



スマートフォンを安心・安全に使うために！

最近、急速に普及しているスマートフォン、社内においても今回貸与している全台数機種変更を実施し切替をしました、従来の携帯電話とは様々な点が異なり、インターネットを利用するパソコンと同等の機能を備えていると言えます。情報セキュリティ対策を行って使わないと、思わぬトラブルに巻き込まれることもあります。

■インターネットとアプリケーション(アプリ)が特長のスマートフォン

スマートフォンは、携帯電話よりも大きな画面でインターネットコンテンツをスムーズに操作できたり、便利なアプリケーション(「アプリ」。地図 検索、画像編集、ゲームなど、利用者が作業の目的に応じて使うソフトウェアのこと)を自由にインストールしたり、多彩な機能を自分が使いやすいように設定して利用できる点が人気を呼んでいます。

その半面、その中には危険なアプリケーションが混じっている場合もあります。

⇒全端末制限を設けます(KDDI Smart Mobile Safety Manager) ※後日設定

☆最近の注意

①不正アプリの増加と多様化！

- ・動画を再生するアプリに見せかけ、インストールするとメールアドレス・電話番号等の個人情報を取得し、架空の料金請求画面を出す、金銭目的としたワンクリックウェアが報告されています。
- ・スマホの機能改善ツールを装い、電話帳情報等の詐取等を目的としたアプリも増加しています。

②不審なメールやSNSの投稿等に記載されたURLからアプリをダウンロードしないように注意しましょう！

③電話帳情報を外部に送信し得る利用許諾を求めるアプリには注意しましょう！

④ブルートゥースによる乗っ取りに注意しましょう！

- ・現在、ブルートゥースは大抵のスマホやパソコンに標準搭載されている。コードレスのヘッドホンやキーボード、マウス、ハンズフリーの通話装置、スマホ画面をテレビ画面に映すシステムなど、多様な使われ方をしています、その中で2分弱のパソコン操作で簡単にスマホを乗っ取り、写真などの情報を抜き取るハッカーが存在し、ハッカーの無線が届く範囲に、ブルートゥース機能を有効にしたスマホがあるだけでよく、駅のホーム、ホテルのロビー、喫茶店など日常の生活エリアでハッキングにあう危険性がある。既に端末メーカーは対策に乗り出したもようだが、対策ソフトなどが配布され利用者に行き渡るまでには時間がかかる可能性がある。内閣サイバーセキュリティセンターでは、基本ソフトを最新のものに更新すること、安全が確認されるまでは**ブルートゥースの機能をオフにする**ことなどを当面の対応として推奨しています。



※社内ツール



LINE WORKSを有効に活用してください！！