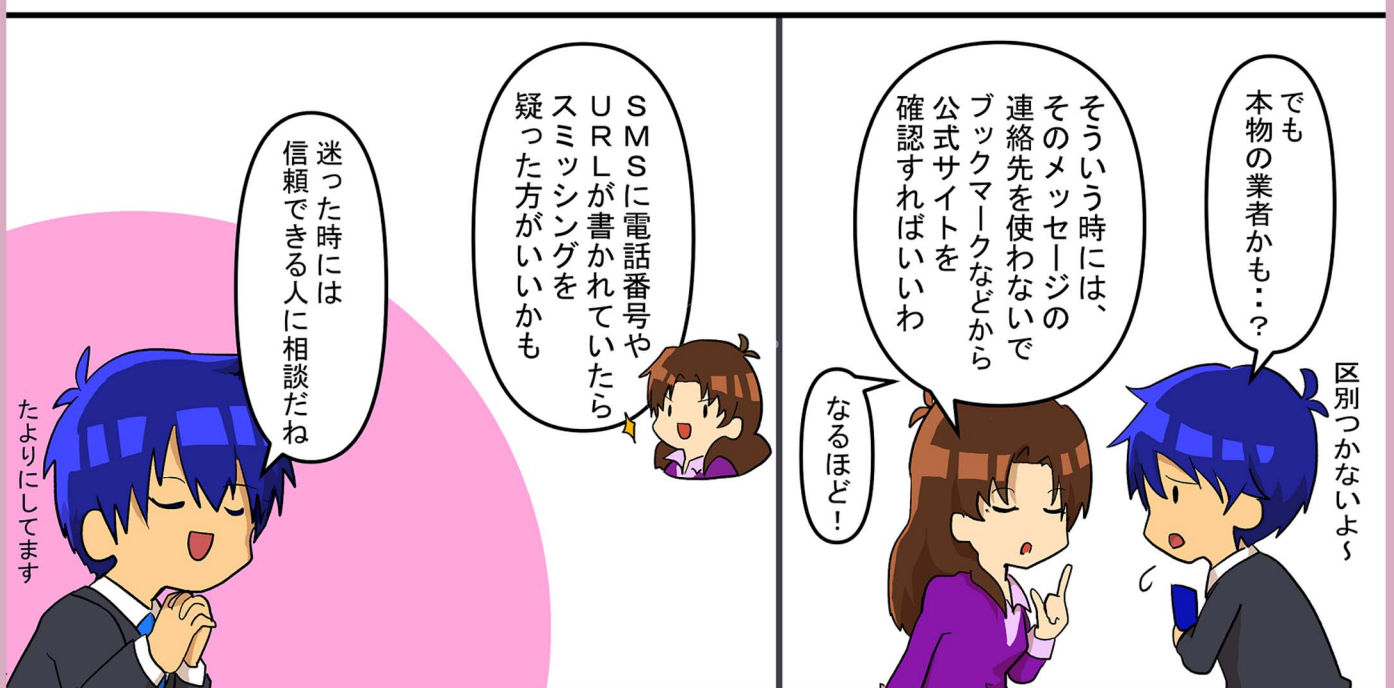
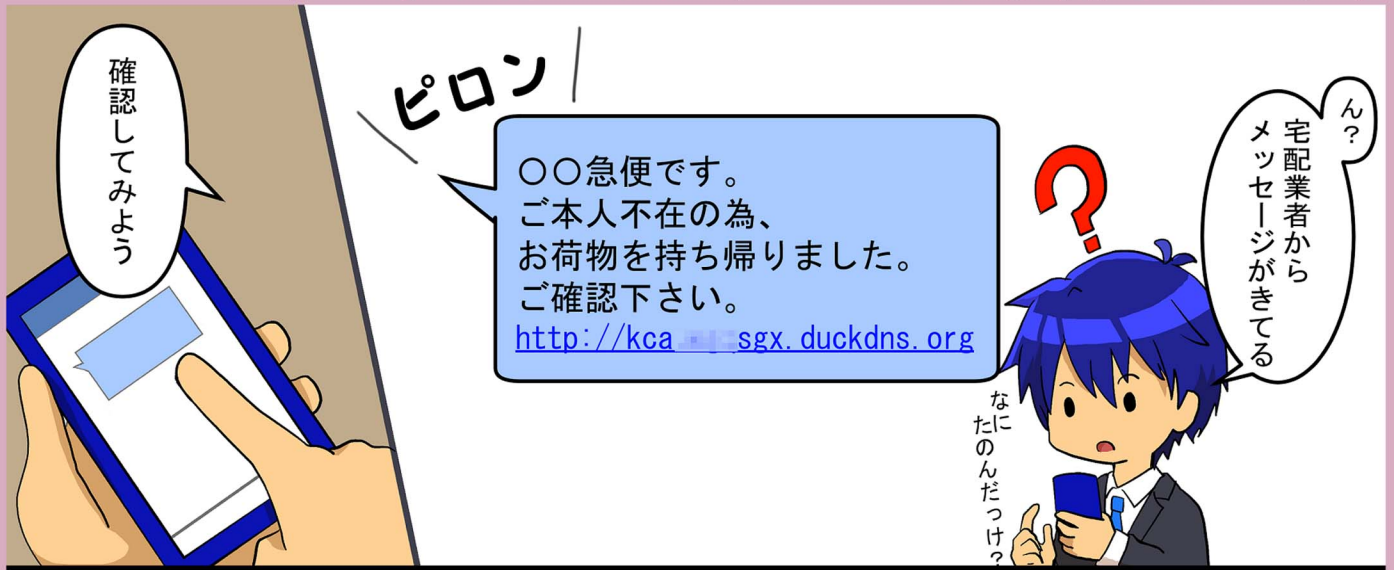


# 「それ、スミッシングじゃない?」

不正なショートメッセージが多発しています

※SMSショートメッセージサービス…携帯端末の電話番号を宛て先にしてメールを送れるサービス



宅配業者等をかたる不正なショートメッセージにご注意ください

宅配業者や通販サイト、クレジットカード会社等を装った不正なSMS（ショートメッセージ）についての相談が継続して寄せられています。

以下のような特徴を持つショートメッセージを受信した場合に、送信元やメッセージ内の電話番号に電話をかけたり、メッセージ内に書かれているURLを開いたりすると、詐欺被害に遭ったり、スマートフォンにマルウェア（不正なアプリ）を仕掛けられるおそれがあります。

#### 特 徴

1. 知らない携帯電話番号から送信されている。
2. 巧みな口実で対応を急がせようとする。

例 荷物を配達しましたが不在でした。

通信料金の未納があります。

通販サイトの決済手段が無効になりました。

新型コロナウイルスのワクチン接種の予約を受け付けます。

3. URLが公式サイト等とは異なる。

例 <http://〇〇〇〇〇〇〇〇〇.duckdns.org>

<http://×××××××.ddns.net> 等

このようなSMSは無視するようにしてください。

通販サイトから荷物が届く予定がある等、心当たりがある時には、正規のメッセージと間違えないよう、より一層の注意をお願いします。

不正なURLを開いて、決済機能のあるアカウントの情報やクレジットカード情報等を入力してしまった場合には、速やかにアカウントのパスワードを変更して不正アクセスを防止すると共に、クレジットカード会社等に連絡し、クレジットカードの決済を停止する必要があります。

無視して良いか分からない時は、メッセージに書かれている連絡先ではなく、公式サイトを確認したり、信頼できる機関の相談窓口にご相談してください。

サイバー犯罪に関する相談、情報提供は

フィッシング110番 088-622-3180

（24時間受付。ただし平日の午後5時15分から翌午前8時30分までの間と年末年始及び休日は、警察本部当直員が対応）