F－CSNET NEWS

Fukuoka small and medium sized enterprises
Cyber security Support NETwork

第１０号
平成２９年１１月
【作成】福岡県警察本部
サイバー犯罪対策課

最近のネット犯罪～主な手口

偽サイト

実在する企業名のサイトに似せたサイトで利用者を騙すもの。「利用者のカード情報や個人情報を盗まれる」「注文したものと異なる模倣品が届く」「商品が届かず返金もない」等の被害が発生

何に気を付けたらいいの？

福岡県警察
サイバーマスコット
「サイビー」

警察への相談も増えています！

注　意　点

□ 不審なサイト（電話番号が掲載されていない／価格が極端に安い／日本語が不自然、等）に注意

ランサムウェア

ウイルスに感染させパソコン内のデータを暗号化して使えないようにし、データの復旧と引き換えに「身代金（ランサム）」を要求する。
メールの添付ファイルを開いて感染するほか、広告バナー等をクリックして感染するおそれもある。

★参考★
本年10月24日にも、ロシア、ウクライナ、ブルガリア、日本等で大規模なランサムウエアの攻撃が確認されました。

何に気を付けたらいいの？

注　意　点

□ OS（Windows等）やソフトウェアの更新を徹底する。

□ ウイルス対策ソフトを導入し、最新版に更新する。

□ 定期的にデータをバックアップする。

社員教員も重要です！

□ 不審な（身に覚えのない）メールの添付ファイルの開封やリンクへのアクセスをしない。

サイバーセキュリティの基本講座②　（バックアップについて）

「ランサムウェア」に感染すると、会社の取引データや顧客情報等が暗号化され、事業に支障が生じてしまいます。
不測の事態に備え、大事なデータについては、定期的なバックアップが有効です。
また「ランサムウェア」は、パソコンに保存されているデータだけでなく、接続している外付けハードディスク等や、USBメモリのデータも感染させてしまうことがあるので、注意が必要です。

サイバー妖怪
「イカサマ」

※　大事なデータを扱うパソコンは、インターネットからの分離も検討しましょう！！