



# サイバーセキュリティの置き薬

2019年  
第2号

## プロジェクト「NOTICE」を知っていますか？

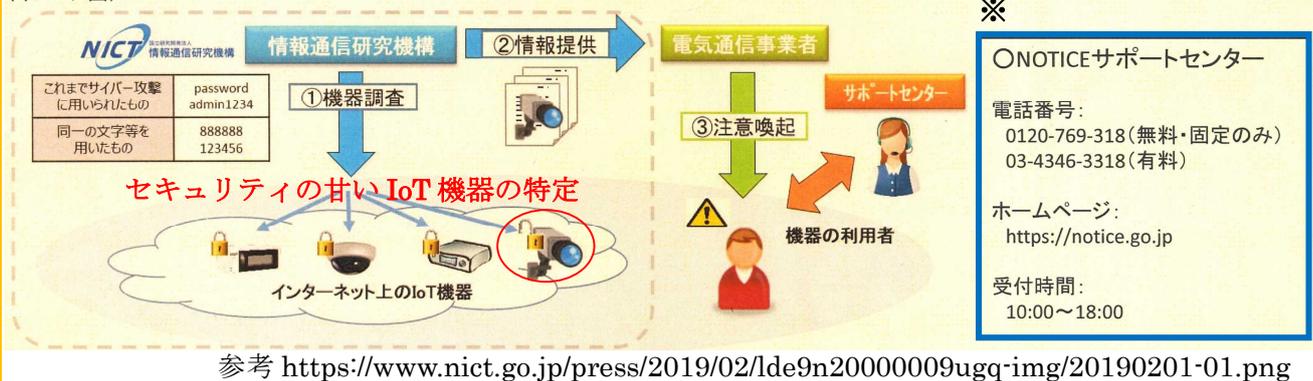
IoT 機器の急激な増加に伴い、今後セキュリティの甘い IoT 機器等を踏み台にしたサイバー攻撃の発生が危惧されています。

そのため、総務省や情報通信研究機構(NICT)などでは、IoT 機器に設定されているパスワードが安易に推測されるもの(例 123456)かなどを確認し、インターネットプロバイダを通じて機器の利用者へ注意喚起を行う取り組みプロジェクト「NOTICE」を平成31年2月20日から実施しています。

### プロジェクト「NOTICE」の概要

- ① NICT がインターネット上の IoT 機器に、容易に推測されるパスワードを入力するなどにより、サイバー攻撃に悪用されるおそれのある機器を特定。
- ② 当該 IoT 機器の情報をプロバイダに情報提供。
- ③ プロバイダが当該 IoT 機器の利用者を特定し、注意喚起を実施。  
※利用者からの問合せ対応等を行うサポートセンターを設置。

(イメージ図)



今後、プロジェクト「NOTICE」の取組を悪用して

- NICT やプロバイダを騙る第三者が利用者の ID・パスワード等の個人情報等を聞きだす
- 対策名目で料金を請求する

等の発生が懸念されます。

利用者への注意喚起は、利用者が契約する

インターネットプロバイダ以外からは行われません。

費用の請求や設定しているパスワードを聞き出すことは絶対にありません。



IoT 機器を安心して使うには、下記のセキュリティ対策を参考にしてください。



- IoT 機器のパスワードは複雑なものに変更する
- IoT 機器のプログラムは常に最新のものにする
- 使用しなくなった IoT 機器は電源を切る