F－CSNET NEWS
Fukuoka small and medium sized enterprises Cyber security Support NETwork

第１４号

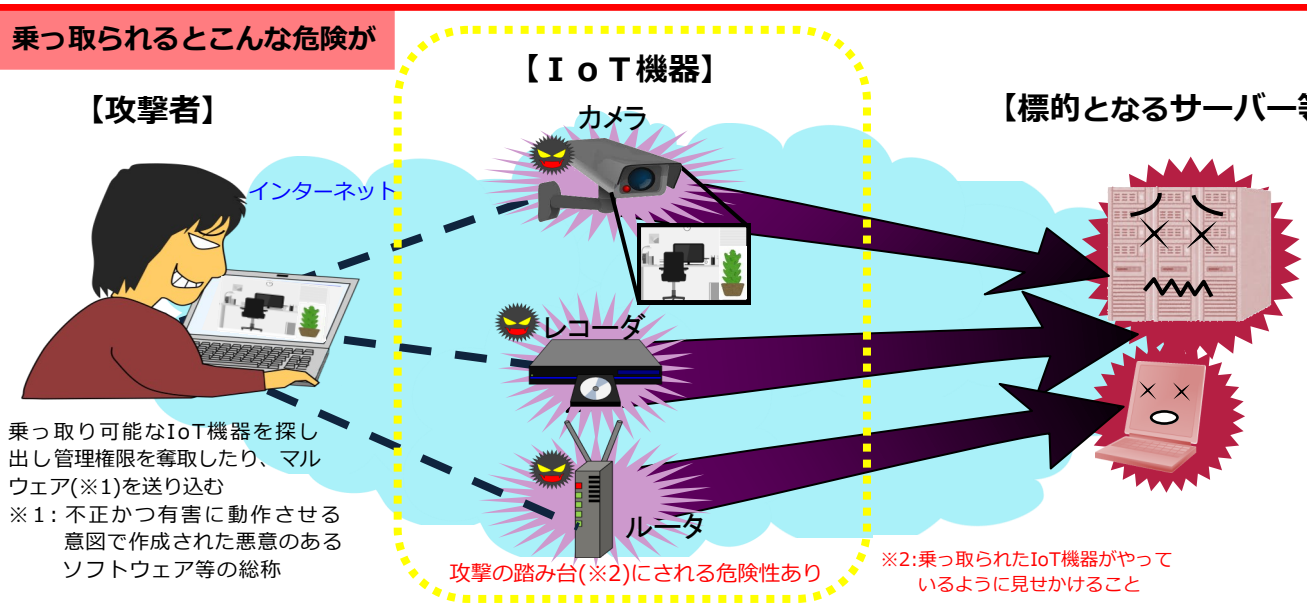
平成３０年５月
【作成】福岡県警察本部
サイバー犯罪対策課

# 「IoT」機器の乗っ取り続発！

**企業や団体等が設置した施設管理用の監視カメラなどが乗っ取られる事案が発生しています！**

※**IoT**（Internet of Things)とは、パソコンやスマートフォンだけではなく電化製品、自動車、監視カメラなどさまざまな「モノ」をインターネットに接続して便利に利用する仕組みです。

## 乗っ取られるとこんな危険が




**利用者が気付かないうちに様々な危険が生じます！**

危険 **プライバシーの侵害**

監視カメラの映像・音声を第三者に見聞きされる。

危険 **ＩｏＴ機器が制御不能**

アクセス権限を乗っ取られ、正規の所有者（管理者）がＩｏＴ機器をコントロールできなくなる。

危険 **ＩｏＴ機器が犯罪に利用される**

マルウェアに感染したＩｏＴ機器が攻撃者の命令によりDDoS攻撃(※3)等に利用される。

※3:Distributed Denial of ServiceAttackの略(分散型サービス妨害)。複数のコンピュータ等から標的のサーバに、大量のアクセスを繰り返し行い、標的のサーバー等を利用不能にする攻撃

## ＩoT機器利用者のためのルール　～　リスクの大半は簡単な注意で回避可能　～

| | |
|---|---|
| 問合せ窓口やサポートのない機器やサービスの購入・利用を控える | インターネットに接続する機器やサービスに何か不都合が生じても、適切に対処することが困難になります。また、アップデートを適切に行えないため、安全な状態で機器やサービスを利用することができなくなります。 |
| 初期設定に気をつける | ・機器のパスワードが他の人に漏れると、インターネット経由で機器が乗っ取られ、正規の所有者になりすまして不正利用されるおそれがあります。<br>・機器の管理画面の認証ID、パスワードは初期状態から推測されにくいパスワードに変更しましょう。<br>・取扱説明書やメーカー等がウェブサイト等で公開するサポート情報を確認し、機器のアップデートを行いましょう。 |
| 使用しなくなった機器の電源を切る | 使用しなくなった機器や不具合が生じた機器をインターネットに接続したまま放置すると、知らず知らずのうちにインターネット経由で機器が乗っ取られ、不正利用されるおそれがあります。 |
| 機器を手放すときはデータを消す | 機器を捨てる、売る、貸し出すなど機器を手放す場合は、機器に記憶されている情報を削除しないと利用者情報が漏洩するおそれがあります。 |

詳しくは　「IoTのセキュリティガイドライン」（ＩｏＴ推進コンソーシアム　総務省　経済産業省　平成28年7月）
IoTのセキュリティについては、IPA(独立行政法人情報処理推進機構）のホームページで確認できます。
https://www.ipa.go.jp/security/iot/