

# サイバーコネクトSHIG@

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。

Cyber connect shig@

## IoT機器のセキュリティ対策

### 被害事例

企業や御家庭で使用中のルーターや、インターネットに接続する防犯カメラ、Webカメラなどが乗っ取られ、

**盗撮**

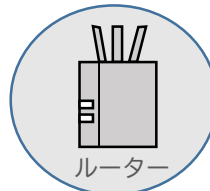
**ウイルス(マルウェア)の拡散**

**ほかの企業や機関へサイバー**

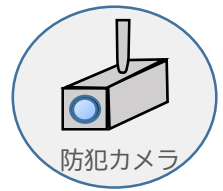
**攻撃を実行するための踏み台**

に悪用されるといった被害が引き続き確認されています。

### 狙われやすいIoT機器



ルーター



防犯カメラ



センサー



セットトップボックス

セットトップボックス (STB) : ケーブルテレビやインターネット上の動画を家庭用テレビで視聴するための機器。放送用の信号をテレビモニターに表示できる信号に変換する。

## IoT機器のセキュリティチェック項目

- 初期パスワードの設定を変更しましたか？
- ファームウェアは最新ですか？ サポートは終了していませんか？
- 使わなくなった機器をネットワークにつないだままにいませんか？

## IoT機器を安全に利用するために・・・

既出「コネクトNo.9」も参照ください！

総務省及びNICT(情報通信機構)は、IoT機器のセキュリティ対策の案内や、サイバー攻撃に悪用されるおそれのあるIoT機器の利用者に、インターネットプロバイダと連携して注意喚起を行うなどの取組を進めています。

IoT機器のセキュリティ対策取組み「NOTICE」

<https://notice.go.jp>



「CS情報SHIG@」 偽ショッピングサイト新手口に注意！

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 →

