気軽に読める暮らしのネタ
イノスマンスリー INOS Monthly
News Letter
2025.12月
Vol. 283

スマート家電（IoT 家電）のセキュリティは大丈夫？安全な使い方とは

インターネットに接続して便利に遠隔操作できるスマート家電ですが、そのぶんプライバシーや個人情報が漏洩してしまうリスクがあります。今回は、そんなスマート家電を安全に使うためのセキュリティ対策をご紹介します。

スマート家電に潜む情報漏えいリスク

スマート家電は、インターネットに接続されているためハッキングなどの悪意ある攻撃を受けるリスクもあります。インターネットを介して悪意をもった相手にのっとられると、個人情報の漏えいや犯罪に巻きこまれる危険があります。

たとえば、玄関のスマートロックを勝手に開けられて空き巣に入られたり、見守りカメラをハッキングされて家の中の映像を見られたりと、さまざまな危険があります。

スマート家電のセキュリティ対策の方法

こうした被害に遭わないために、以下の対策を行いましょう。

1.　信頼できるメーカーの製品を信頼できるお店で買う

出どころの不明な製品や安すぎる製品には、マルウェアが仕込まれていたり、初期 ID とパスワードが漏えいしていたりする危険があります。信頼できるメーカーの製品を選びましょう。

2.　初期パスワードを複雑なものに変更する

メーカー出荷時の初期パスワードは推測されやすいものが多いため、英数字や大文字小文字、記号を混ぜた複雑なものに変更しましょう。ID も変更できる場合は変更しておきましょう。

3.　使わない機能をオフにする

誰でもアクセスできる機能など、明らかにリスクの高い機能や使わない機能は、オフにしておきましょう。

4.　ソフトウェアを定期的に更新する

ソフトウェア(ファームウェア)の更新には、セキュリティの脆弱性を修正する重要な役割があります。更新を怠ると、ハッキングされる危険性が高まります。自動更新機能がある場合は有効化しておきましょう。

5.　使わない IoT 家電の電源は切っておく

使わなくなった IoT 家電でも、電源が入っているとハッキングの標的になる可能性があります。特に古い製品はサポートが終了している場合があるため、使用しない場合は電源を切るかネットワークから切断しましょう。

6.　Wi-Fi ルーターの ID とパスワードを変更する

IoT 家電だけでなく、Wi-Fi ルーターのセキュリティも重要です。こちらも初期 ID とパスワードは複雑なものに変更しておきましょう。

有限会社 滝本工務店
0120-916-672
〒959-0214 新潟県燕市吉田法花堂 1623
TEL 0256-93-4844 FAX 0256-93-4877