SCIS 2022 2022 Symposium on Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics, Information and Communication Engineers

IP カメラのセキュリティに対する調査手法の検討と判明した問題点の考察
A study of research methods for IP camera security and Consideration of the problems identified

下山　啓 *　　松井 俊浩 †
Kei Shimoyama　　Toshihiro Matsui

キーワード IoT, IP カメラ, セキュリティ, 脆弱性

あらまし

近年 IoT デバイスの普及が進み、世界で 2022 年には 309 億台、2023 年には 340 億台になると予測されている。さまざまなものがインターネットに接続されることでウェアラブル機器や家電製品、コネクティッドカー、医療機器といったような多岐にわたって用いられるようになり、私たちの生活に大きな利便性をもたらしている。しかし、IoT デバイスが増加することにより、攻撃者が人の関与しない IoT デバイスをターゲットとすることは容易に推測でき、攻撃数も増加すると考えられる。

IoT デバイスには、プロセッサ、電力、メモリなどの制約があることから、堅牢なセキュリティが考慮されない設計となっていることが多い。その結果 2016 年、IoT デバイスをターゲットとしたマルウェア「Mirai」による感染が拡大し、世界中に大きな被害をもたらした。この件以降、IoT デバイスについて必要なセキュリティ対策を施すことが期待されたが、現状は、依然として万全な対策が施されているとは言い難い。また IoT デバイスは、誰の手にも届く場所に設置されることが多く、それは攻撃者においても直接操作ができるということであることから、物理的なセキュリティ対策も求められる。

IP カメラは、多くの IoT デバイス同様、常にインターネットにつながっていることや、セットアップ後のセキュリティ管理がほとんど行われていないといったことに加え、他の IoT デバイスに比べると比較的高性能であり、また高速大容量の通信帯域を利用できること、近年の防犯意識向上による設置数の増加といった点から特に攻撃対象となりやすい。本研究は、その攻撃対象となりやすい IP カメラのセキュリティ対策と問題点に焦点をあて、製品の分解の容易さ、チップの製造元やデータシートなどの調査、シリアル接続の可否と OS の構造調査、通信内容の調査などを系統的に実施し、適切な調査手法を検討した上、脆弱性調査を実施した。

その結果、調査対象である複数台の IP カメラにおいて、シリアル接続により Wi-Fi パスワードが容易に確認できてしまうことや IP カメラの OS として一般的に使用される Linux のシェルを管理者権限で取得できてしまうことなどいくつもの問題点を発見した。特に重要な問題点として、Linux のシェルを取得することができた場合、保存されたパスワードファイルが確認できるなど、不正操作が可能なことである。さらに確認されたパスワードについては、同一メーカーにおいて使いまわされている状況も判明した。管理者権限を持つユーザーのパスワード管理は非常に重要であり、流出してしまうと、telnet サービスの動作している機種であれば、攻撃者に不正に遠隔操作されてしまう可能性が示された。

これらの問題点は、シリアル接続による不正操作が可能であることが原因であるから、製品販売時においてデバッグ用ポートを残さない、接続が可能であっても、不要な情報を表示しない、不正に操作させないなどといった対策が必要である。

* 情報セキュリティ大学院大学 〒 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1. Graduate School of Information Security 2-14-1 Tsuruya-cho, Kanagawa-ku, Yokohama-city, Kanagawa, 221-0835, Japan.
† *