ＺＴＶ技術コラム	『意外な情報流出の可能性！？』
第 42 回	

情報流出と聞くとP2P ソフトから流出と思い浮かべる方も見えるのではないでしょうか？

最近、パソコンの USB から色々な装置の充電をしている光景をよく目にします。USB はコンセントがなくても、接続装置に電源供給する目的で設計されていて、携帯電話や携帯音楽装置などの充電に使用している方も多いのではないでしょうか？ところが、これが新たな情報流失の原因になりつつあります。その原因の一つに、**「ポッドスラーピング」**と呼ばれるものがあります。

ポッドスラーピングとは、iPod のような大容量のデータが保存可能な携帯音楽端末をパソコンに接続し、特殊なソフトを使用して重要な文章、データ、個人情報などのファイルを抜き出す行為の事を言います。「ポッド」は代表的な携帯デジタル音楽端末であるアップル社 iPod の略で、「スラーピング」とは、英語で「一気飲み」を意味し、100MB 程度のデータならわずか 1～2 分程度で一気に吸い出すことができる為、この名前が付けられました。これらを合わせて作られた合成語です。

携帯音楽端末を音楽ファイルの追加・削除・変更・充電のため USB 経由でパソコンに接続して行うものが多いため、ごく自然に見えます。

また、接続されている端末が、音楽を聴くための機器として認知されている携帯音楽端末は、実際は大容量 HDD であるのに関わらず、重要な文章、データ、個人情報などを持ち出しても不信感を感じさせない可能性があります。現在の情報漏洩事件のほとんどが、内部の人間による社内データの持ち出しがきっかけになっているのを考えると深刻な問題に発展する可能性もあります。

ポッドスラーピングを防ぐには、大きく2つが考えられます。

①クライアントパソコンのセキュリティ対策

（１）ＵＳＢポートの使用制限
（２）不要なソフトのインストール禁止
（３）パソコン監視体制の強化

②重要データの管理

（１）別パソコンもしくは端末に管理しデータを分ける
（２）重要データをコピーできなくするようなアプリケーションを導入する

個人では、管理には限界があると思われますので、パソコンの起動にパスワードをかけるなどの簡単なセキュリティでも効果はあると思います。

また、企業では携帯音楽端末だけではなく、パソコンへ接続される機器（例えば、携帯、デジタルカメラ、USB メモリなど）を個人で携帯する物までも管理する必要が出てきたのかも知れません。企業ポリシーとして、日々増加するデータをどのように管理しているのかを考えなければならないのではないでしょうか？