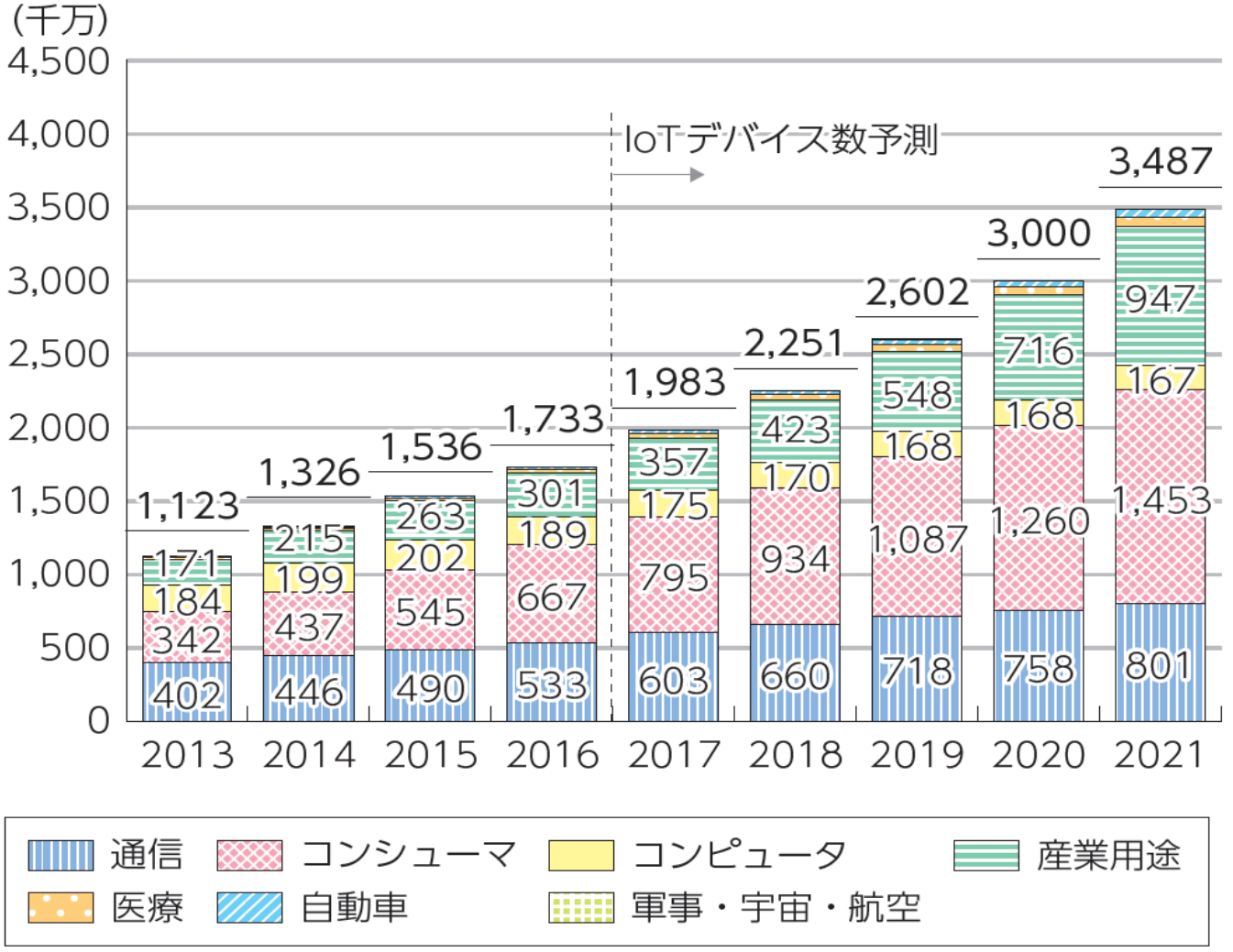
資料２

IoTセキュリティ総合対策について

平 成 ２ ９ 年 １ ２ 月
総　　務　　省
サイバーセキュリティ課

IoT機器の推移と普及分野

○ IHS Technology の推定によれば、2016年時点でインターネットにつながるモノ（IoTデバイス）の数は173億個であり、2021年までにその２倍の349億個まで増加するとされており、そのうち、約４割が消費者向けのものである。

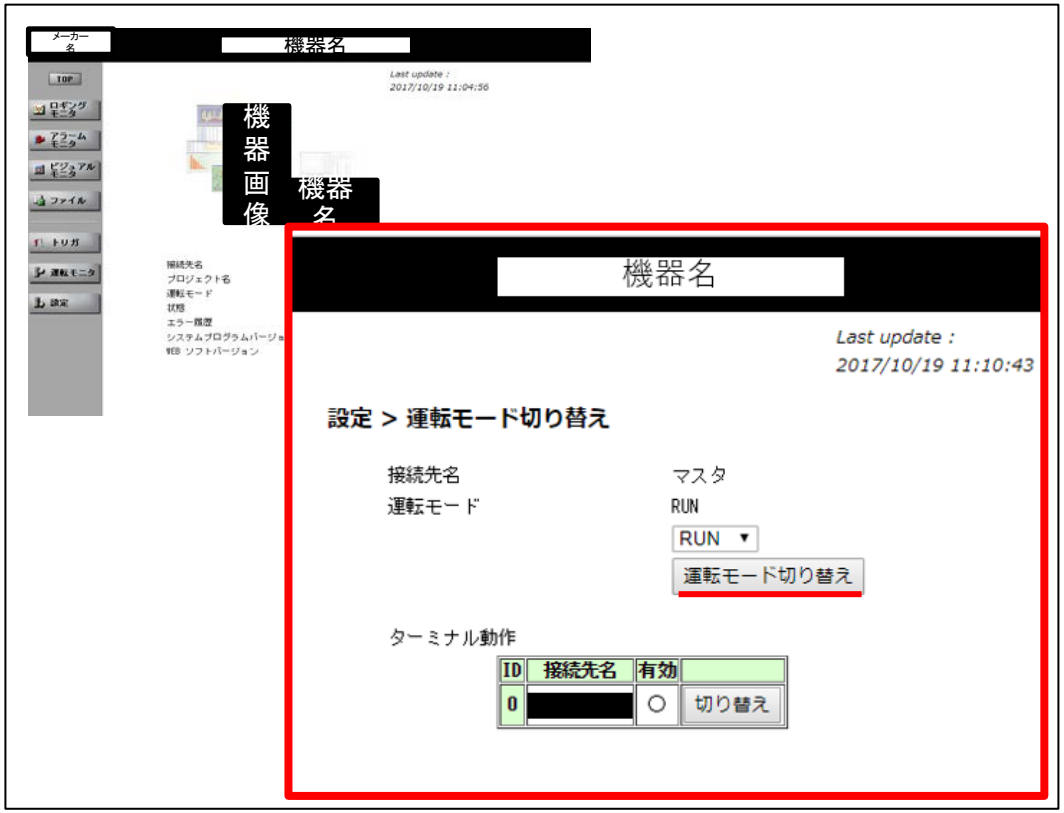


（出典）IHS Technology

IoT機器におけるサイバーセキュリティ上の脅威の具体例

水道関連設備

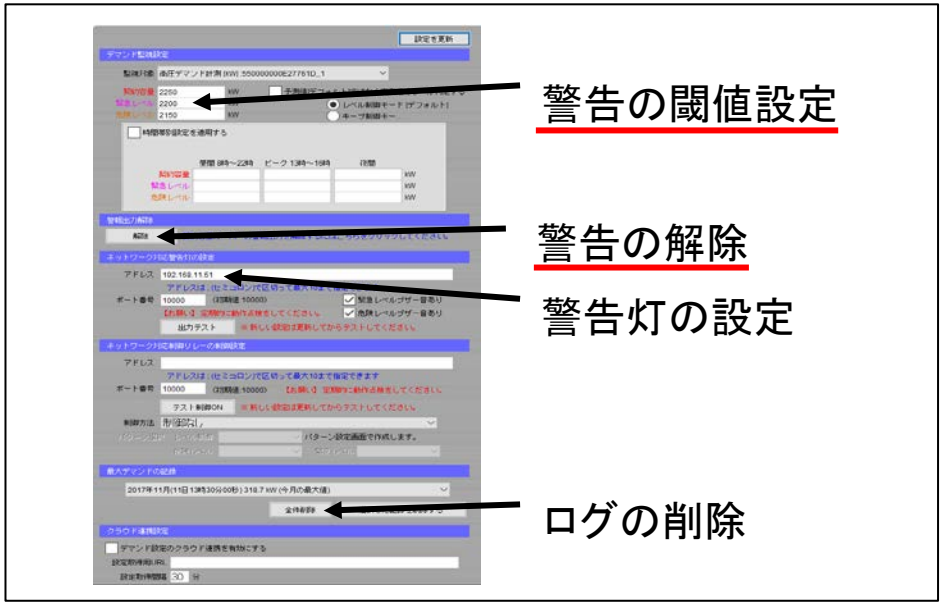
病院等に設置された水道関連設備のデータロガーがインターネット側からアクセス可能なまま運用されており、動作状況が外部から閲覧可能な状態であることに加え、第3者から運転モード(RUN/STOP)の切り替えが可能な状態になっていることが判明。



電力監視設備

工場等に設置された電力監視機器システムがインターネット側からアクセス可能なまま運用されており、警告の閾値の変更、警告の解除、プロキシ設定、再起動等の操作が、第3者が可能な状態になっていることが判明。

※イメージ



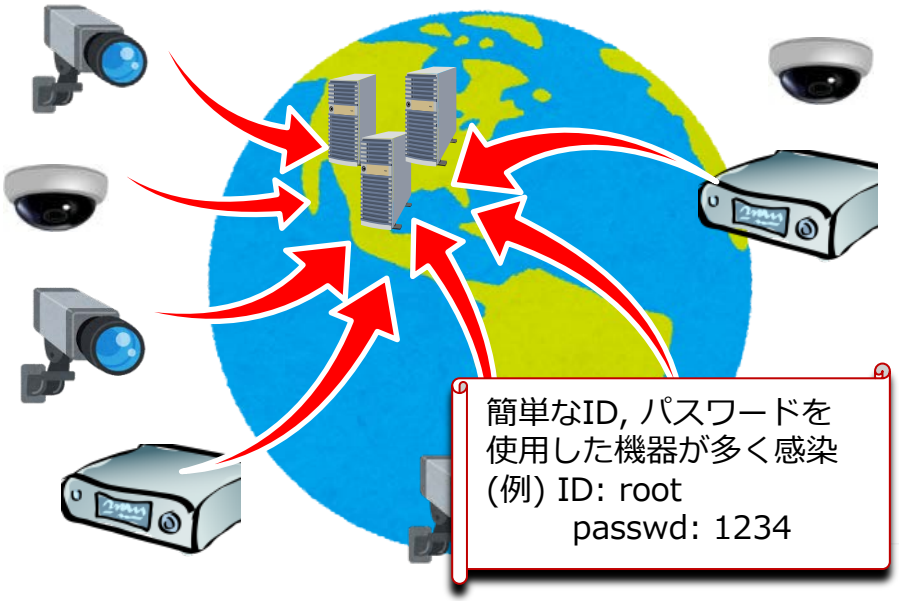
IoTにおけるサイバーセキュリティ上の脅威の具体例②

○　ユーザー側には、インターネットにつながっている意識がないことが多く、またウィルス駆除ソフトのインストールなどの対策が困難なため、システムが容易に乗っ取られる例や攻撃の踏台にされる例が急増している。

（出典）横浜国立大学吉岡准教授講演資料より抜粋

IoTにおけるサイバーセキュリティ上の脅威の具体例③

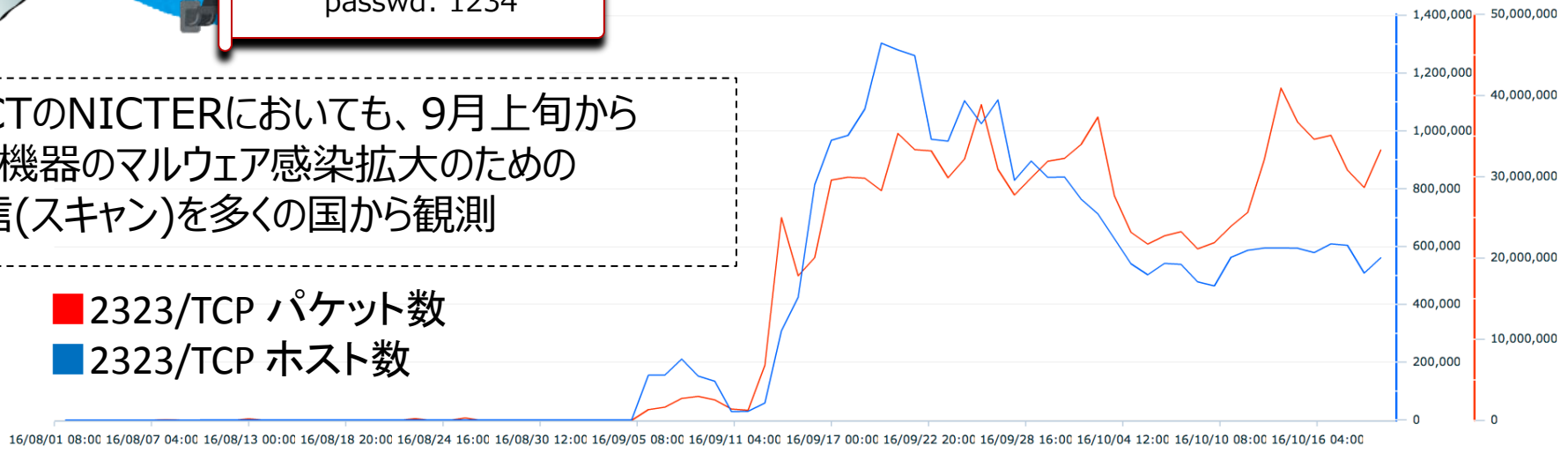
○ 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。
○ 同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。
サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。



- ✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生
- ✓ 最大で1.2Tbpsに達したとの報告もあり。
- ✓ 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

出典: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

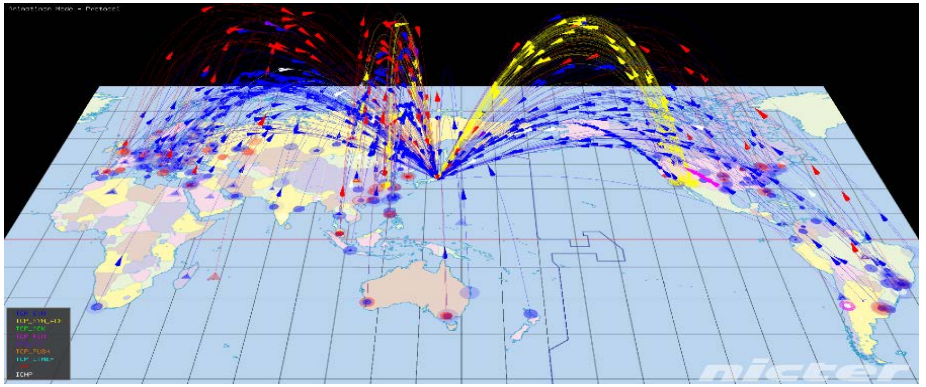
- ✓ NICTのNICTERにおいても、9月上旬からIoT機器のマルウェア感染拡大のための通信(スキャン)を多くの国から観測



IoT機器を狙った攻撃が急増（NICTERによる観測）

○　国立研究開発法人 情報通信研究機構（NICT）では、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による観測イメージ

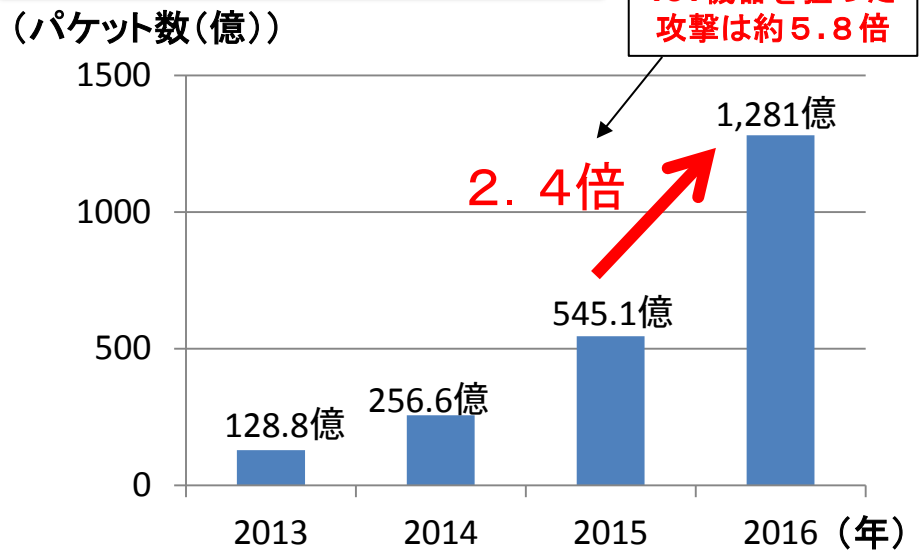


・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

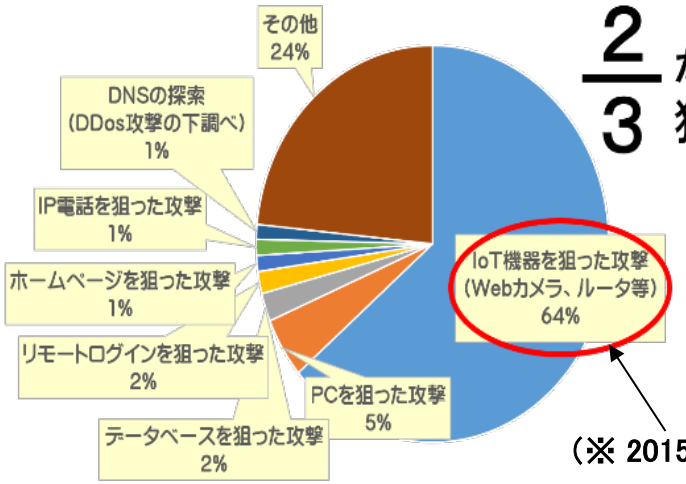
- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

1年間で観測されたサイバー攻撃回数

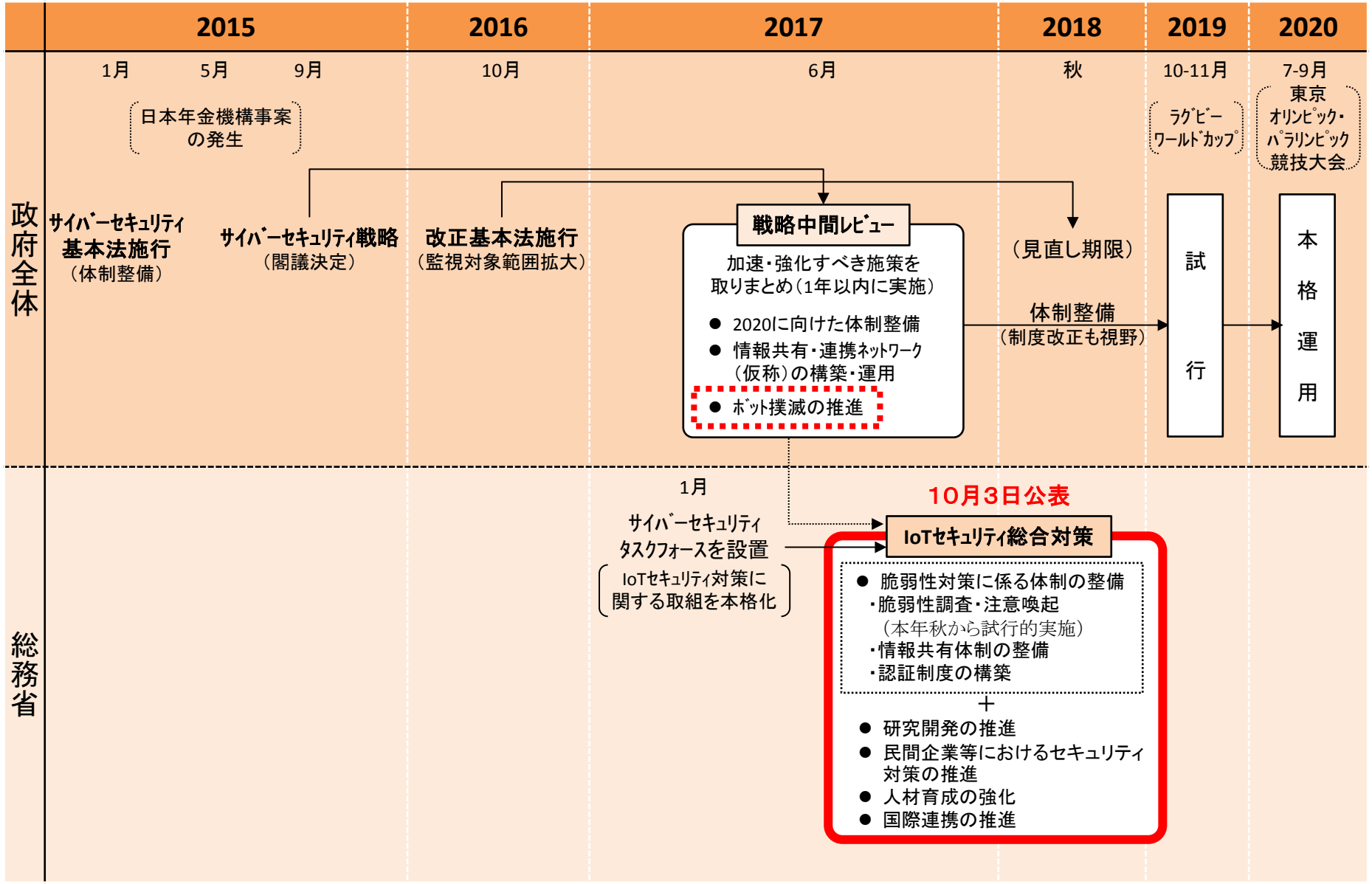


観測したサイバー攻撃の内訳（2016年）

観測された全サイバー攻撃1,281億パケットのうち、



サイバーセキュリティ対策関連スケジュール



IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

（ライフサイクル全体を見通した対策）

- セキュリティ・バイ・デザイン等の意識啓発・支援の実施
- 認証マークの付与及び比較サイト等を通じた推奨
- IoTセキュアゲートウェイ
- セキュリティ検査の仕組み作り
- 簡易な脆弱性チェックソフトの開発等
- 利用者に対する意識啓発の実施や相談窓口等の設置

（脆弱性調査の実施）

- 重要なIoT機器に係る脆弱性調査
- サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査
- 被害拡大を防止するための取組の推進
- IoT機器に関する脆弱性対策に関する実施体制の整備

研究開発の推進

- 基礎的・基盤的な研究開発等の推進
- 広域ネットワークスキャンの軽量化
- ハードウェア脆弱性への対応
- スマートシティのセキュリティ対策の強化
- 衛星通信におけるセキュリティ技術の研究開発
- AIを活用したサイバー攻撃検知・解析技術の研究開発

民間企業等におけるセキュリティ対策の促進

- 民間企業のセキュリティ投資等の促進
- セキュリティ対策に係る情報開示の促進
- 事業者間での情報共有を促進するための仕組みの構築
- 情報共有時の匿名化処理に関する検討
- 公衆無線LANのサイバーセキュリティ確保に関する検討

人材育成の強化

- 実践的サイバー防御演習（CYDER）の充実
- 2020年東京大会に向けたサイバー演習の実施
- 若手セキュリティ人材の育成の促進
- IoTセキュリティ人材の育成の促進

国際連携の推進

- ASEAN各国との連携
- 国際的なISAC間連携
- 国際標準化の推進
- サイバー空間における国際ルールを巡る議論への積極的参画

脆弱性対策に係る体制の整備（ライフサイクル全体を見通した対策）

脆弱性対策に係る体制の整備（ライフサイクル全体を見通した対策）

設計・製造段階

■ **セキュリティ・バイ・デザイン等の意識啓発・支援の実施**

セキュリティ・バイ・デザインの考え方を踏まえ設計された機器に認証マークを付与し、当該認証マークの付された機器の使用を推奨すること等について検討を行い、意識啓発・支援を実施。

販売段階

■ **認証マークの付与及び比較サイト等を通じた推奨**

一定のセキュリティ要件を満たしているIoT機器に対する認証マークの付与や、比較サイト等を通じた利用者が容易に認証取得の有無等を確認できる仕組みの構築について検討。

設置段階

■ **IoTセキュアゲートウェイ**

IoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組について実証を進めるとともに、セキュリティ評価や実際の導入を進める仕組みの検討。

運用・保守段階

■ **セキュリティ検査の仕組み作り**

継続的な安全性を確保するためのセキュリティ検査の仕組み作り（機器の脆弱性に係る接続試験を行うテストベッドの構築を含む）と、対策が不十分なIoT機器への対応の検討。

■ **簡易な脆弱性チェックソフトの開発等**

IoT機器の利用者が簡易にその脆弱性をチェックできるソフトを開発して配布する取組や、脆弱性を調査する民間サービスの実施を促進する取組の検討。

利用段階

■ **利用者に対する意識啓発の実施や相談窓口等の設置**

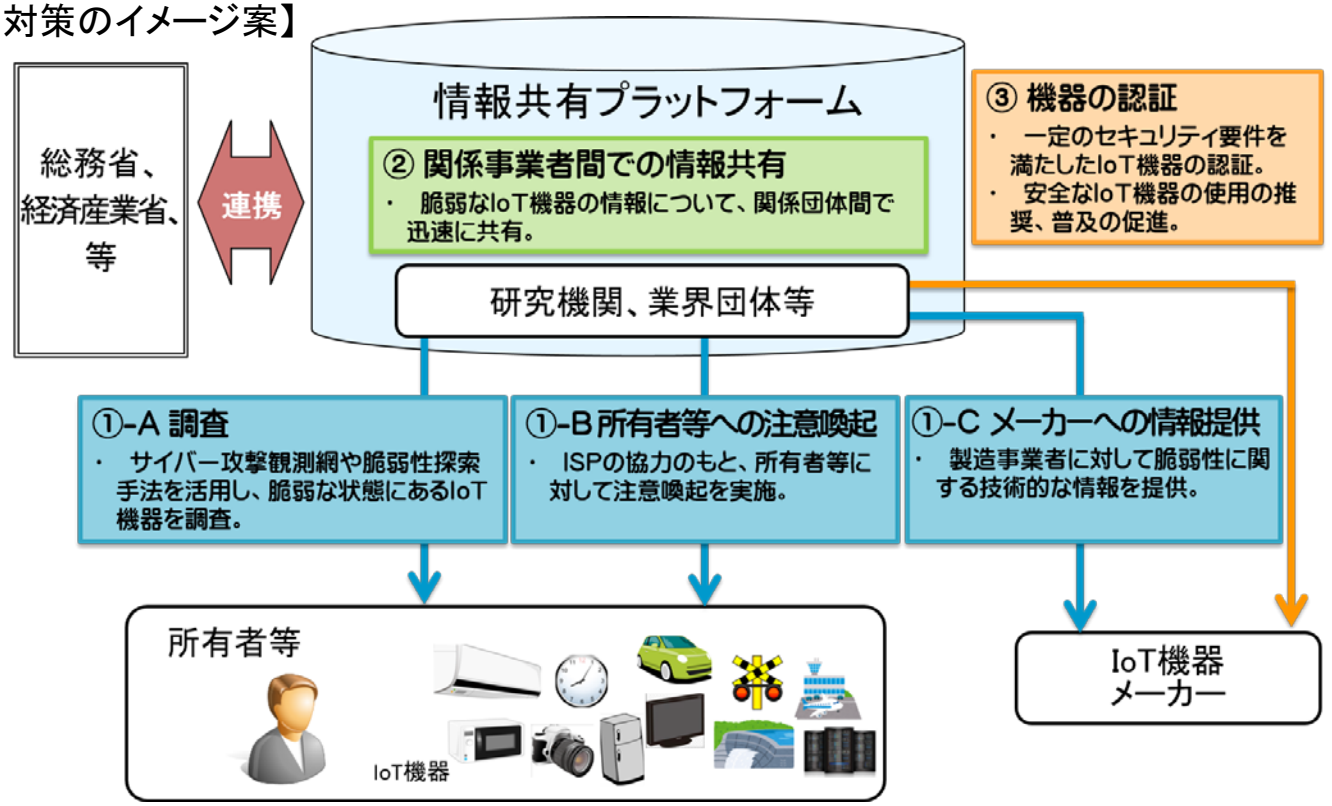
ID/パスワード設定、ファームウェアのアップデート、Wi-Fi設定の3点を中心とした利用者への意識啓発の実施、利用者からの相談窓口や、脆弱性が見つかった場合の関係機関との調整窓口の設置。

脆弱性対策に係る体制の整備（脆弱性調査の実施）

脆弱性対策に係る体制の整備（脆弱性調査の実施）

■ **重要IoT機器に係る脆弱性調査**
■ **サイバー攻撃の踏み台となるおそれがある機器に係る脆弱性調査**

【対策のイメージ案】



○脆弱なIoT機器の実態調査、所有者等への注意喚起

・IoT機器の調査を実施し、脆弱性を持つIoT機器が発見された場合は、インターネットサービスプロバイダ(ISP)等の協力のもと、当該機器の所有者・運用者・利用者へ注意喚起を実施。

○IoT機器の脆弱性情報の関係事業者間での共有

・IoT機器の製造事業者等が脆弱性に迅速に対応することを可能とするため、IoT機器の脆弱性情報を関係事業者間で共有する仕組みを構築。

■ **被害拡大を防止するための取組の推進**

・ 脆弱性を有するIoT機器が踏み台となったことが確認された場合、ISPによるC&Cサーバとの通信制御の実施を推進するとともに、当該取組を促進するための方策について検討（年度内を目途に方向性）。

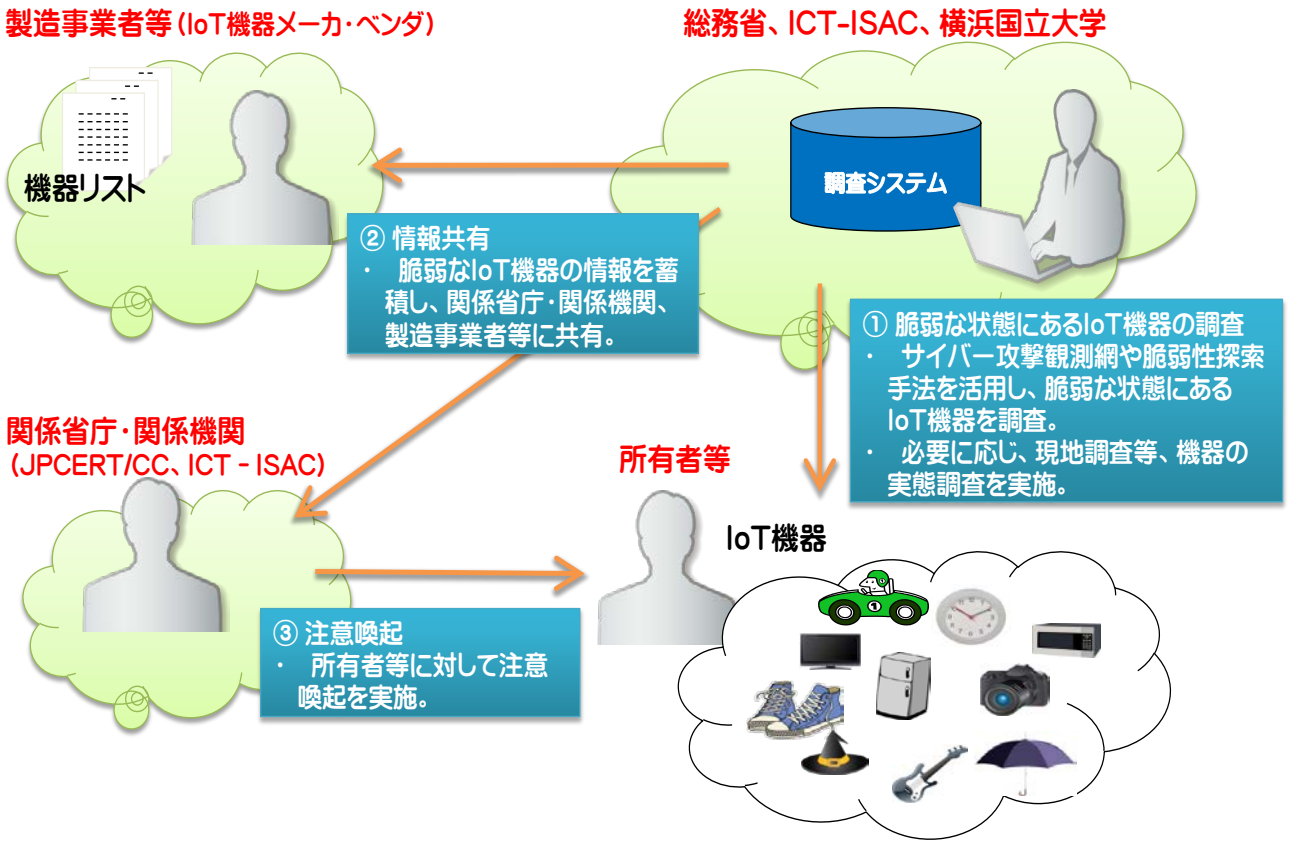
■ **IoT機器に関する脆弱性対策に関する実施体制の整備**

・ IoT機器に対する脆弱性対策を実施する体制（IoTセキュリティ対策センター（仮称））のあり方について検討（年度内を目途に結論）。

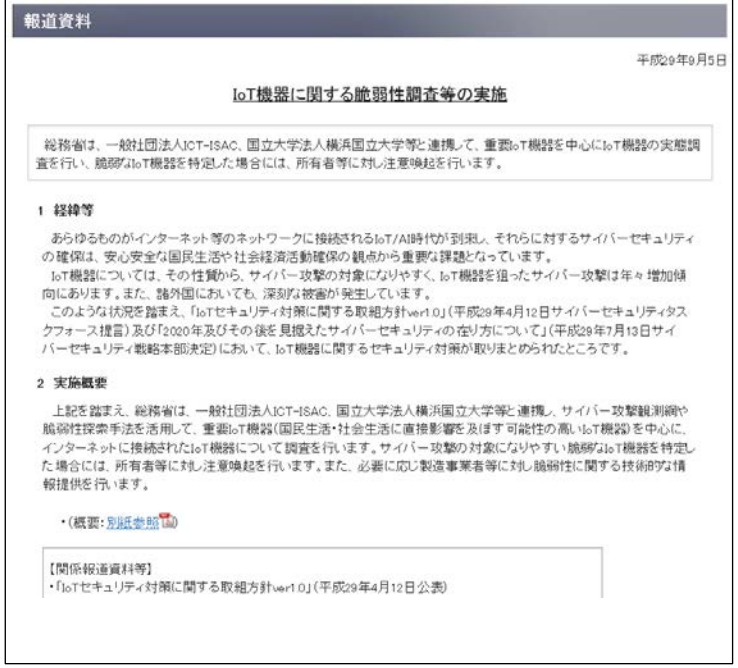
IoT機器に関する脆弱性調査等（平成29年9月5日　報道発表）

○　サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を実施。

○　サイバー攻撃の対象になりやすい脆弱なIoT機器を特定した場合には、所有者等に対して注意喚起を実施。また、必要に応じて製造事業者等に対して脆弱性に関する技術的な情報提供を実施。



【報道発表（平成29年9月5日）】



報道資料

平成29年9月5日

IoT機器に関する脆弱性調査等の実施

総務省は、一般社団法人ICT-ISAC、国立大学法人横浜国立大学等と連携して、重要IoT機器を中心にIoT機器の実態調査を行い、脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。

1　経緯等

あらゆるものがインターネット等のネットワークに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や社会経済活動確保の観点から重要な課題となっています。

IoT機器については、その性質から、サイバー攻撃の対象になりやすく、IoT機器を狙ったサイバー攻撃は年々増加傾向にあります。また、諸外国においても、深刻な被害が発生しています。

このような状況を踏まえ、「IoTセキュリティ対策に関する取組方針ver1.0」（平成29年4月12日サイバーセキュリティタスクフォース提言）及び「2020年及びその後を見据えたサイバーセキュリティの在り方について」（平成28年7月13日サイバーセキュリティ戦略本部決定）において、IoT機器に関するセキュリティ対策が取りまとめられたところです。

2　実施概要

上記を踏まえ、総務省は、一般社団法人ICT-ISAC、国立大学法人横浜国立大学等と連携し、サイバー攻撃観測網や脆弱性探索手法を活用して、重要IoT機器（国民生活・社会生活に直接影響を及ぼす可能性の高いIoT機器）を中心に、インターネットに接続されたIoT機器について調査を行います。サイバー攻撃の対象になりやすい脆弱なIoT機器を特定した場合には、所有者等に対し注意喚起を行います。また、必要に応じ製造事業者等に対し脆弱性に関する技術的な情報提供を行います。

・（概要：別紙参照）

【関係報道資料等】
・「IoTセキュリティ対策に関する取組方針ver1.0」（平成29年4月12日公表）