

■「スマートフォン情報セキュリティ3か条」を守りましょう

スマートフォンにおいて、利用者が最低限取るべき情報セキュリティ対策として、国は「スマートフォン情報セキュリティ3か条」を取りまとめています。この3か条を実践して、スマートフォンを安全に使いましょう。

■スマートフォン情報セキュリティ3か条

1. OS（基本ソフト）を更新

スマートフォンはOS（AndroidやiOSなど基本ソフト）の更新（アップデート）が必要です。古いOSを使っていると、ウイルス感染の危険性が高くなります。OSの更新を促す通知が来た際には、すみやかに最新版のOSをインストールしましょう。

詳しくは携帯電話会社などに相談してください。

2. ウイルス対策ソフトの利用を確認

先の事例で紹介したとおり、ウイルスの混入したアプリが発見されています。スマートフォンでは、携帯電話会社などによってモデルに応じたウイルス対策ソフトが提供されています。

ウイルス対策ソフトの利用については、携帯電話会社などに確認しましょう。

3. アプリの入手に注意

アプリの事前審査を十分に行っていないアプリ提供サイトではウイルスの混入したアプリが発見される例があります。OS提供事業者や携帯電話会社などが安全性の審査を行っているアプリ提供サイトを利用するようにしましょう。

インストールの際にはアプリの機能や利用条件に注意しましょう。

■注意すべき「スマートフォンプライバシーガイド」

スマートフォンは、常に電源を入れてネットワークに接続された状態で持ち歩きます。そのためパソコンに比べて利用者との結びつきが強く、電話帳、位置情報、通信履歴、行動履歴など、利用者のプライバシーに関わる多種多様な情報が取得・蓄積されています。

国では、利用者自身が注意すべき事項を整理して「スマートフォンプライバシーガイド」としてまとめています。主な内容は次のとおりです。

■スマートフォンを利用する際の注意事項

1. スマートフォンのサービス構造を知りましょう

- ・スマートフォンは携帯電話会社のみによるサービスではありません。アプリ提供者やアプリ提供サイトの運用者など多くの事業者が、それぞれ役割を持ってサービスを提供しています。
- ・無料のアプリなどの中には、広告収入などによって収益を得ることにより、アプリの提供を実現しているものもあります。このような場合、アプリに情報収集を行うプログラムが組み込まれていると、利用者情報が広告配信事業者などへ提供される場合もあります。

2. アプリの信頼性に関する情報を自ら入手し理解するように努めましょう

- ・スマートフォンには、電話帳データ、通信履歴、ウェブページの閲覧履歴、など様々な利用者情報が蓄積されます。アプリをインストールすると、これらの情報は、アプリを通じたサービス提供に利用されます。同時にこれらの情報が広告配信事業者などへ提供され、利用者の趣味・趣向に応じた広告の表示などに利用される場合もあります。
- ・利用者情報が収集・送信されて利用されることについて、プライバシー上の不安がある場合、利用者も受け身ではなく、アプリの機能や評判、提供者など、アプリの信頼性に関する情報を自ら入手し、理解に努めるようにしましょう。

3. 利用者情報の利用許諾画面などを確認しましょう

- ・アプリの信頼性を確認するためには、利用者情報がどのような目的で収集されているか、必要以上の利用者情報が収集されていないかなどもヒントになります。
- ・アプリをダウンロードする際や利用（起動）時に、収集する利用者情報に関する利用許諾を求める画面が表示される場合がありますのでよく確認してください。
- ・利用許諾画面や利用規約などにおいて、収集される利用者情報の範囲などをよく確認し、内容を理解した上で、同意・利用するように努めましょう。

（出典：総務省ホームページ、政府広報オンライン）