安心・安全にIoT機器を利用するためには

IoT機器のセキュリティインシデント発生の危険性及び利用者に求められる対策

セキュリティインシデント発生の危険性

- 自動車の制御ソフトウエアの遠隔操作の危険性
- 医療機器が遠隔操作可能となる危険性
- ネットワークカメラの映像の第三者による視聴の危険性
- ウイルス感染したIoT機器が踏み台としてサイバー攻撃に悪用される危険性

IoT機器利用者に求められる対策

- 初期設定されたパスワードを複雑なものへ変更
- ファームウェアの最新化
- 使用していないIoT機器はインターネットに接続しない

ライフサイクルの長いIoT機器はサイバー攻撃に狙われやすいです。マルウェアに感染したIoT機器がサイバー攻撃に悪用される事例も出ています。

IoT機器を安心・安全に使うために重要な事項

Point 1	IoT機器に初期設定されたパスワードを複雑なものへ変更する
Point 2	IoT機器のファームウェアは最新のものにする ファームウェア：コンピューターやデジタル機器を制御する基本となるソフトウェア
Point 3	使用していないIoT機器はインターネットに接続しない

参考：NOTICEホームページ(https://notice.go.jp)より

（参考）脆弱/マルウェアに感染しているIoT機器の利用者への注意喚起

総務省・NICT（国立研究開発法人 情報通信研究機構）では、脆弱なID・パスワード設定等のためサイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組（NOTICE）を平成31年2月より実施しています。約1億のIPアドレスを対象に調査した結果、約98,000件において**ID・パスワードの入力が可能**、そのうちログインまで可能だった505件が**注意喚起の対象**となりました。

詳細：総務省報道資料「脆弱なIoT機器及びマルウェアに感染しているIoT機器の利用者への注意喚起の実施状況(2019年度第2四半期）」
(http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00043.html)

作成日 令和元年１２月