IoT機器を御購入されるお客様へ

様々なIoT機器に対する乗っ取り事案に御注意ください！！

※ IoT機器＝インターネットに接続された家電や自動車、工場設備などのあらゆる電子機器

乗っ取りによる被害事例

○ 防犯用、業務用のネットワークカメラが「操作不能となる」「画像を不正に盗み見られる」「記録データや設定を改ざんされる」などの被害を受ける。

○ ファックスや複合機（プリンター）へ外部から接続され、コピーや印刷したファイルが盗み取られる。

○ 遠隔操作を目的とするウイルスや不正プログラムに感染させられ、サイバー攻撃の踏み台とされる。

○ エアコンなどのIoT機器を遠隔操作され、生活に支障をきたす。

対策方法

1 初期設定のパスワードは、推測されにくいパスワードに必ず変更しましょう。

2 最新のソフトウェアに更新しましょう。

3 動作上問題なければ、ルーター経由でネットワークに接続し、不要な通信をブロックしましょう。

4 通常使用しない機能は停止しておきましょう。

便利なIoT機器を快適に利用していただくためのお願いです。

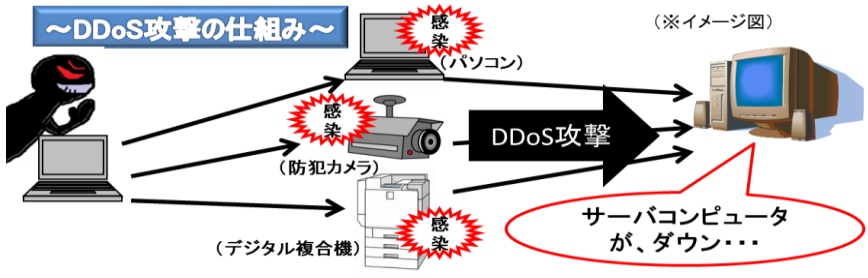
対策を怠ると・・・

1 犯罪の踏み台にされる。

知らない間にウイルスに感染し、

「DDoS攻撃」

に加担している可能性があります。



※ DoS攻撃＝サーバやネットワークなどに意図的に過大な負荷をかけたり、脆弱性を利用してサービスの提供を不能とする攻撃

※ DDoS攻撃＝複数のコンピュータを用いて行われるDoS攻撃

2 防犯機能の低下、プライバシーの侵害、平穏な生活の妨害

IoT機器に不正アクセスされることで、「防犯上の弱点を把握される。」「各機器に記録された内容から私生活を盗み見られる。」「ウイルス感染した家電を不正に操られる。」などのおそれがあります。

発行：相談窓口

愛媛県警察本部生活安全部サイバー犯罪対策課 TEL089-934-0110