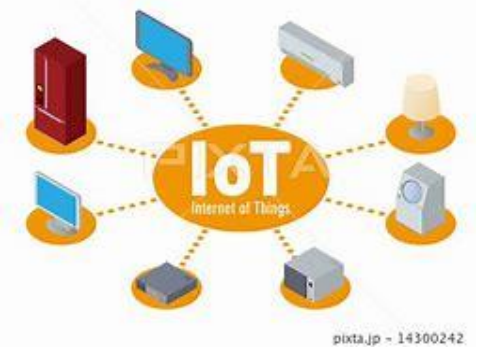
Ksisnetだより
発行:Ksisnet事務局
令和 2年 6月 19日
Vol.80

IoT機器の情報セキュリティ対策してますか？



新型コロナウイルスでテレワークやオンライン学習が広がり、新たな「ＩｏＴ機器」を導入する会社や家庭が増える中、サイバー攻撃のリスクが増しています。

「ＩｏＴ機器」は非常に便利な反面、誤った状態でネットワークに接続し、利用し続けると、攻撃者によるサイバー攻撃の対象となり、自身が被害者となるだけでなく、世界中に大きな被害を与えることがあります。

【攻撃手口】

攻撃者は、IoT機器の脆弱性をついて**不正アクセス**したり**ウイルスに感染**させることにより、IoT機器に登載されている**機能を不正利用**したり、ウェブサイトやサーバー等に**DDoS攻撃**を行ったりします。

更にウイルスに感染したIoT機器は、同じ脆弱性を持つIoT機器がインターネット上にないかを探し、存在すればそのIoT機器もウイルスに感染させ、**次々と感染範囲を拡大**させていきます。

現在使用中の
ＩｏＴ機器があれば、
まずパスワードの確認を！
初期設定のままや、
連続する数字などの
推測されやすい
パスワードはNG！！

IoT機器を安全に利用する上で考慮しなくてはいけないこと

① IoT機器購入前

セキュリティ機能やサポート体制はメーカーにより異なります。
必ず**内容を確認**し、利用目的に最も適した機器を購入する。

② ネットワーク接続前

まずマニュアルを熟読し、初期設定や設定変更方法を把握した上で
◎ 必ず**パスワードの変更**をする
◎ **セキュリティ機能の**確認をし、**設定を有効**にする

③ ネットワーク接続後

機器の最新バージョンが公開されたら**アップデート**を確実に実施し、サポート終了前に他機種の購入を検討する。

電源をオフにしておくことで駆除できるウイルスもあるので、機器を使用しない時は電源をオフにしておく。

④ IoT機器廃棄時

機器に保存されている個人情報が漏えいしないよう、確実に**初期化**する。

情報セキュリティ対策をしっかりとし、組織内で情報共有しましょう！

（IPA「情報セキュリティ10大脅威2018」「情報セキュリティ10大脅威2019」「情報セキュリティ10大脅威2020」を基に作成）