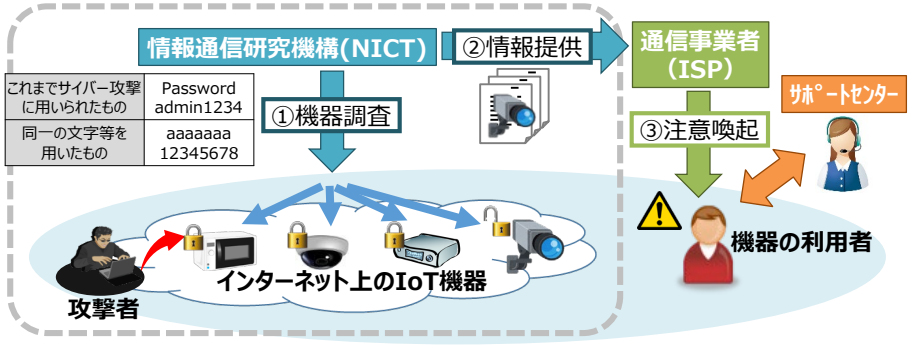
IoT機器調査及び利用者への注意喚起（NOTICE等）

別紙

- 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。

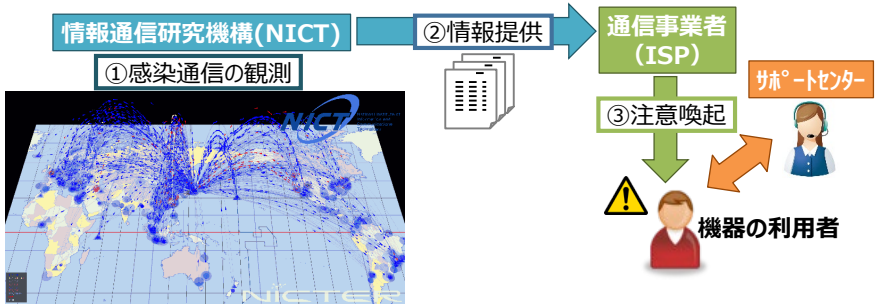
【NOTICEの概要】



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12月まで）

➢ 2019年12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）41社に係る約1.1億IPアドレスに対して調査を実施。

【NOTICEの取組結果】

ID・パスワードが入力可能であったもの → 約111,000件（直近での調査）【9月時点：約98,000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1,328件【9月時点：延べ505件】

【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】

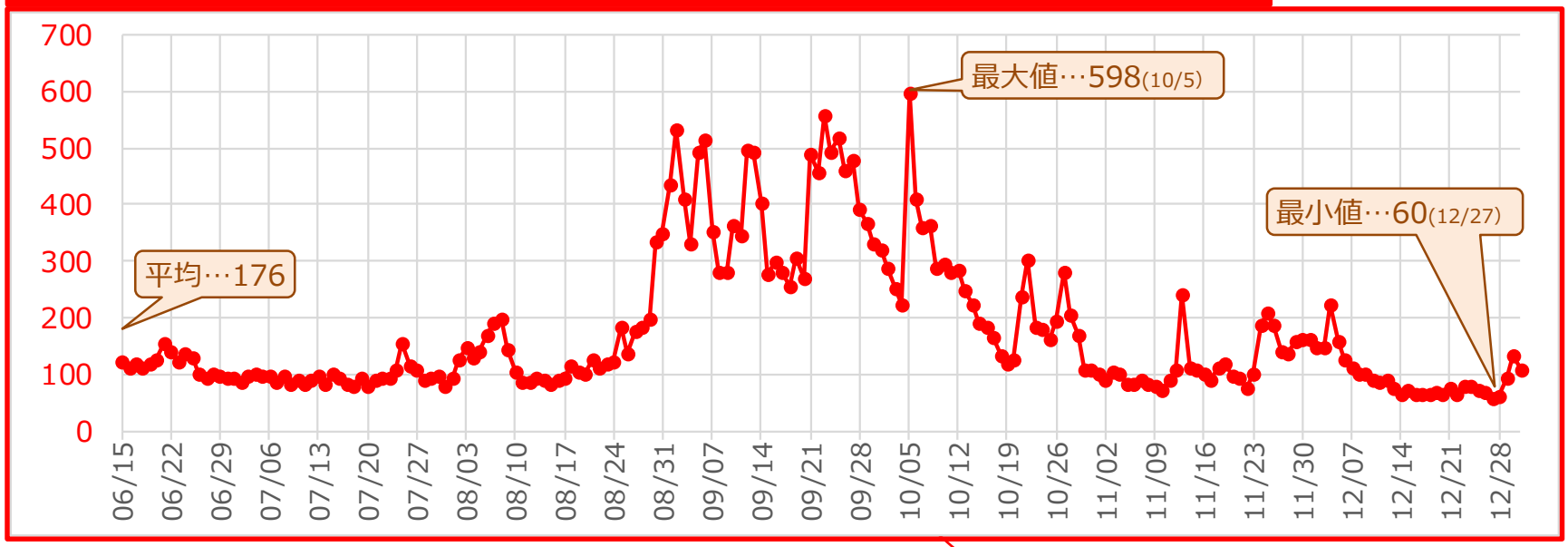
ISPに対する通知の対象となったもの → 60～598件（１日当たり）【9月時点：80～559件】

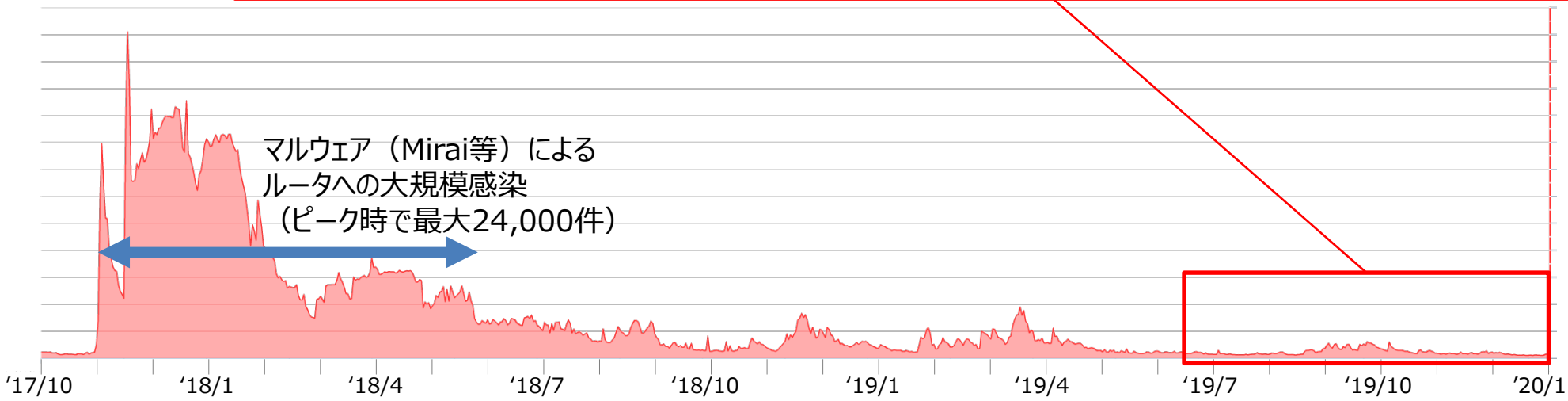
（参加ISP：計41社） ※下線は2019年度第3四半期の新規参加ISP（7社）

株式会社秋田ケーブルテレビ
諫早ケーブルメディア株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
株式会社愛媛CATV
近鉄ケーブルネットワーク株式会社
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
株式会社TOKAIコミュニケーションズ
ビッグローブ株式会社
株式会社朝日ネット
イッツ・コミュニケーションズ株式会社
株式会社NTTドコモ
株式会社オプテージ
グリーンシティケーブルテレビ株式会社
株式会社ケーブルテレビ品川
GMOインターネット株式会社
株式会社ZTV
株式会社テレビ岸和田
東北インテリジェント通信株式会社
株式会社ベイ・コミュニケーションズ
アルテリア・ネットワークス株式会社
株式会社インターネットイニシアティブ
株式会社NTTぷらら
株式会社Qtnet
KDDI株式会社
株式会社ケーブルネット鈴鹿
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
株式会社TOKAIケーブルネットワーク
ニフティ株式会社

（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（2019/6/15～12/31）





NICTERプロジェクトにおける長期的な観測傾向（2017/10/1以降）