

被害者・加害者
にならないために

IoTのセキュリティ対策は万全ですか？

とても身近になってきたIoT機器ですが、みなさんの家庭にもテレビ、ゲーム機、スマートスピーカー、WEBカメラ、スマート家電などインターネットに接続された機器が1台くらいはあるのではないのでしょうか？インターネットから映像や音楽やゲームなどをダウンロードして楽しんだり、スマホからカメラや家電を操作や管理したり、インターネットを介することでとても便利に利用できる反面、様々な危険が潜んでいることを御存じでしょうか？機器のほとんどにはパスワードが設定されていますが、購入してから一度もパスワードを変更していないという方は少なくないのではないのでしょうか。パスワードを初期設定のまま使用することはとても危険です。今回はこのようなセキュリティリスクへの対策を考えていきたいと思います。

IoT機器のセキュリティチェック！

なぜIoT機器のセキュリティチェックが必要なのでしょうか？インターネットに繋がっているということは、外部と接続されており攻撃を受ける可能性があるということです。機器が乗っ取られ情報が盗み取られたり、知らない間にサイバー攻撃に加担させられたり、被害者にも加害者にもなりうるのです。そうならないためにも対策を講じておく必要があります。

1.何がインターネットと繋がっているかを把握する

パソコンやスマホはインターネットと繋がっていることは理解していても、IoT機器がインターネットと繋がっていると意識している方は少ないのではないのでしょうか？まずはどの機器がインターネットと繋がっているか、現状どのようなセキュリティ対策をしているのかを把握することが重要です。

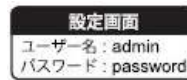


2.初期パスワードの変更

最近の機器は買ってすぐに使えるようにしていることが多く、パスワードなどが簡単に設定されている傾向があります。買ったままのパスワードはすぐに破られ、機器が乗っ取られる危険性があることを認識しましょう。もし買った状態のパスワードを使用している場合は、今すぐ説明書を読んでパスワードを変更されることをお奨めします。

また変更する際は簡単なパスワードや他のものとの使いまわしも避けましょう。

さらに定期的にパスワードを変更するとよりセキュリティを強固にすることができます。



メーカーによっては左のような簡単なパスワードが初期設定されています。必ず変更しましょう。

3.ファームウェアの更新

機器によっては「ファームウェア」という機器を制御するソフトが組み込まれているものがあります。ファームウェアは不具合や脆弱性の修正や機能の改善などの度にメーカーから提供されます。ファームウェアを最新のものに保つことでセキュリティの穴を防ぐこととなりますので、定期的にチェックし更新しましょう。またファームウェアの更新などのメーカーサポートや問い合わせ窓口がないような機器の購入や使用は控えた方が良いでしょう。



4.インターネットに直接つながらない、可能であればポート管理する

インターネットをPCやスマホなど複数で使用されているのであれば、インターネットへの出口にはルーターという機器が設置されているかと思いますが、IoT機器も必ずこのルーターを介してインターネットへ接続するようにしましょう。ルーターである程度の脅威を防ぐことができます。またセキュリティ対策をしていない機器をフリーWi-Fiに繋ぐことも危険ですので控えるようにしましょう。

さらにIoT機器の23番ポート(telnet)への攻撃が増えていますので、ルーター側で適切なポート管理を行うことも対策として効果があります。インターネットやルーターのメーカーホームページ、取扱説明書でポート管理の方法を確認しましょう。

5.インターネットへの接続が必要か考える

IoT機器にインターネットへの接続機能がある場合でも、機能自体が不要であれば接続せずに使うことも検討しましょう。

また使用してないものや頻度が少ないものは電源を切っておくか、必要な場合のみインターネットへ接続するように心掛けましょう。

IoTの未来...

IoT機器は急速に普及が進んでおり、5Gのサービス(大容量で超高速な通信サービス)が2020年春ごろから開始されることも考えますと、今後も増え続けていくことが考えられます。家の中のあらゆる家電がインターネットを介して便利に利用できることはもちろん、自動車もインターネットと接続され、自動運転の一端を担ったり、渋滞などの情報収集やエアコンを事前につけるなど外部からの命令も可能となってくることでしょ。

そうなってくるとIoT機器への攻撃は、単純に「情報が盗み取られた」「サイバー攻撃に加担させられた」ということでは済まなくなり、命を脅かすことにもなりかねません。

今後はIoT機器に対するセキュリティリスクを正しく認識すること、セキュリティ意識を向上し適切な対策を講じていくことがますます重要となってきます。

被害者や加害者とならないためにも今からIoTのセキュリティに関する知識を蓄え、来たるIoT時代に備えておきましょう。

スマホで操作できる機器



IoT LEDランプ

スマホで電球のON、OFFや調光ができ、遠隔で照明を操作することでセキュリティ効果も期待できます。



めざましカーテン モーニンプラス

スマホでカーテンを開ける時間を設定でき、太陽の光で気持ちよく起きる事ができます。もちろん閉める時間も設定でき、こちらもセキュリティ対策に役立ちます。

これらの他に、スマホで家の鍵を施錠できたり、施錠を確認できるシステムもあります。そんなシステムが第三者に乗っ取られたら大変です。IoT機器のセキュリティには十分注意しましょうね。

開発室から



前号では本州最北端、青森県下北半島の大間崎に行ったことをお伝えしましたが、今回は九州の宮崎に行って来ました。夕方に金沢を出て、宮崎の青島には朝の6時ごろに到着しました。鶴戸神宮や堀切峠に行き、南国のムードを味わいました。帰りは阿蘇の草千里に寄り道もしました。とても楽しいドライブでしたが、片道15時間はやっぱり辛いです...

