別紙

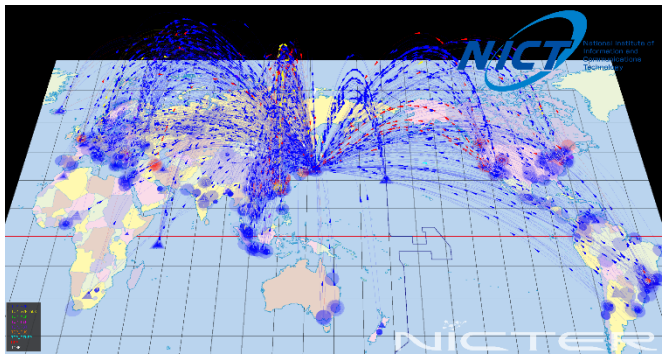
IoT機器調査及び注意喚起の実施状況について

2019年６月

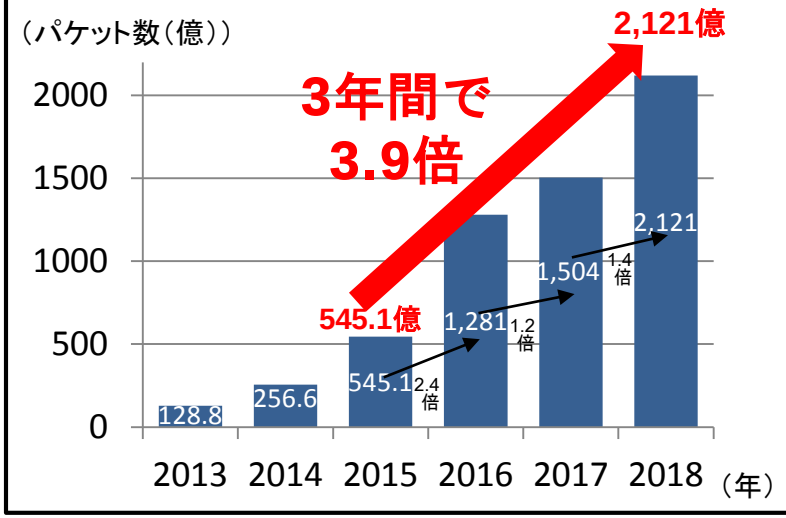
IoT機器を狙ったサイバー攻撃の状況

- 国立研究開発法人情報通信研究機構（NICT）では、大規模サイバー攻撃観測網であるNICTERにおいて、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測。

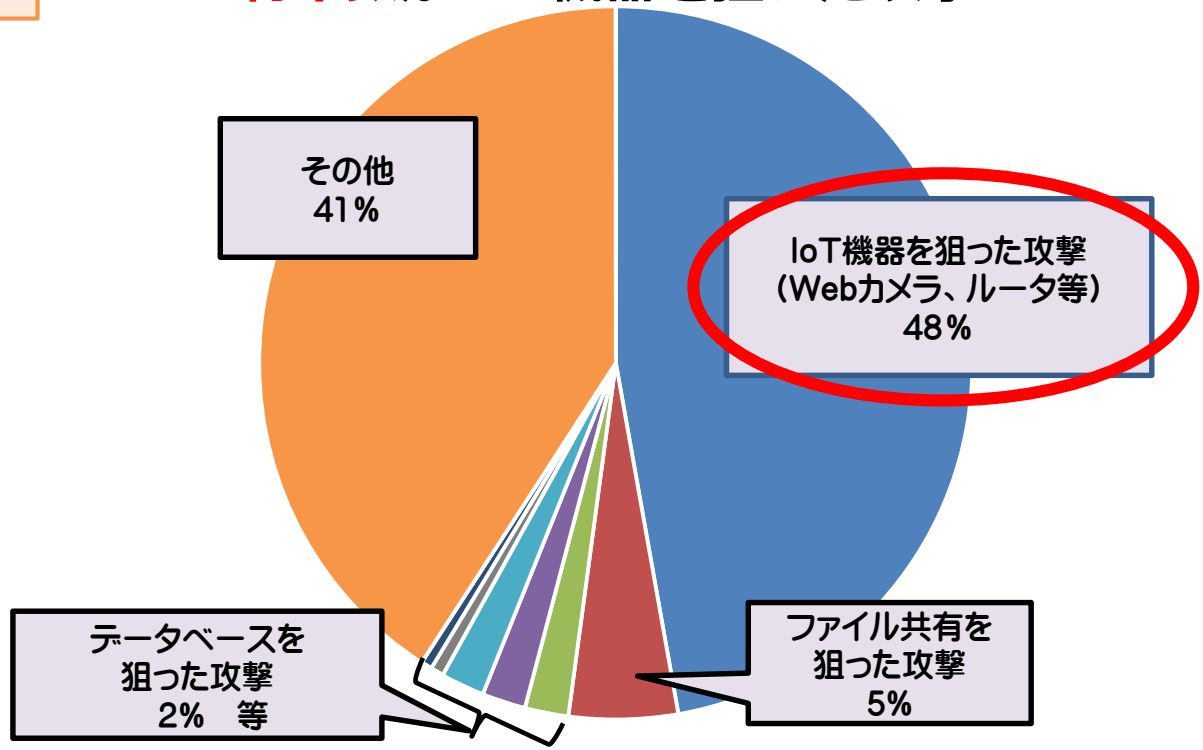
NICTERにより観測されるサイバー攻撃の様子



NICTERで１年間に観測されたサイバー攻撃関連通信数



約半数がIoT機器を狙った攻撃



（注１）　NICTERで観測されたパケットのうち、サービスの種類（ポート番号）ごとに割合の多い上位から30位までを分析したもの。

（注２）　IoT機器を狙った攻撃は多様化しており、ポート番号だけでは分類しにくいものなど、「その他」に含まれているものもある。

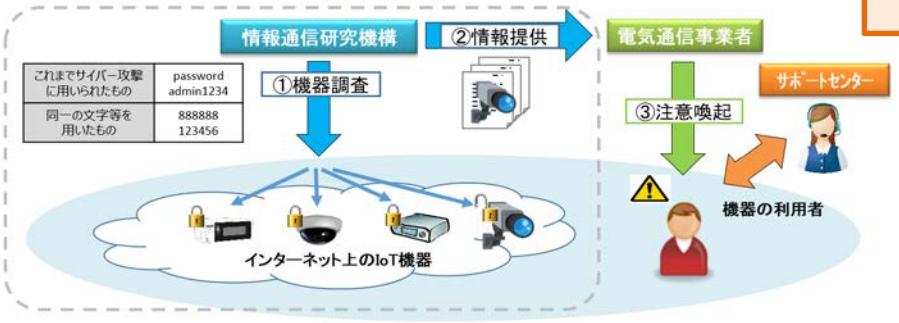
IoT機器調査及び利用者への注意喚起の取組

■ 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、インターネットプロバイダ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、インターネットプロバイダから利用者へ注意喚起を行う取組を2019年６月より実施。

※ 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。

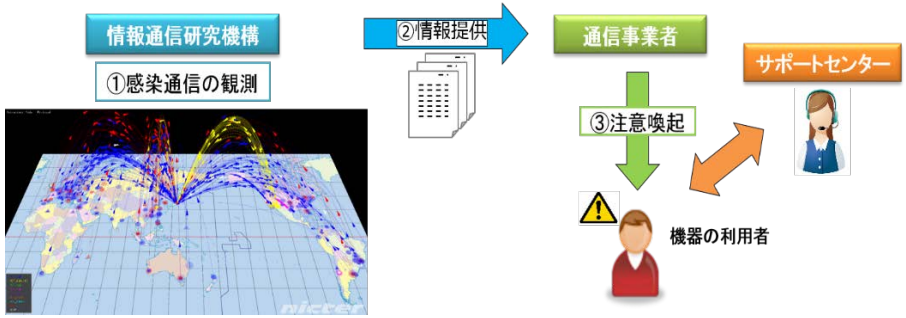
【NOTICEの概要】



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特定。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダ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。
② 当該機器の情報をインターネットプロバイダに通知。
③ インターネットプロバイダが当該機器の利用者を特定し、注意喚起を実施

※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

IoT機器調査及び利用者への注意喚起の実施状況

● 日本国内の約2億のIPアドレスのうち、これまでに調査に係る手続が完了しているインターネットプロバイダ33社に係る約9,000万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31,000～約42,000件	ISPに対する通知の対象となったもの	1日当たり112件～155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147件		

（参加インターネットプロバイダ：計33社）

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
NTT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
株式会社オプテージ
KDDI株式会社
ソニーネットワークコミュニケーションズ株式会社
ソフトバンク株式会社
ニフティ株式会社
ビッグローブ株式会社
株式会社秋田ケーブルテレビ
イッツ・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
株式会社ケーブルテレビ品川
株式会社ケーブルネット鈴鹿
山陰ケーブルビジョン株式会社
株式会社シー・ティー・ワイ
株式会社ジュピターテレコム（グループ会社計10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