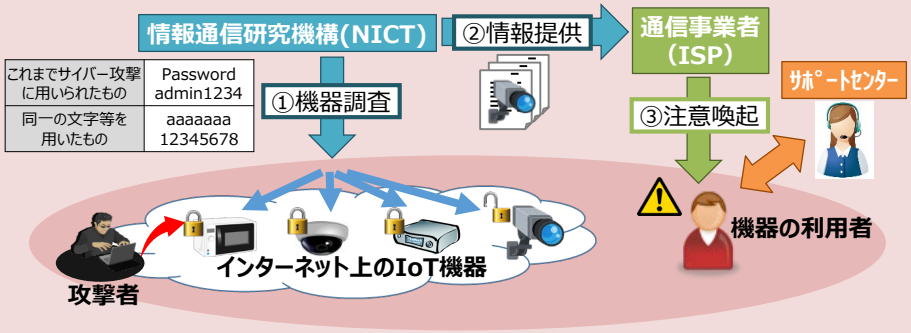
IoT機器調査及び利用者への注意喚起

- 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注意喚起の概要】

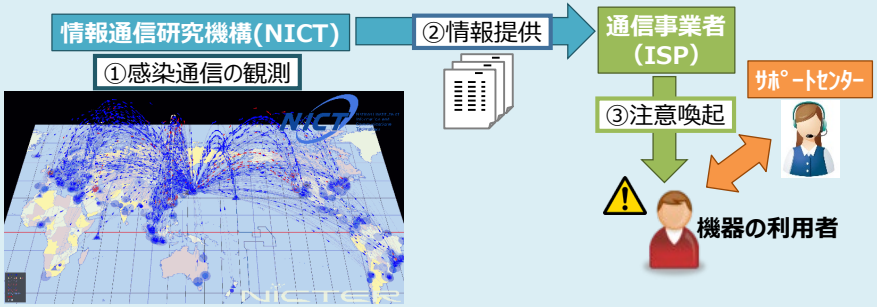


調査対象：パスワード設定等に不備があり、**サイバー攻撃に悪用されるおそれのある**IoT機器

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。

【NICTER注意喚起※の概要】

※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



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