

IoT機器をお使いの際は、

- 機器設定用パスワードは複雑なものに!
- 機器のファームウェアは最新の状態に!
- NOTICE※からの注意喚起には適切な対応を!

生活や暮らしを快適にする
IoT機器やスマート家電、
ウェブカメラ、ルーター、
センサー機器が危険な状態かも……。

※セキュリティ対策が必要なIoT機器の利用者に、ご契約のプロバイダから、
注意喚起を行う「**NOTICE**」プロジェクトを実施しています。
サポートセンターにて、パスワード変更等の必要なセキュリティ対策を案内します。

(注) プロバイダからの注意喚起や、サポートセンターでの案内にあたり、
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。

お問い合わせ **NOTICE** サポートセンター 受付時間 10:00～18:00 (年末年始を除く)

0120-769-318 (無料・固定電話のみ)

TEL 03-4346-3318 (有料)

さらに詳しい情報はWEBでも公開中
<https://notice.go.jp>



⚠️セキュリティ対策が不十分なIoT機器は、サイバー攻撃に悪用される可能性があります。

IoT機器とは

近年、技術の進展により、あらゆるものがインターネット等のネットワークに接続されるIoT：Internet of Things/AI時代が到来し、IoT機器の普及が進んでいます。センサーやウェブカメラなどのIoT機器は、①機器の性能が限定されている、②管理が行き届きにくい、③ライフサイクルが長いなど、サイバー攻撃に狙われやすい特徴を持っています。



IoT機器を狙ったサイバー攻撃とは

インターネット上のサイバー攻撃のうち、特にIoT機器を狙ったものが急増しています。脆弱なID・パスワード設定がされているなどセキュリティ対策に不備があるIoT機器は、マルウェアに感染しサイバー攻撃に悪用されるおそれがあります。諸外国においては、IoT機器を悪用した大規模なサイバー攻撃（DDoS攻撃）によりインターネットサービスが停止し、社会経済に深刻な被害が生じた例があります。



安心・安全にIoT機器を利用するためには

- ⚠️ IoT機器の管理用パスワードは複雑なものにする（初期設定の共通パスワードは避ける）。
- ⚠️ IoT機器のファームウェアは常に最新のものにする。
- ⚠️ 使用していないIoT機器はインターネットに接続しない（または電源を切る）。

NOTICEの概要



NICT 国立研究開発法人 情報通信研究機構

1 機器調査

NICTは、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ことなどにより、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報をプロバイダに通知します。

プロバイダ

2 注意喚起

プロバイダは、NICTから受け取った情報を元に当該機器の利用者を特定し、電子メールなどにより注意喚起を行います。

利用者

3 設定変更等

注意喚起を受けた利用者は、注意喚起メールやサポートセンターサイトの説明などに従い、パスワード設定の変更、ファームウェアの更新など適切なセキュリティ対策を行っていただくようお願いします。

サポートセンター

4 ユーザサポート

総務省が設置するサポートセンターは、ウェブサイトや電話によるお問い合わせ対応を通じて利用者に適切なセキュリティ対策等をご案内します。

- 注意**
- 利用者への注意喚起は、ご契約のプロバイダ以外からは行いません。
 - プロバイダからの注意喚起や、サポートセンターでの案内にあたり、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。
 - ご不明、ご不安な点があれば、サポートセンターへお問い合わせください。

お問い合わせ NOTICE サポートセンター 受付時間 10:00～18:00 (年未年始を除く)

0120-769-318 (無料・固定電話のみ)
03-4346-3318 (有料)

さらに詳しい情報はWEBでも公開中
<https://notice.go.jp>

