



# サイバーセキュリティの置き薬

2020年  
第16号

そのショートメッセージ(SMS)は本物？

## SMSのURLはすぐに押さないで！

電話番号でメッセージの送受信ができるショートメッセージサービス(SMS)。通信会社、ショッピングサイトのほか様々な企業が、顧客へのお知らせなどに利用しています。それを悪用したフィッシングメールに注意が必要です！

不安になるようなメッセージにしよう！

お客様のアカウントに異常ログインの可能性が  
あります。  
下記URLから確認をお願いします。

<https://www.abcxxx.xx/login>

タップ

ログインページ

ID  
パスワード  
ログイン

偽のサイト

ID・パスワードなど、  
入力した重要な情報が  
抜き取られる

盗まれたID・パスワードで  
不正ログインされる

気になるような文章にしよう！

【重要なお知らせ】  
お支払い方法が変更になりました。  
下記URLから手続きをお願いします。

<https://www.abcxxx.xx/login>

タップ

お客様情報

クレジットカード番号  
セキュリティコード  
有効期限

偽のサイト

クレジットカード情報など、  
入力した重要な情報が  
抜き取られる

クレジットカードが  
不正利用される

多くの人に関係があるような内容にしよう！  
ひっかかってくれるはず。

お客様宛にお荷物のお届けにあが  
りましたが、不在の為持ち帰ら  
ました。下記よりご確認ください。

<https://abcxxx.xx>

タップ



ウイルスに感染！

連絡先など重要な情報が  
抜き取られたり、  
データのやり取りを盗み  
見られたりする

普段使っているサービスや、  
大手企業の名称でメールが  
来ても、用心！  
フィッシングメールかも  
しれません…。



## 対策

- ★ メッセージ内のリンクは安易に押さない  
(リンク先で、ID・パスワードの入力や、アプリの  
ダウンロードを促すものは要注意！)
- ★ URLのリンクからではなく、公式ホーム  
ページから確認する。