

スマートフォンにもウイルス対策を

埼玉県教育委員会

スマートフォンをねらったウイルスは日々増加しており、その手口もだんだん巧妙になっています。そのため、パソコンと同様、スマートフォンにもしっかりとウイルス対策を行う必要があります。

スマートフォンがウイルス感染する原因は何か？

スマートフォンがウイルス感染する主な原因としては、以下の4つがあげられます。

1.不正アプリのダウンロード

名前やアイコンを似せて、人気のゲームアプリなどを装った不正アプリや、「ウイルスに感染しました」などの偽の警告画面を表示させ、ウイルス対策アプリを装ってダウンロードさせようとする不正アプリなどが確認されています。

2.「フリーWi-Fi」の利用

外出先で誰でも「Wi-Fi」が利用できる「フリーWi-Fi」の中には、アクセスしたスマートフォンをウイルス感染させるものも存在します。

3.Webサイトの閲覧

Webサイトの中には、犯罪への利用などを目的として作られたものもあり、こうしたサイトを閲覧すると、ウイルスに感染する可能性があります。

4.メールに添付されたファイルの開封

著名な企業をかたって送られてきたメールの添付ファイルを開くと、ウイルス感染してしまったという被害が発生しています。

スマートフォンがウイルスに感染すると、こんな被害を受けることが……

- ・電話帳のデータを抜き取られ、不正に利用される
- ・位置情報を盗み取られ、住所を特定される
- ・通話を盗聴されたり、メールのやりとりを盗み見られたりする
- ・勝手に不審な電話番号に電話をかけられ、高額な通話料を請求される
- ・他の誰かに、不正アプリのダウンロードを促すメッセージを送られる



スマートフォンがウイルスに感染するリスクを減らすために

スマートフォンのウイルス感染のリスクを減らすためには、**セキュリティソフトの利用**が有効です。セキュリティソフトには、不正アプリのダウンロードを防いだり、危険なWebサイトへのアクセスを制限したり、受信したメールと、メールに添付されたファイルにウイルスがひそんでいないかチェックしたりする機能があります。

自分のスマートフォンにセキュリティソフトが入っているかは、アプリ一覧のページか、契約内容一覧のページで確認してください。もし入っていなかった場合は、携帯電話会社が提供しているサービスに加入するか、公式アプリストアでダウンロードしてください。

セキュリティソフトを利用したうえで、自身でも以下のような点に気をつけましょう。

- ・アプリのダウンロードは公式ストアからだけにする
- ・あやしいURLや広告はクリックしない（例：運送業者を装って送られてきたメッセージ内に掲載されたURLや、応募した覚えのない商品が当選したという広告）
- ・OSやアプリのバージョンは最新版にアップデートする
- ・提供元が不明な「フリーWi-Fi」（例：誰かの名前のWi-Fiや、意味不明な文字列のWi-Fi、飲食店と似た名前を使ったWi-Fi など）は使わない、「Wi-Fi」に自動接続にしておかない
- ・知らないアドレスからきたメール及び、添付されたファイルは開かない

セキュリティソフトを利用したうえで、自身でもウイルス対策を意識してスマートフォンを利用しましょう

※本資料は、埼玉県教育委員会の委託により、PITCREW株式会社が作成したものです。