滋賀県警察サイバーセキュリティ情報

サイバーコネクトSHIG@

R５年度 No. 9

今、注目のサイバーセキュリティに関する情報をお届けします。

ネットにつながっているモノ放 置していませんか？

皆様の事業所では、使っていないIoT機器はどうしていますか？ 使っていないけど、とりあえずインターネットに繋げたまま、電源も入れたままにしていませんか？

警察庁では、インターネットとの接続点にセンサーを設置し、不審な通信の観測を実施しています。

令和４年の観測では、１日・１IPアドレスあたり7,707.9件と、我が国に向けられる不審な通信が多いことが分かっています。すなわち、サイバー攻撃者は、常に攻撃可能な場所を探っており、ネット上では、こうした探索行為が日常茶飯的に行われている状況です。

事業所におけるサイバーインシデントは、特に、夏休み明けといった休み明けに発覚することが多い傾向にあります。今回は、攻撃者に狙われやすい「IoT機器の放置物件」「初期設定のまま放置されている物件」について、注意すべき事項を紹介します。

事業所で使っているIoT機器の点検を実施し、もし、放置している機器があれば、対策を施し、攻撃されるリスクを少しでも減らしましょう。

サイバー攻撃者に狙われる 放置IoT物件達

使っていないWebサーバ、Webページ

○ 過去使っていたWebサーバ、Webページ
○ Webページのバックアップで管理していないもの
○ 放置バナー、リンク切れURL
○ 非公開設定するも、アクセス可能なサーバ

開設当初の設定のままのWebページ

○ IDやパスワードが初期設定のままの管理者設定
○ ユーザ権限が初期設定のままのWeb管理
○ ユーザ名などがインターネット上から見える状態で放置されているもの
○ Webページの更新は定期的に行っているもの、Web管理や設定事項が初期設定のままのもの

使っていないIoT機器

○ 使っていないのに電源が入っている、ネットにつながっているネットワークカメラや防犯カメラ
○ コロナ対策で設置しているサーモグラフィカメラやサーマルカメラ(温度測定カメラ)が乗っ取られることがある。
○ インターネットTVなどで利用されているセットトップボックス(STB)が攻撃の踏み台として乗っ取られることがある。

使っていない通信機器

○ 使っていないのに電源が入っている、ネットにつながっているルータやVPN機器
○ 初期設定のままのルータやVPN機器などの通信機器、ファイアウォールやUTMなどの制御機能
○ 大手メーカーの機器は、初期設定値が統一されており、公開されているので、そのままでは乗っ取られる可能性大


☜コネクトSHIG@では、Webページの定期的な点検をオススメしています。
なお、今回紹介した件については、次のIPAや総務省のWebページも参考にしてください。
IPA：https://www.ipa.go.jp/security/vuln/websecurity/sitecheck.html
総務省:https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/13.html

«CS情報SHIG@»サポート詐欺に注意！

滋賀県警察本部 サイバー犯罪対策課 077-522-1231（代表） 詳細は県警webページで →