

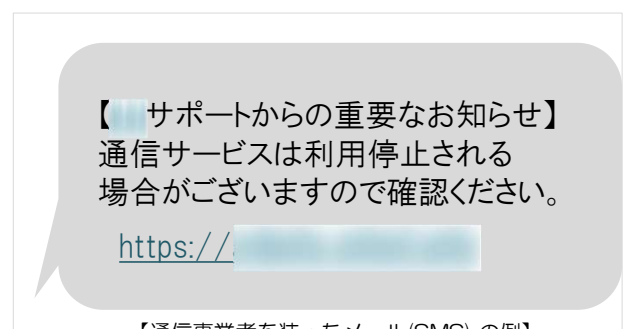
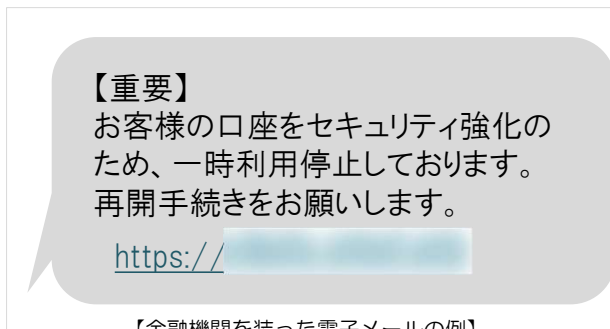
## フィッシング被害に遭わないために

### ◇ フィッシングとは ◇

実在する事業者を装ったSMSやEメールを通じ、偽サイトに誘導し、ID・パスワード等のアカウント情報やクレジットカード情報等を入力させて盗む手口

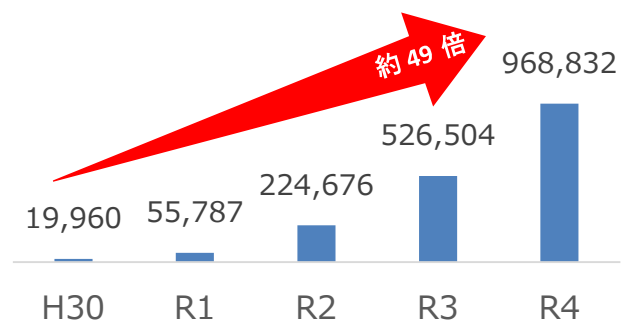
### ◇ フィッシングメールの特徴 ◇

- 「利用停止」、「サービスの利用停止」等、不安を煽る、緊急を装う
- URL等のリンクからフィッシングサイトへ誘導



### ◇ フィッシングの情勢 ◇

フィッシング対策協議会によると、令和4年中のフィッシング報告件数は96万8,832件で、4年前の約49倍に激増しています。



### ◇ フィッシング被害に遭わないために ◇

リンクは便利な機能ですが、巧妙化するフィッシングメールを見破るのは困難です。メールの内容を確認する際には、

## メールのリンクは押しちゃダメ!!

を合い言葉に、

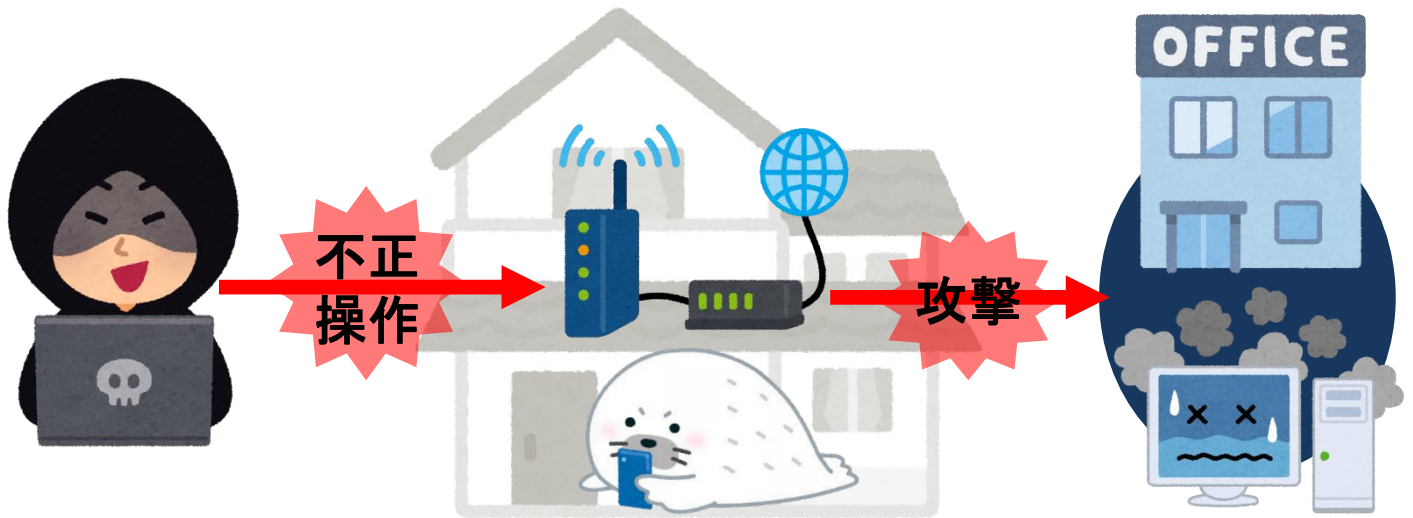
- ブックマークに登録した公式サイトからアクセスする
- 正規のアプリから確認する

ことを習慣づけましょう！



# 自宅のWi-Fiルーターが狙われる!?

犯人があなたの自宅のWi-Fiルーターを不正操作して、サイバー攻撃の踏み台にしているかもしれません！



春の新生活が始まったこの機会に、是非ルーターの設定を見直してみましよう。

今すぐ

## 攻撃の踏み台にされないための4対策！

- ① 初期設定の単純なIDやパスワードを変更
- ② 常に最新のファームウェア（ハードウェアを動かすためのソフトウェア）を使用
- ③ サポートが終了したルーターは買換え
- ④ **見覚えのない設定変更がされていないか確認！**

ルーターの設定については、取扱説明書やメーカーホームページを確認してください



～ご家庭でWi-Fiルーターをより安全にお使い頂くために～  
一般社団法人デジタルライフ推進協会のサイトもご覧ください

