

⚠ USBデバッグモード接続の危険性

スマートフォンへの情報漏えい対策、本当に大丈夫?



最近よく耳にする「個人情報漏えい問題」。

先日でも大規模な情報漏えい事件があり、自社のセキュリティを見直された企業の方も多いのではないのでしょうか。

スマートフォンをパソコンへUSB接続した場合、一般的な接続方式としては下記の3方式があります。

- 1 USB大容量ストレージ・リムーバブルディスク・MSCモード** (Mass Storage Class, MSC)
- 2 MTPデバイスモード** (Media Transfer Protocol, メディア転送プロトコル)
- 3 PTPデバイスモード** (Picture Transfer Protocol, 画像転送プロトコル)

この3方式については、Windowsのグループポリシーでの制御*やIT資産管理ツールのデバイス制御機能で、おおよその対応は可能です。しかし、スマートフォンの接続方式には、一般的には知られていないもう一つの方法があるのです。

* Windowsローカルポリシー内の「リムーバブルディスク」制御機能と、「WPD (Windows Portable Device=MTP/PTPデバイス)」制御機能で使用禁止にすることが可能

🔒 デバッグモードの危険性

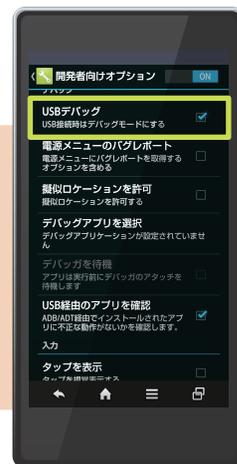
もう一つの接続方法とは、アプリケーション開発者向けに用意されている「USBデバッグモード」。

デバッグモードの通信は、MTP・PTP・MSCの通信を禁止していてもファイルが書き出せてしまいます。

4 USBデバッグモード

USBデバッグモードとは、アプリケーション開発者向けに用意されたモードです。

スマートフォンとパソコン上のアプリケーションが相互通信を行うことで、MSCやMTP・PTP通信を用いずに、データの送受信を可能とします。



!!! 写真や音楽をパソコンで整理できるアプリに注意

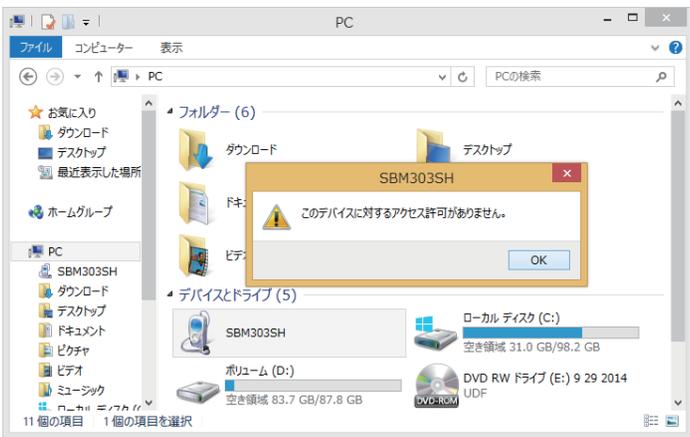


知らないうちにパソコン利用者がデバッグモードを使用してしまう例として、スマートフォンのデータをパソコンで整理したり、バックアップするソフトウェアの利用があげられます。

これらのソフトは、デバッグモードでの通信を利用している場合が多いため、MSCやMTP、PTPを制御していたとしても、情報漏えいしてしまう危険性があります。

スマートフォン(Android)のUSBデバッグモードをSTOP!

DeviceLockを使用すれば、USBポートレベルでデバイスの使用を禁止することができるため、USBデバッグモードも使用禁止にすることが可能です。また、リムーバブルやMTP（PTPを含む）デバイスの制御もできるため、スマートフォンのUSB接続4方式に対して制御が可能になり、スマートフォンによる情報漏えいに対するセキュリティを実現することができます。

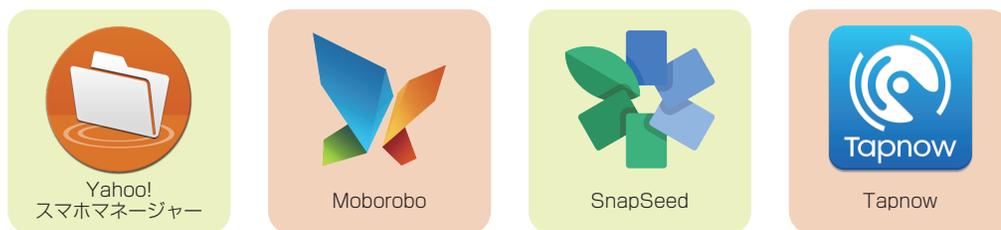


Windowsのファイルシステム上で使用不可となります。



スマートフォン同期アプリケーションとの同期もできないようになります。

スマートフォンとパソコン間でファイルのやり取りをする際、デバッグモードの通信を行うソフトは下記のようなソフトがあります。



DeviceLock 100ライセンスの購入例

製品名	標準価格・数量	合計金額
DeviceLock Base ライセンス 100-199	@5,800 × 100本	¥580,000

- ※ 上記のライセンスには、初年度（1年間）の保守が含まれております。
- ※ プログラムは、ダウンロードで入手可能です。
- ※ 全ての価格には消費税が含まれておりません。
- ※ 全ての価格表は2016年4月現在のものです。
- ※ 全ての価格は予告無く変更される可能性があります。
- ※ メディアキットのご購入は任意です。（標準価格：¥5,500）

http://devicelock.jp/article/debug_mode.html



株式会社 ラネクシー
<http://www.runexy.co.jp>

<http://devicelock.jp/>
dl_sales@runexy.co.jp

お問い合わせ