平成２４年９月１日号
第６４０号

優和のミニかわら版

（この資料は全部お読みいただいても60秒です）

スマートフォンのセキュリティリスク

ここ数年、インターネットの利用環境が大きく変化しています。スマートフォンやタブレット端末の普及により、いつでもどこでも必要な情報にアクセスできるようになりました。しかし、利便性が高まる一方で気をつけなければならないセキュリティの問題があります。

【紛失・盗難のリスク】

通常の携帯電話に比べてスマートフォンは外出中でも社内メール宛のメール確認や返信をスムーズに行え、添付ファイルの閲覧・編集もできるので、PC がなくても多くの作業が手軽にできるメリットがあります。当然、肌身離さず持っているスマートフォンですから、外出時も社内にいるのと同じように仕事ができます。PC は企業によってセキュリティポリシー上、社外持ち出し不可であっても、電話として使うスマートフォンは容易に持ち歩けます。しかしその反面、紛失・盗難といったリスクがあります。PC に近い情報を扱うスマートフォンを盗まれたり、失くしたときのリスクは通常の携帯電話に比べて増大します。紛失・盗難の注意はもちろん、万が一の紛失に備えて端末の起動をパスワードで保護するなどの対策は行っておきましょう。

【OS によるリスク】

ではスマートフォンならどんな端末でも同様のリスクがあるかというと、そうではなく端末に搭載される OS によって危険度は異なります。代表的な例としては、アプリの配布方法が OS によって異なります。Apple 社の提供する iOS 向けアプリは App Store からのみインストールが可能です。「App Store にあるすべてのアプリは Apple 社による審査があるため、悪意ある不正アプリが混入する可能性は低いと言われています。一方、Android 向けアプリでは Google Play（旧 Android マーケット） 以外でも、多種多様なアプリの入手先が存在します。個人的なサイトでのアプリ配布も可能で、それらを規制することはできないため、インストールしたアプリから知らない間にウイルスに感染する恐れが大きいと考えられます。

実際、不正アプリにより電話帳に登録されているすべての「名前」「メールアドレス」「電話番号」が流出した事件も起こっており、Andoroid 端末へのセキュリティソフトのインストールは必須といえます。しかし、無料のセキュリティソフトでは、最新の脅威に対応出来ない可能性があります。また無料のセキュリティソフトを装い、個人情報や、金銭を要求するソフトもありますので有料の信頼できるセキュリティソフトの利用をお勧めします。