青い森のサイバーセキュリティ

令和５年正月
青森県警察本部
サイバー犯罪対策課

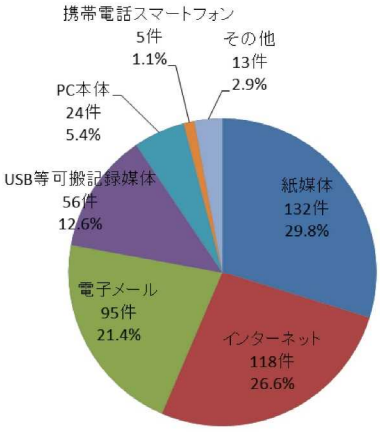
USBメモリの管理

◎紛失の絶えないUSBメモリ

セキュリティ関連のニュースサイトでは、USBメモリ紛失事故の記事がひと月に複数件載ることも珍しくありませんが、USBメモリの管理は適切に出来ていますでしょうか？

USBメモリは大容量化と高速化が進み、テラバイト級のデータを簡単に持ち歩くことも可能になる一方、小型で軽量なため、使用後の不適切な保管や移動中の落下など、ちょっとしたミスで紛失しやすく、情報漏えいに直結してしまう危険性が非常に高くなっています。

特に、個人情報など機密性の高いデータを取り扱う業務に使用する場合には、暗号化などのデータに対する適切なセキュリティの設定、使用後の確実な消去など、USBメモリの高度な管理が求められます。



2017年（N=386件）		2018年（N=443件）
紙媒体（150件）	→	紙媒体（132件）
インターネット（87件）	→	インターネット（118件）
電子メール（77件）	→	電子メール（95件）
USB等可搬記録媒体（41件）	→	USB等可搬記録媒体（56件）

紙媒体による漏えい件数が最も多い

インターネット・電子メール・USB経由が増加

引用：JNSA（日本ネットワークセキュリティ協会）「2018年情報セキュリティインシデントに関する調査結果」

◎サイバー攻撃の経路にも

管理の行き届いていないUSBメモリは、インターネットに接続されていないシステムがマルウェアに感染する経路となり易いほか、USB自体がマウスや通信端末など様々なデバイスを接続出来る極めて高機能なインターフェースであるため、これを悪用し、接続するだけでマルウェアに感染したり、高電圧によりPCを物理的（電気的）に破壊するなどの細工が施された危険なUSBデバイスによる攻撃（BadUSB攻撃）が見られています。

最近では、そのような悪意のある細工を仕掛けたUSBメモリを郵送で送りつけたり、意図的に落とし物のように見せて関係者に拾わせるなどの方法で標的のシステムに接続させるという手法も見られることから、不審なファイルだけでは無く、入手経路のはっきりしないUSBメモリ自体もリスクであると考え、対策に取り組みましょう。