

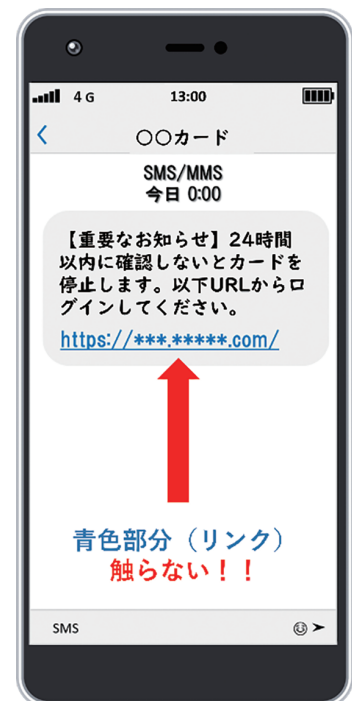
第11 サイバー犯罪対策

1 インターネットバンキングに関する情報等を盗む「フィッシングメール」に注意！

フィッシングとは、実在するサービスや企業をかたり、偽のメールやSMS（ショートメッセージ）で偽サイトに誘導し、インターネットバンキングに関する情報、クレジットカード情報、会員情報（ID・パスワード）等を盗む手口です。金融機関、クレジットカード会社、ショッピングサイト、宅配会社等をかたるフィッシングメールが確認されています。緊急を装ったメールや、現に利用中のサービスに関するメールの場合、騙されてしまう可能性が高まります。特に、インターネットバンキングに関する情報がフィッシングによって盗まれてしまうと、口座の預金が不正に送金されてしまう可能性があるので注意しましょう。

<フィッシング（偽）メールの例>

- ① 金融機関やカード会社を装ったもの
不正な取引があったため、一時利用停止しています。すぐに確認してください。
- ② ショッピングサイトを装ったもの
支払い方法が確認できないため、会員情報を速やかに確認してください。
- ③ 携帯電話会社を装ったもの
【利用停止予告】未払い料金お支払いのお願い。
- ④ 宅配会社を装ったもの
お客様が不在のため、荷物を持ち帰りました。こちらから確認してください。



<フィッシングの被害防止対策>

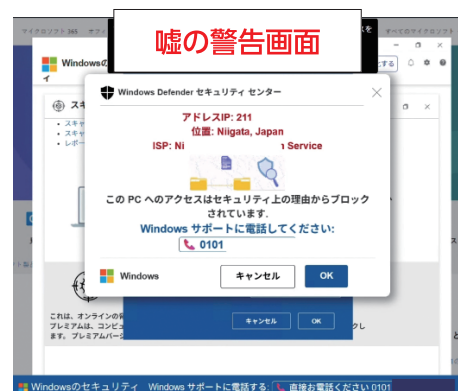
- ① メールやSMSのリンクを開かない。
- ② リンクを開いてしまってもパスワード、クレジットカード情報等を入力しない。
- ③ パスワードの使いまわしはしない（サービスごとに違うものを設定する）。
- ④ サイトへのログインは、公式アプリや公式サイトからアクセスする。
- ⑤ 迷惑SMSブロック機能やセキュリティ対策ソフトを利用する。
- ⑥ おかしいと感じたら警察や家族等身近な人に必ず相談する。

2 サポート詐欺に注意！

サポート詐欺とは、インターネット利用中に、突然、ウイルス感染したかのような嘘の画面を表示させたり、警告音を発生させたりするなどして、ユーザーの不安を煽り、画面に表示されたサポート窓口で電話をかけさせ、ウイルス削除等のサポートの名目で金銭を騙し取ったり、遠隔操作ソフトをインストールさせたりする手口です。

<サポート詐欺の被害防止対策>

- ① 不審な警告画面に表示された電話番号には電話しない。
- ② 不審な警告画面は無視して閉じる。
(キーボード左上の「Esc」キーを長押しして、ブラウザの「×」をクリックして画面を閉じる)
- ③ ウイルス対策ソフトを導入する。



3 IDやパスワードなどの適切な管理とセキュリティ対策を！

パソコンやスマートフォンがコンピュータウイルスに感染したり、フィッシング等によってIDやパスワード、クレジットカード情報が流出したりすることにより、「クレジットカードで身に覚えがない請求がきた。」など、インターネットに関わる様々な被害が発生しています。

こうした被害を防止するために、皆さん一人一人がサイバーセキュリティについて考えるとともに、安全にインターネットを利用できる環境作りをしましょう。

<基本的なセキュリティ対策>



- ① **セキュリティ対策ソフト・対策機器を導入し、常に最新の状態にアップデートする。**
 - ・ ウイルスの検知や、悪質サイトの警告表示等が行われるようになります。
- ② **OSやアプリケーションだけでなく、ネットワーク関連機器も最新の状態にする。**
 - ・ サイバー攻撃に対する「ぜい弱性」は、パソコンやスマートフォンのOSや各種アプリはもちろん、Wi-Fiルーター等のネットワーク関連機器にも存在します。
アプリ等と同様に、ネットワーク関連機器等のソフトウェアについてもアップデートを行う必要があります。
- ③ **ID、パスワードを適切に管理する。**
 - ・ サービス毎に複雑なパスワード（大文字・小文字、数字や記号を合わせて10桁以上）を設定し、2段階認証、多要素認証を利用する。
 - ・ ネットワーク関連機器等は購入時の初期パスワードから必ず変更する。
(パスワードの適切な設定方法は、各種セキュリティ関係ウェブサイトを参考にしてください。)
 - ・ ID・パスワードは不用意に入力せず、入力先が正規のサイト等であるかよく確認する。