滋賀県警察からのお知らせ

# サイバーセキュリティ情報 CSI

事業者の皆さまに、注目のサイバーセキュリティに関する情報をお届けします。

R３年度No. 5

## 新型コロナウイルス関連フィッシングに注意

新型コロナウイルス感染に関して、厚生労働省を装ったり、給付金に関するフィッシングメールが確認されています。

滋賀県では、緊急事態宣言が発令（令和3年8月27日から同年9月12日まで）されています。
事業者向けの給付金や補助金に関するフィッシングメールが出回る可能性もあります。
新型コロナウイルス感染に関するフィッシングメールや標的型メール攻撃に注意してください。
各情報は、行政機関の公式サイトを必ず確認するようにしてください。

### フィッシングサイトの特徴

フィッシングサイトは、正規のサイトをコピーして作成されていることが多く、見分けることが非常に困難です。

フィッシングサイトは、ID/パスワード、個人情報（氏名、住所、生年月日、職業、クレジットカード情報、インターネットバンキング関連情報）の入力のほか、身分証明書（運転免許証、保険証、マイナンバーカード、パスポート等）の画像の送信を要求される場合があります。

【フィッシングサイトに情報入力した場合の主な影響】

- ID/パスワードが不正に使用され情報を書き換えられる。
- ショッピングサイトで不正に商品を購入され、商品代金を請求される。
- 自分名義のアカウントを作成され、なりすまされる。
- 個人情報が売買される。

### フィッシングメール対策

- **ウイルス対策ソフトを必ず導入してください。**
  **スパムメールとして検知してくれます。**
  **（全て検知できるというわけではありません）**
- **メールアドレスを確認してください。**
  **行政機関や団体からのメールの場合、正規のアドレスと似せている場合があります。**
- **リンク先のサイトのURLを必ず確認してください。**
  **リンク先にアクセスしただけは、情報は洩れません。アクセス先のURLを確認するようにしてください。**
- **万が一、フィッシングサイトに情報を入力してしまった場合は、管理者に連絡した上、パスワードを変更してください。**


↑実際に送付されたフィッシングメール。バナー（画像）をクリックすると、フィッシングサイトが表示され、個人情報の入力を求められます。

参照：フィッシング対策協議会（特別定額給付金に関する通知を装うフィッシング）
https://www.antiphishing.jp/news/alert/kyufukin_20210824.html

### ランサムウェア情報

海外では、新たなランサムウェア「LockBit2.0」による脅威が拡大している模様です。
データの暗号化と脅迫の手口により、企業や組織に多額の身代金の支払いを要求する手口です。
日本でも被害が発生するおそれがありますので、ランサムウェアにも注意しましょう。

**«注意»巧妙化する標的型メール攻撃にご注意願います。**

滋賀県警察本部　サイバー犯罪対策課　077-522-1231（代表）