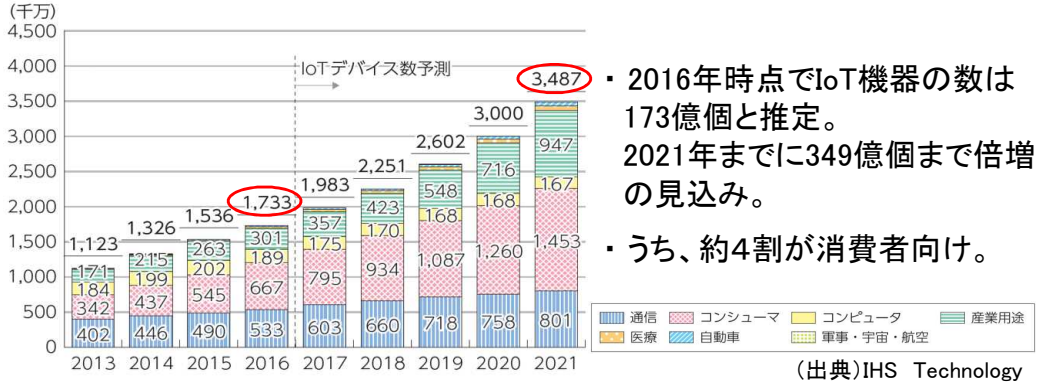
IoTセキュリティ総合対策（2017年10月） 参考1

現状

○IoT機器の幾何級数的な増加

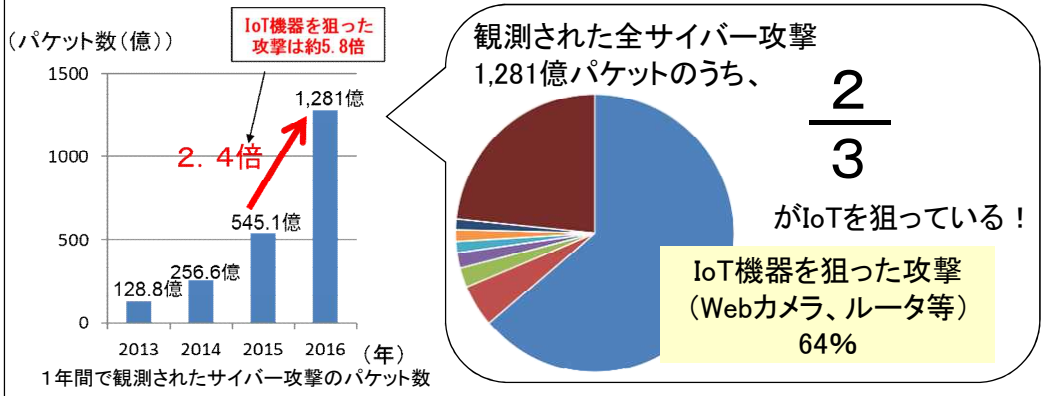


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

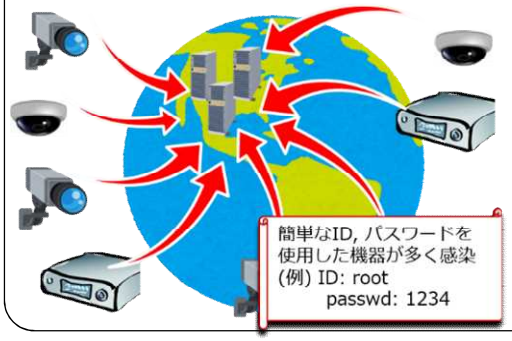
・うち、約4割が消費者向け。

（出典）IHS Technology

○IoT機器を狙った攻撃が急増



○IoT機器を踏み台にした大規模攻撃が発生



・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。

対策

IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

・IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。

・脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

・セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等におけるセキュリティ対策の促進

・民間企業等のサイバーセキュリティに係る投資を促進。

・サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

・圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

・二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証
（関係府省と連携）

2020東京大会に向けた実践的サイバー演習（サイバーコロッセオ）

○　近年さらに高度化・多様化するサイバー攻撃に備え、東京2020オリンピック・パラリンピック競技大会の適切な運営を確保することを目的として、**大会関連組織のセキュリティ担当者等を対象とした、**高度な攻撃に対処可能な人材の育成を行う**実践的サイバー演習「サイバーコロッセオ」を平成30年２月から本格的に実施**。

○　サイバーコロッセオは、**国立研究開発法人情報通信研究機構（NICT）が実施主体となり**（※）、NICTが有する大規模演習環境及び長年のサイバーセキュリティ研究による知見を活かした、**実際の機器やソフトウエアの操作を伴う「実践的なトレーニング」を実施**。

（※）平成29年４月、NICTに実践的サイバー演習を行う「ナショナルサイバートレーニングセンター」が組織されている。

イメージ図

■　大規模演習環境を用いて、東京大会の公式サイト、大会運営システム等ネットワーク環境を忠実に再現した、仮想のネットワーク環境を構築。

■　仮想のネットワーク環境上で、東京大会時に想定されるサイバー攻撃を擬似的に発生させ、攻撃・防御手法の検証及び訓練を実施。

東京2020オリンピック・パラリンピック競技大会のサイバーセキュリティを確保