資料3

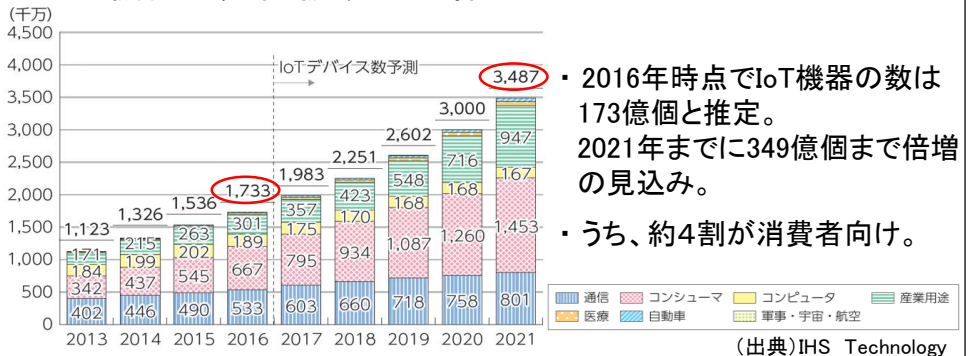
実践的サイバー防御演習（CYDER）について

平成２９年１２月２０日
総　　務　　省
情 報 流 通 行 政 局
サイバーセキュリティ課

IoTセキュリティ総合対策（2017年10月）

現状

○IoT機器の幾何級数的な増加

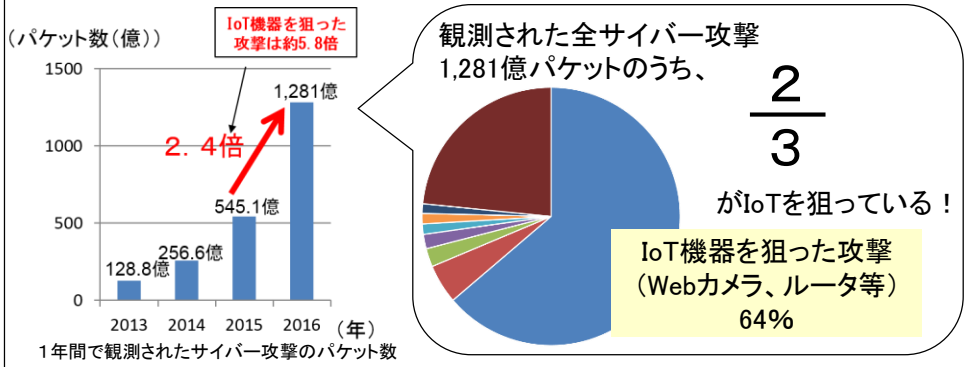


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

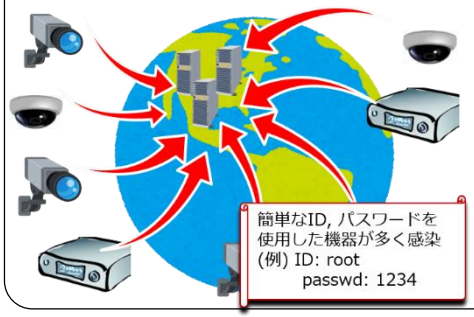
・うち、約4割が消費者向け。

（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）

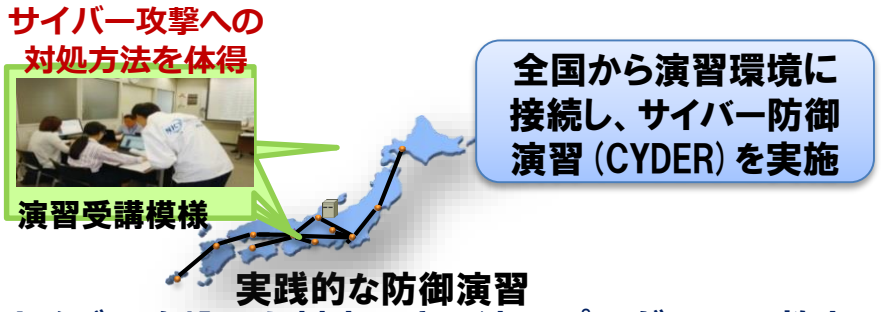
セキュリティ人材の育成（ナショナルサイバートレーニングセンター）

○　巧妙化・複合化するサイバー攻撃に対し、実践的な対処能力を持つセキュリティ人材を育成するため、平成29年4月に国立研究開発法人情報通信研究機構（NICT）に組織した「ナショナルサイバートレーニングセンター」において、下記取組を実施。

① 国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等に対するサイバー攻撃について、実践的な防御演習を実施 （CYDER）

② 2020年東京オリンピック・パラリンピック競技大会の適切な運営に向けたセキュリティ人材の育成（サイバーコロッセオ）

③ 若手セキュリティエンジニアの育成 （SecHack365）



新たな手法のサイバー攻撃にも対応できる演習プログラム・教育コンテンツを開発

東京大会に向けた人材育成

若手セキュリティエンジニアの育成

実践的サイバー防御演習(CYDER)の概要

CYDER: CYber Defense Exercise with Recurrence

○ サイバー攻撃が発生した場合の被害を最小化するための一連の対処方法(攻撃を受けた端末の特定・隔離、通信記録の解析による侵入経路や被害範囲の特定、同種攻撃の防御策、上司への報告等)を体得。

○ 150台の高性能サーバを用いた数千人規模の仮想ネットワーク環境(国の行政機関や大企業を想定)上で演習を実施。

○ 我が国固有のサイバー攻撃事例を徹底分析し、最新の演習シナリオを用意。

演習のイメージ

平成29年度の実施内容

演習規模を拡大し、全国47都道府県において約3000人を目標に実施中(全100回実施予定)

Aコース　59回　(地方公共団体向け(初心者向け))

B-1コース　21回　(地方公共団体向け)

B-2コース　20回

(国の行政機関、独立行政法人、指定法人、重要インフラ事業者向け)

対象となる重要インフラ事業者

情報通信	金融	航空	鉄道	電力	ガス
医療	水道	物流	化学	クレジット	石油