものです。



4 標的型メールを見破るための「6」のポイント

- ① **メール本文のURLや添付ファイルを開かざるを得ない内容**
 - ・新聞社や出版社からの取材申込や講演依頼
 - ・就職活動に関する問合せや履歴書送付
 - ・製品やサービスに関する問合せ、クレーム、アンケート調査
 - ・議事録、講演原稿などの内部文書 ・著名人に関する情報
- ② **これまで届いたことのない官公庁や有名企業からの連絡**
 - ・熊本地震・大雨など災害情報
- ③ **IDやパスワード、口座番号などの入力を要求するメール**
 - ・メールボックス、サーバーなどの容量オーバーの警告文
 - ・金融機関からの登録情報の確認や口座凍結防止の案内
- ④ **送信メールアドレスがおかしい**
 - ・官公庁や大手企業からのメールなのにフリーメルを使用している
 - ・差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なっている
- ⑤ **メール本文の日本語表記がおかしい**
 - ・日本で使われていない漢字が表記されている
 - ・使われない言い回し(翻訳ソフト使用)
- ⑥ **実行形式ファイル(exe、scr、cplなど)や圧縮ファイル(ZIP)が添付**
 - ・拡張子とアイコンの組み合わせが異なっている



5 ランサムウェアへの対策

- ① パソコンのOS、ソフトウェアを**最新の状態**にする
OS及びソフトウェアのバージョンを常に最新の状態に保ち、脆弱性をなくすことでドライブ・バイ・ダウンロードによる感染リスクを低減します。
- ② **ウイルス対策ソフト**を導入し、パターンファイルを常に最新の状態にする
インターネットにアクセスするパソコンには、必ずウイルス対策ソフトを導入し、パターンファイル
- ③ 重要なファイルは定期的に**バックアップ**する
基本的には、ランサムウェアによって暗号化されたファイルは復元できません。そのため、重要なファイルについては、定期的にバックアップする必要があります。
バックアップは、ランサムウェアへの対策としてだけでなく、パソコンが突然故障してしまった場合の備えにもなります。
- ④ 心当たりのないメールを**安易に開かない**こと
心当たりのないメールに添付されたファイル(特にexeファイル、ZIPファイル)を安易に開いたり、本文に記載のURLに不用意にアクセスをしないで下さい。
メールの送信者に対して、電話などで送信の有無を確認して下さい。



あなたの会社や団体で研修の一環として、サイバーセキュリティカレッジを開催しませんか？
小学生から大人まで幅広く対応できます。下記の連絡先にご相談下さい。

大分県警察本部生活安全部生活環境課サイバー犯罪対策室
サイバーセキュリティ係

Tel:097-534-2048