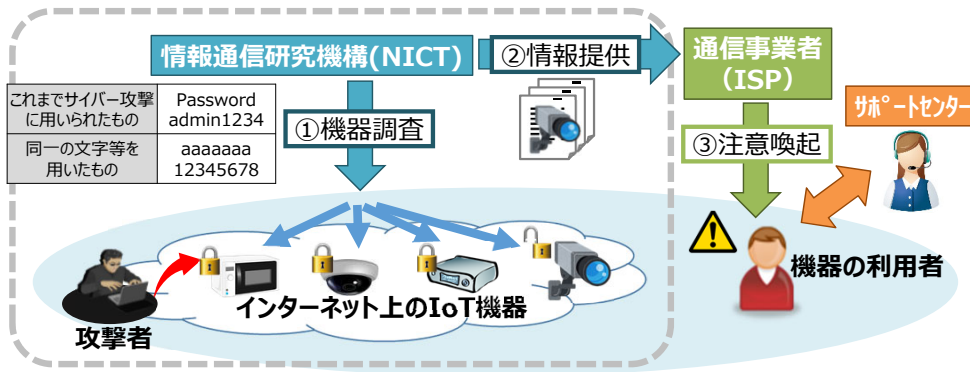


# IoT機器調査及び利用者への注意喚起（NOTICE等）

- 情報通信研究機構(NICT)がサイバー攻撃に悪用されるおそれのあるIoT機器を調査し、インターネット・サービス・プロバイダ(ISP)を通じた利用者への注意喚起を行う取組「NOTICE」を2019年2月より実施。
- NOTICEの取組に加え、マルウェアに感染しているIoT機器をNICTの「NICTER」プロジェクト※で得られた情報を基に特定し、ISPから利用者へ注意喚起を行う取組を2019年6月より開始。

※NICTが、インターネット上で起こる大規模攻撃への迅速な対応を目指したサイバー攻撃観測・分析・対策システムを用いて、ダークネットや各種ハニーポットによるサイバー攻撃の大規模観測及びその原因（マルウェア）等の分析を実施。

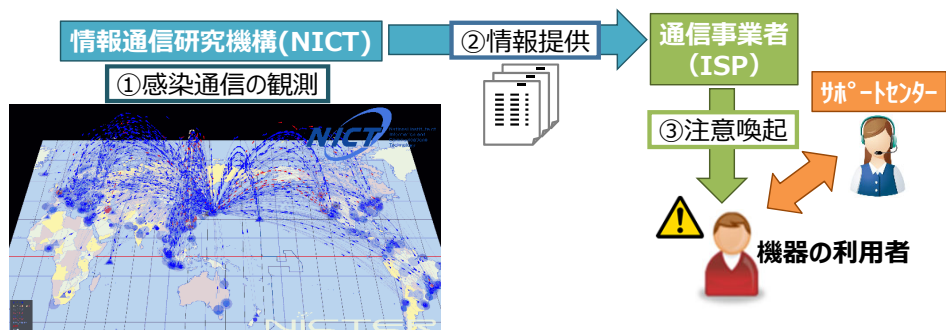
## 【NOTICEの概要】



調査対象：パスワード設定等に不備があり、サイバー攻撃に悪用されるおそれのあるIoT機器

- 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して、サイバー攻撃に悪用されるおそれのある機器を特定。
- ② 当該機器の情報をISPに通知。
- ③ ISPが当該機器の利用者を特定し、注意喚起を実施。

## 【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取組概要】



調査対象：既にMirai等のマルウェアに感染しているIoT機器

- ① NICTが「NICTER」プロジェクトにおけるダークネット※に向けて送信された通信を分析することでマルウェアに感染したIoT機器を特定。  
※NICTがサイバー攻撃の大規模観測に利用しているIPアドレス群
- ② 当該機器の情報をISPに通知。
- ③ ISPが当該機器の利用者を特定し、注意喚起を実施

# IoT機器調査及び利用者への注意喚起（2019年9月まで）

- 2019年9月までに調査のための手続きが完了しているインターネット・サービス・プロバイダ（ISP）34社に係る約1.0億IPアドレスに対して調査を実施。

## 【NOTICEの取組結果】

## 【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取組結果】

ID・パスワードが入力可能であったもの

約98,000件

（直近での調査）

【6月時点：約42,000件】

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの

延べ505件

【6月時点：延べ147件】

ISPに対する通知の対象となったもの

80～559件

（1日当たり）

【6月時点：112～155件】

## （参加ISP：計34社）

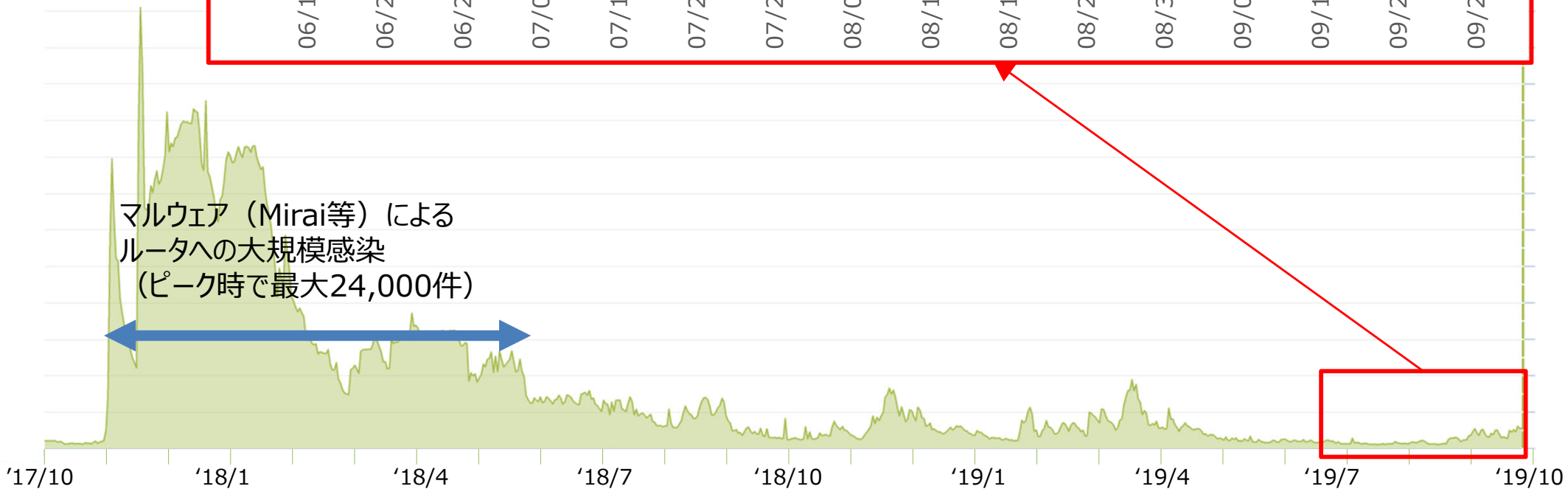
株式会社秋田ケーブルテレビ  
イツ・コミュニケーションズ株式会社  
株式会社NTTドコモ  
株式会社QTnet  
ケーブルテレビ株式会社  
山陰ケーブルビジョン株式会社  
株式会社ZTV  
株式会社TOKAIケーブルネットワーク  
株式会社ベイ・コミュニケーションズ

株式会社朝日ネット  
株式会社インターネットイニシアティブ  
株式会社愛媛CATV  
近鉄ケーブルネットワーク株式会社  
株式会社ケーブルテレビ品川  
株式会社シー・ティー・ワイ  
ソニーネットワークコミュニケーションズ株式会社  
ニフティ株式会社

アルテリア・ネットワークス株式会社  
エヌ・ティ・ティ・コミュニケーションズ株式会社  
株式会社オプテージ  
KDDI株式会社  
株式会社ケーブルネット鈴鹿  
株式会社ジュピターテレコム（グループ会社計10社）  
ソフトバンク株式会社  
ビッグロブ株式会社

# (参考) マルウェアに感染しているIoT機器の検知状況について

## マルウェアに感染しているIoT機器の検知数 (2019/6/15~9/30)



NICTERプロジェクトにおける長期的な観測傾向 (2017/10/1以降)