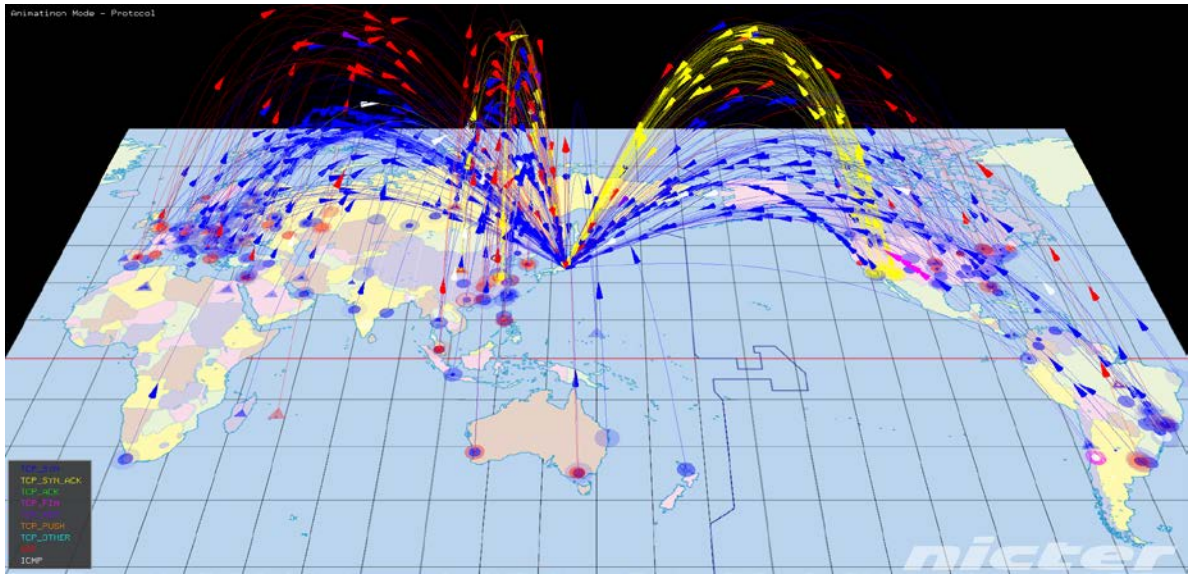
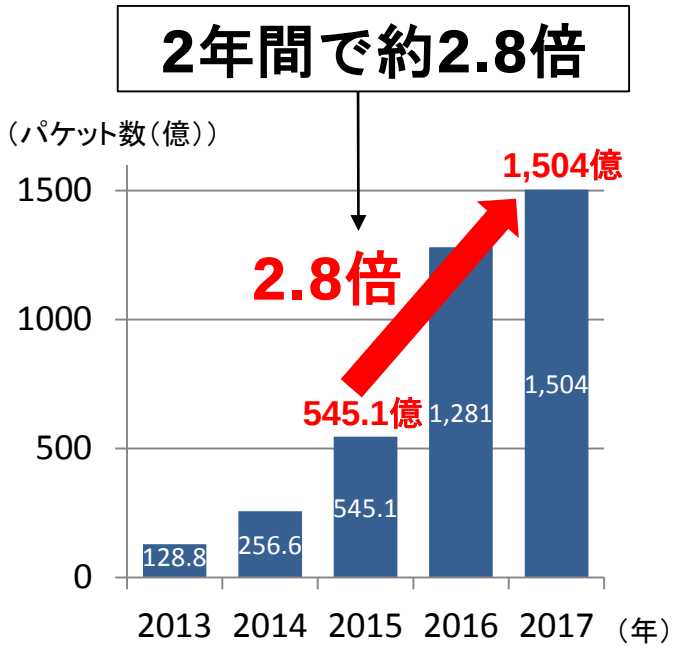

IoT機器調査及び
利用者への注意喚起
NOTICE
National Operation Towards IoT Clean Environment
ABOUT NOTICE
NOTICEについて

平成３１年２月１３日

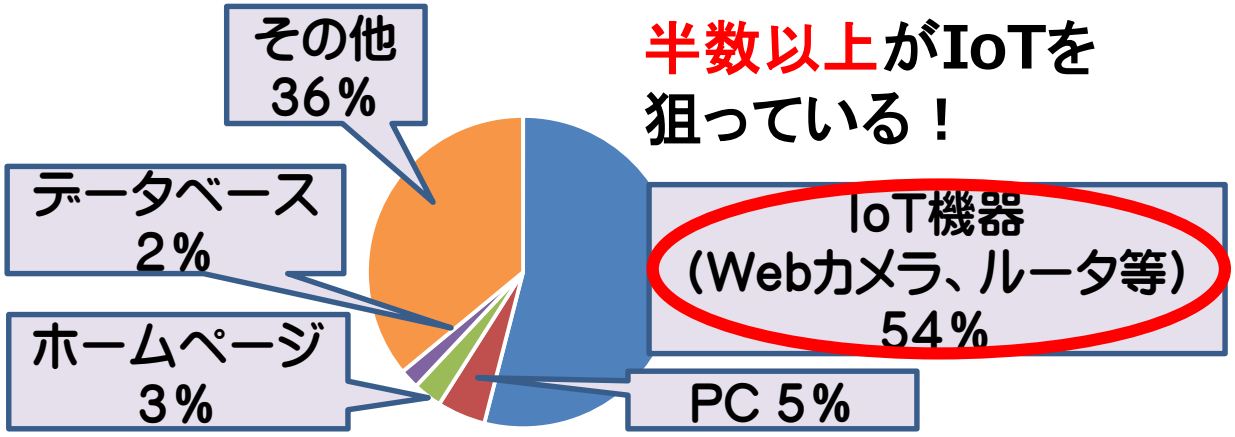
IoT機器に対するサイバー攻撃の増加



サイバー攻撃量の推移（ＮＩＣＴＥＲの観測）



サイバー攻撃の内訳（2017年）



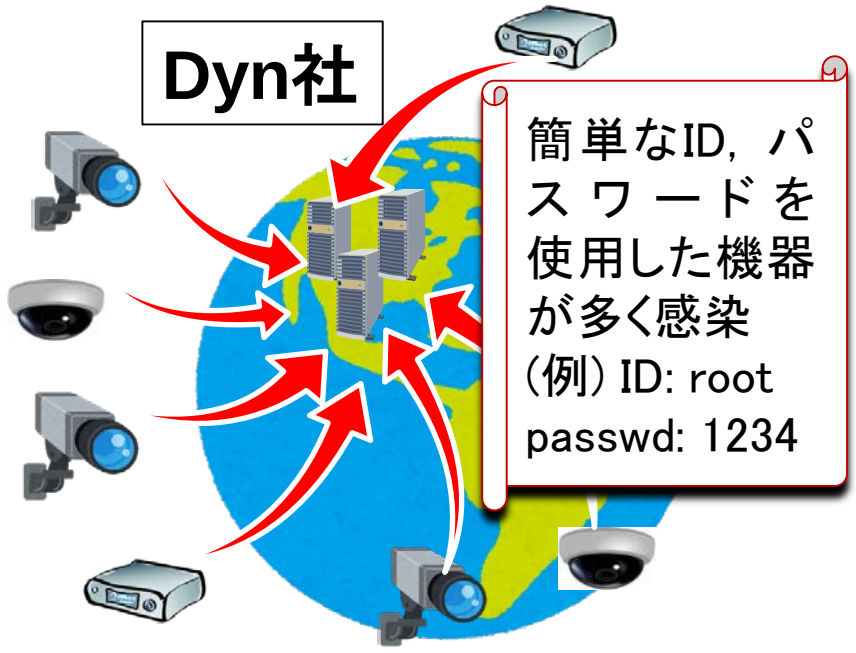
半数以上がIoTを狙っている！

IoT機器を狙った攻撃は約5.7倍

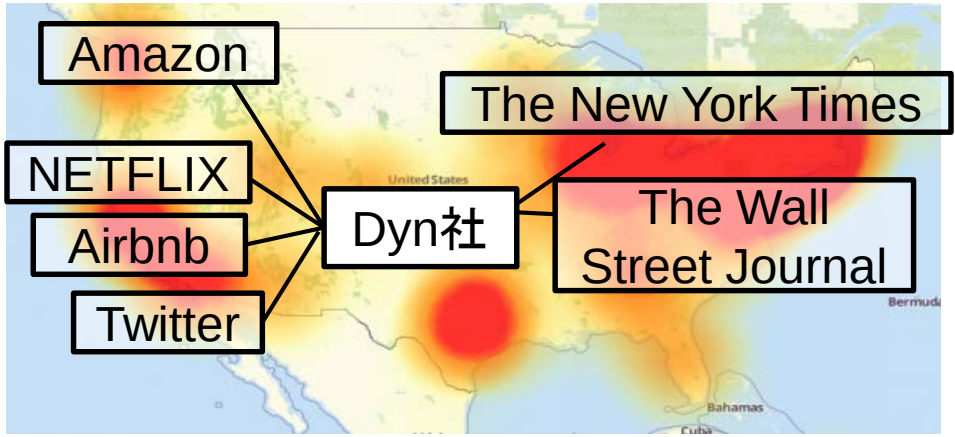
IoT機器を踏み台とした大規模DDoS攻撃

○ 2016年10月21日、米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。その結果、多数の企業のサービスにアクセスしにくくなる等の障害が発生。

○ 「Mirai」というマルウェアに感染した10万台を超えるIoT機器から、大量の通信（最大1.2Tbps）が発生したことが原因。



システムダウンの状況



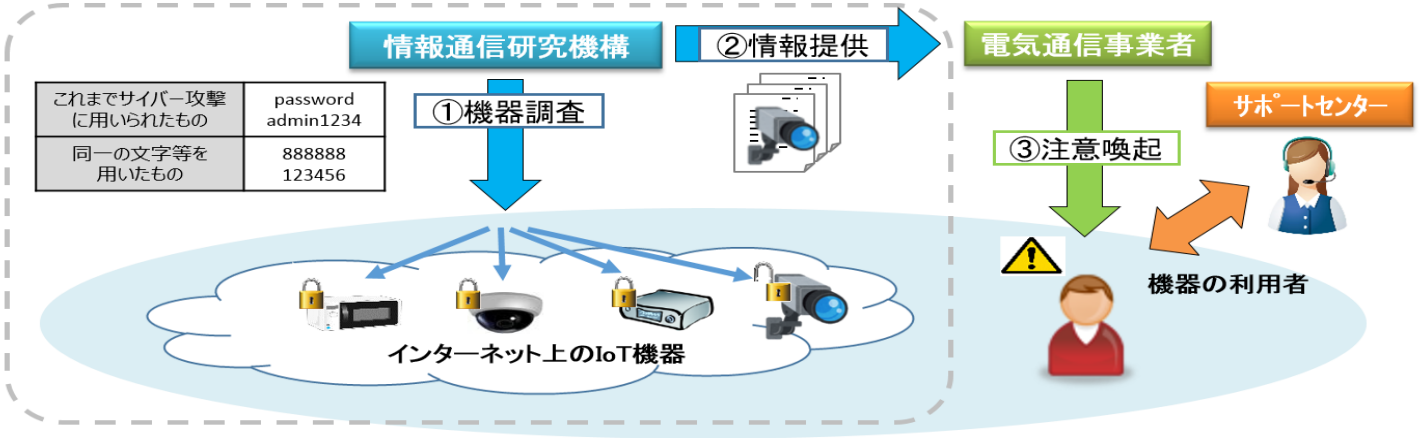
Dyn社のDNSサービスを使用した数多くの大手インターネットサービスやニュースサイトに影響。

IoT機器調査及び利用者への注意喚起

サイバー攻撃に悪用されるおそれのある機器を調査(※1)し、利用者への注意喚起を行う取組「NOTICE(※2)」を開始。

※1：サイバー攻撃に悪用されるおそれのあるIoT機器の調査等を実施するため、国立研究開発法人情報通信研究機構法を平成30年5月に改正。
※2：National Operation Towards IoT Clean Environment

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等により、サイバー攻撃に悪用されるおそれのある機器を特定。
② 当該機器の情報を電気通信事業者に通知。
③ 電気通信事業者が当該機器の利用者を特定し、注意喚起を実施。




おかしいだろ、
ソレ！
家のカギかけるよな？
サイフ置きっぱにしないよな？
IoTセキュリティだけテキトーって
2019年2月より、サイバー攻撃に悪用されるおそれのあるIoT機器の調査、注意喚起を行うプロジェクト「NOTICE」※1を実施します。
セキュリティ対策が必要なIoT機器のユーザには、ご契約のインターネットプロバイダからパスワード設定変更などの注意喚起を行います。お問い合せは、NOTICEサポートセンターまで。※2
※1：総務省、国立研究開発法人情報通信研究機構（NICT）、インターネットプロバイダが連携して実施するプロジェクトです。
※2：インターネットプロバイダからの注意喚起や、NOTICE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。
■お問い合せ NOTICEサポートセンター
さらに詳しい情報はWEBでも公開中 | https://notice.go.jp
TEL:0120-769-318（無料・固定電話のみ） 03-4346-3318（有料）
総務省 Ministry of Internal Affairs and Communications
NICT 国立研究開発法人 情報通信研究機構
NOTICE National Operation Towards IoT Clean Environment

FAQ

（1）調査の「対象となる機器」は？

グローバルIPアドレス（IPv4）によりインターネット上で外部からアクセスできるIoT機器、具体的には、ルータ、ウェブカメラ、センサーなどです。

（2）この調査は「不正アクセス行為」に該当しないのか？

NICTは実施計画に基づき、容易に推測されるID、パスワードを外部から入力し、サイバー攻撃に悪用されるおそれのあるIoT機器を特定します。この調査は、改正NICT法（※）において、不正アクセス禁止法で禁止されている不正アクセス行為から除外されています。

（※）附則第８条第７項に規定。

FAQ

（3）本調査は「通信の秘密」を侵害しないのか？

本調査は、容易に推測可能なパスワードを外部から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であるかを確認するものです。IoT機器と第三者との間の通信の内容等を知得、窃用又は漏えいするものではないため、通信の秘密を侵害することはありません。

（4）利用者はどのように特定されるのか？

インターネットプロバイダはNICTから受け取った情報（注意喚起の対象となるIoT機器のIPアドレス、タイムスタンプ等）を元に、対象機器の利用者を特定します。

ＦＡＱ

（５）「情報の保管や取扱」はどのようになされるのか？

NICTでは、政府で最も機密性の高い情報に求められる措置と同等の厳格な安全管理措置を講じています。入退室は多要素認証、サーバには進入検知システムやファイアウォール等により外部からの接続不可、情報へアクセスできる職員を限定するアクセス制御機能を導入し、そのログを監視するなどの措置を講じています。

（６）ルールに反した場合、「罰則」はあるのか？

情報の漏洩等はNICT法第１２条の秘密保持義務違反、実施計画に定める範囲を超えて特定アクセス行為を行った場合等は不正アクセス禁止法違反となり、いずれも罰則の対象となります。

ＦＡＱ

（7）利用者にはどのような方法で注意喚起が行われるのか？

ご契約のインターネットプロバイダから、電子メールなどによる注意喚起が行われます。

（8）本取組で得られた結果は公表するのか？

我が国のサイバーセキュリティ確保の観点にも留意しつつ、本取組の実施状況を取りまとめ、公表することを予定しています。

まとめ

○　パスワード設定が不適切なIoT機器を放置すれば、サイバー攻撃の踏み台となるおそれ。

○　関係機関が協力して、「NOTICEプロジェクト（調査及び注意喚起）」を２月２０日から実施。

○　幅広く周知広報を行うとともに、専用のWebページやサポートセンターを活用。消費者相談窓口とも連携し利用者の方々にきめ細かく対応。