資料2

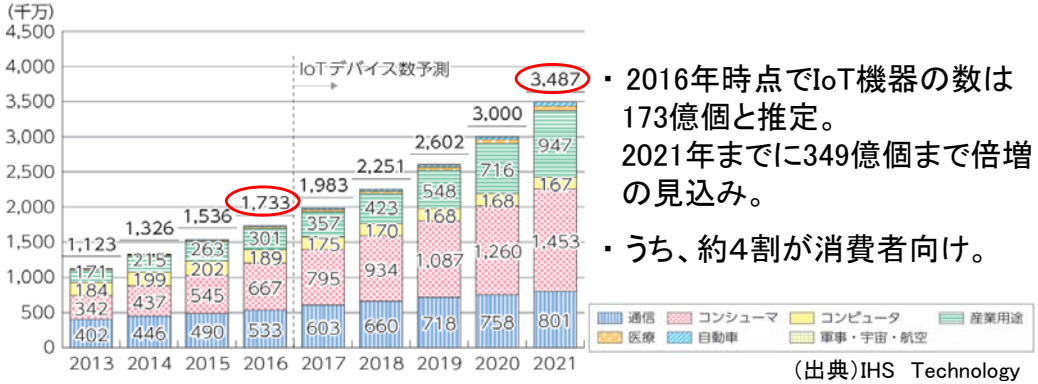
IoTセキュリティに関する取組状況

平成３０年６月１４日
総　　務　　省
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

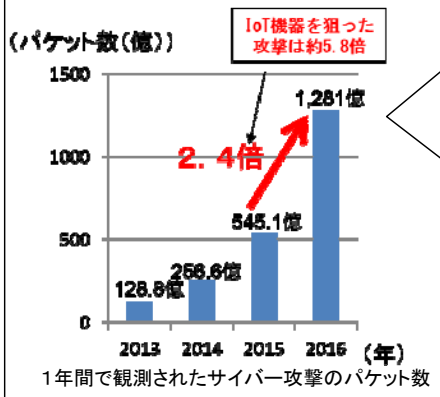


・2016年時点でIoT機器の数は173億個と推定。
2021年までに349億個まで倍増の見込み。

・うち、約4割が消費者向け。

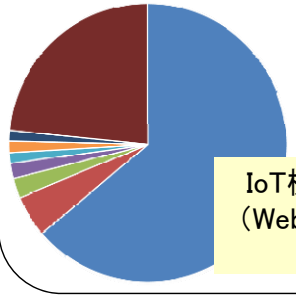
（出典）IHS　Technology

○IoT機器を狙った攻撃が急増



1年間で観測されたサイバー攻撃のパケット数

観測された全サイバー攻撃
1,281億パケットのうち、

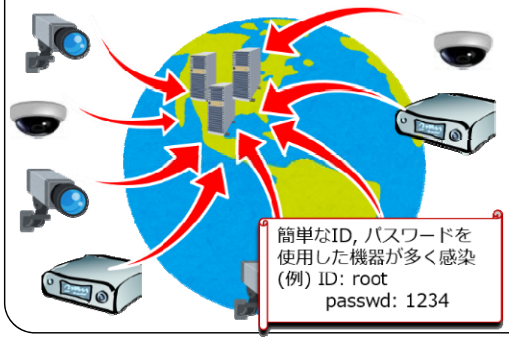


$\frac{2}{3}$

がIoTを狙っている！

IoT機器を狙った攻撃
（Webカメラ、ルータ等）
64%

○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）

セキュリティ対策に係る制度整備

- 国立研究開発法人情報通信研究機構法の一部改正
- 電気通信事業法の一部改正
- IoT機器を含む端末設備のセキュリティ対策に係る検討

国立研究開発法人情報通信研究機構法の一部改正について

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行うもの。

サイバー脅威の深刻化

•IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

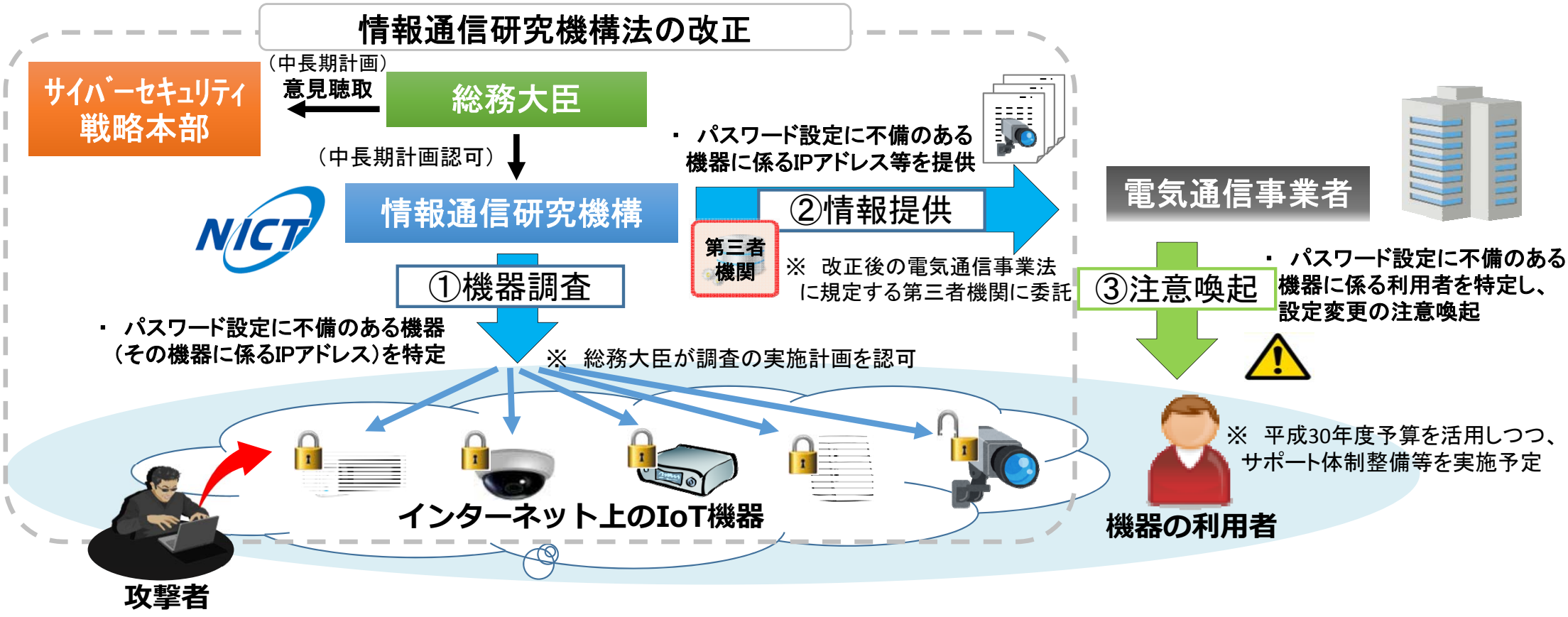
※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性

•パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

•NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。



電気通信事業法の一部改正について

- サイバー攻撃を行う**マルウェア**※**感染機器**やそれらに**指令を出すサーバへの対処を促進**するため、**第三者機関**を中心として**通信事業者が必要な情報共有をする**ための制度を整備。

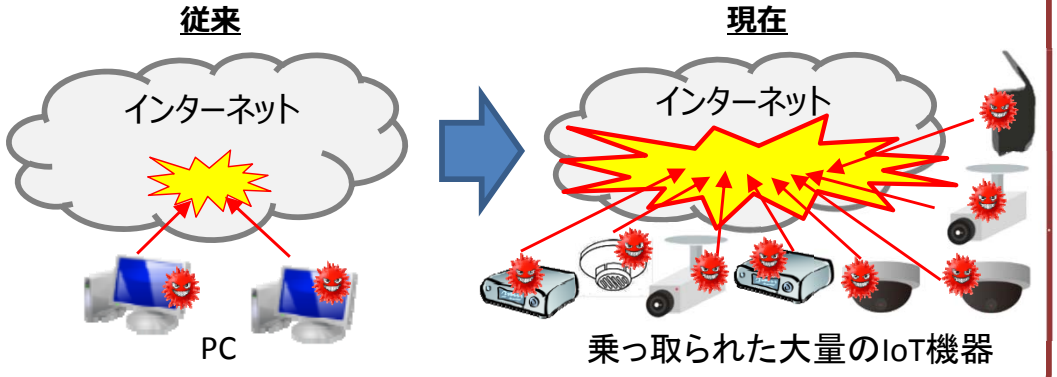
※悪意あるソフトウェアの総称であり、コンピュータに感染することによって、サイバー攻撃などの遠隔操作を自動的に実行するプログラムのこと。

現　状

インターネットの障害の深刻化

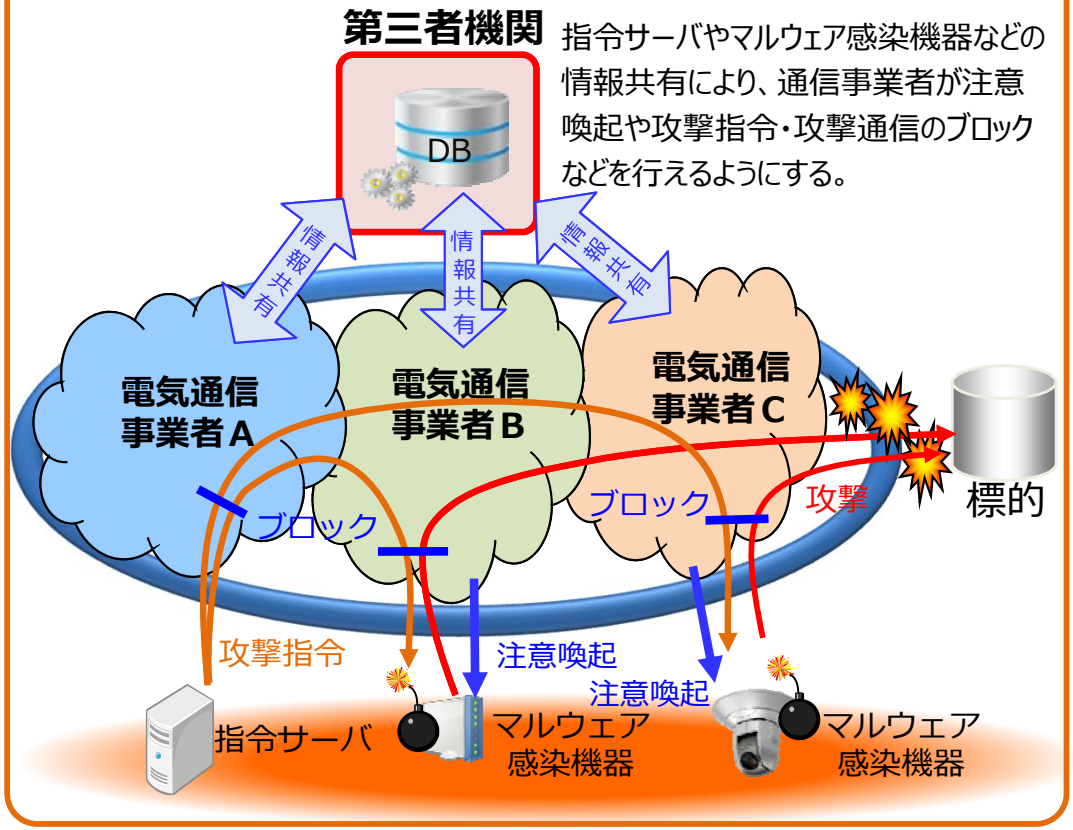
- サイバー攻撃によるインターネットの障害が発生し、国民生活や社会経済活動に影響
- 増加するIoT機器※を悪用したサイバー攻撃によりインターネットに重大な障害が発生
- 2020年の東京オリンピック・パラリンピック競技大会に際して、日本に対する大規模なサイバー攻撃の発生の懸念

※インターネットに接続される家庭用機器や業務用センサーなどの機器



制度整備（イメージ）

第三者機関を中心とした情報共有基盤の構築



IoT機器を含む端末設備のセキュリティ対策の検討（情報通信審議会）

■ 近年、Webカメラやルーター等のIoT機器が乗っ取られ、DDoS攻撃等のサイバー攻撃に悪用されて、インターネットに障害を及ぼすような事案が増加。このような中、情報通信ネットワークの安全・信頼性を確保するため、DDoS攻撃の原因となるIoT機器がマルウェアに大量感染する事態を防止すること等を目的として、IoT機器を含む端末設備の技術基準に最低限のセキュリティ対策を追加することについて、情報通信審議会において月内に報告(案)をまとめる方向で検討が行われている。

■ なお、IoTセキュリティを確保するためには、本対策だけではなく、本年5月に改正された電気通信事業法等に基づく、電気通信事業者の情報共有等の新たな取組みや、ガイドラインの活用や周知啓発など総合的な対策が必要。また、IoTのグローバル市場への展開や国際競争力確保といった観点から、今後もIoTセキュリティ対策に関する国際動向の把握に努める必要がある。

具体的な検討の内容（概要）

（１）端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

・インターネットプロトコルを使用する端末設備であって、電気通信回線を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについては、大量感染を防ぐための最低限のセキュリティ要件として、アクセス制御機能、アクセス制御の際に使用するID/パスワードの適切な設定を促す等の機能及びファームウェアの更新機能、又はそれらと同等以上の機能※が必要。

※ 同等以上の機能を持つものとしては、ISO/IEC15408に基づくセキュリティ認証(CC認証)を受けた複合機等が含まれる。

・ なお、PCやスマートフォン等については、アンチウィルスソフトを導入する等、利用者が容易に必要な対策を行うことが可能であるため、当該セキュリティ要件の規定の対象外とする。

（２）技術基準適合認定等の対象機器の範囲

・現在、技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しており、セキュリティ要件が追加された場合においても、ネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、技術基準適合認定等の対象は、従来と同様に電気通信回線設備に直接接続可能な端末機器とする。

・ただし、恒常的に既認定機器を介して接続する機器（例：大物白物家電等）を除く。

企業等におけるセキュリティ対策の促進

- 情報開示分科会報告書
- 公衆無線LANセキュリティ分科会報告書

情報開示分科会報告書概要（2018年6月）

○　民間企業における**セキュリティ対策の情報開示による「セキュリティ対策の見える化」を通じて、**民間企業の経営層が自社のセキュリティ対策の現状を認識し、また、他社の状況と比較することにより、さらに必要な具体的な　対策を検討し、導入する**「セキュリティ対策の好循環」が起こる環境の実現**が期待される。

○　情報を開示するにあたっては、開示の対象者によってその考え方、取組が異なることから、報告書（案）においては、**①社内の情報共有（第一者開示）**、**②契約者間等の情報開示（第二者開示）**、**③社会に対する情報開示（第三者開示）**の3つの側面に分けて整理している。

社内の情報共有（第一者開示）

…自社のセキュリティ対策について、セキュリティ対策の担当部署だけでなく、社内全体で共有すること。

・　経営層の理解を深め、気づきを与えるとともに、セキュリティ対策の担当部署の現場と経営層の間を繋ぐ、いわゆる「橋渡し人材」等の育成に向けた取組を進める必要がある。

（社内の情報共有に向けた橋渡し人材等の育成）

1. **人材のスキルの具体化**、スキル取得のための**教育コンテンツの開発・普及**、**スキル認定を行う仕組みを産学官により構築するための検討**。

【平成30年度中を目途に方向性を整理】

契約者間等の情報開示（第二者開示）

…契約の相手方等、対象を限定して自社のセキュリティ対策を開示すること。

・　契約者間等で確認すべき事項や必要な対策の整理、サプライチェーン全体またはグループ全体における情報共有体制の構築の促進が必要である。

・　サイバーセキュリティ保険について、対策の実施及び開示のインセンティブとなるような割引制度の普及や、グループ全体・サプライチェーン全体で一括して加入するような保険商品の展開が期待される。

（関係者間の情報共有促進のための仕組みづくりの検討）

2. **米国等におけるISAO(※)等の動向等について調査**するとともに、**公的支援のあり方について検討**。　【平成30年度中を目途に検討結果を取りまとめ】

(※)ISAO：Information Sharing and Analysis Organization

3. **セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進**し、標準仕様化に向けて検討。また、**企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討**。

【モデル事業については平成30年度に検討】

社会に対する情報開示（第三者開示）

…社会の幅広い対象に向けて、自社のセキュリティ対策を開示すること。

・　事業者の規模や取組状況に応じて、セキュリティ対策の自己宣言制度や主要5項目（※）の開示、「情報セキュリティ報告書」の作成など、段階的に対策を講じていくことが望ましい。

※　①基本方針等の策定状況　②管理体制　③教育・人材育成　④社外との情報共有体制　⑤第三者評価・認証

（第三者開示の促進に向けたガイドラインの策定）

4. **「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表**。

【平成30年秋を目途にガイドラインを策定】

5. 導入予定の「コネクティッド・インダストリー税制」の活用状況を分析するとともに、**企業のニーズ等を反映した投資促進のための政策支援のあり方について検討**。

【支援税制の運用にあわせて適宜実施】

公衆無線LANセキュリティ分科会報告書概要（2018年3月）

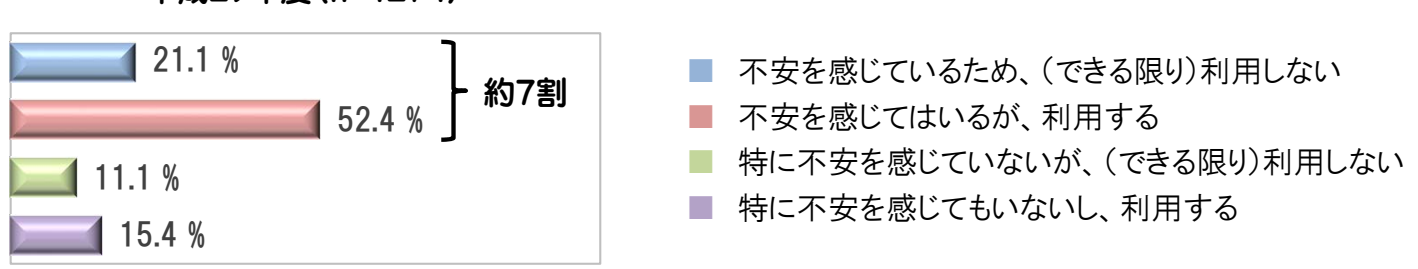
○ 公衆無線LANについては、観光や防災の観点から、その普及が進んでいるが、**公衆無線LANサービスの中には、セキュリティ対策が十分でないものも多い現状**にある。

○ こうした状況を踏まえ、**利便性と安全性のバランスに配慮**しつつ、必要なセキュリティ対策について基本的考え方を示すとともに、**セキュリティに配慮した公衆無線LAN環境の普及策**として、**①利用者・提供者の意識向上**、**②データ利活用施策との連携**、**③優良事例の普及**を図ること等を報告書として取りまとめ。

公衆無線LANの現状

○ 利用者の**約7割が公衆無線LANのセキュリティに不安**を感じており、また、十分なセキュリティ対策を実施していない状況。

利用者における公衆無線LANのセキュリティに関する意識



公衆無線LANのセキュリティ対策のあり方

① 利用者・提供者がどのような利用シーンにおいてどのようなセキュリティ対策を講ずればよいか、適正な対策方法について、周知・啓発 → **1. 利用者・提供者の意識向上**

② 一律に、特定の認証方式や暗号化方式を推奨するのではなく、提供者は多様な方式を提供するなどサービスの選択肢を増やし、利用者がそれらのサービスを適切に選択できる環境を整備 → **2. データ利活用施策との連携**

③ 自治体等におけるセキュアな公衆無線LANサービスの環境整備の取組に必要なガイドラインの策定や、優良事例となる公衆無線LANサービスの環境整備の実証等を推進 → **3. 優良事例の普及**

「セキュアな公衆無線LAN環境の実現に向けた行動計画」を策定し、推進。

セキュアな公衆無線LAN環境の実現に向けた行動計画

1. 利用者・提供者の意識向上

公衆無線LAN版
安全・安心マーク

（国における取組）

- Wi-Fi利用者・提供者向けマニュアル（手引き）の改定（2018年夏頃を目途）
- オンライン教育等の教育コンテンツを活用した周知・啓発（2018年秋頃を目途に開始）
- e-ネットキャラバン等の活動を通じた青少年・高齢者向けの周知・啓発（2018年度以降に実施）
- 「公衆無線LAN版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）

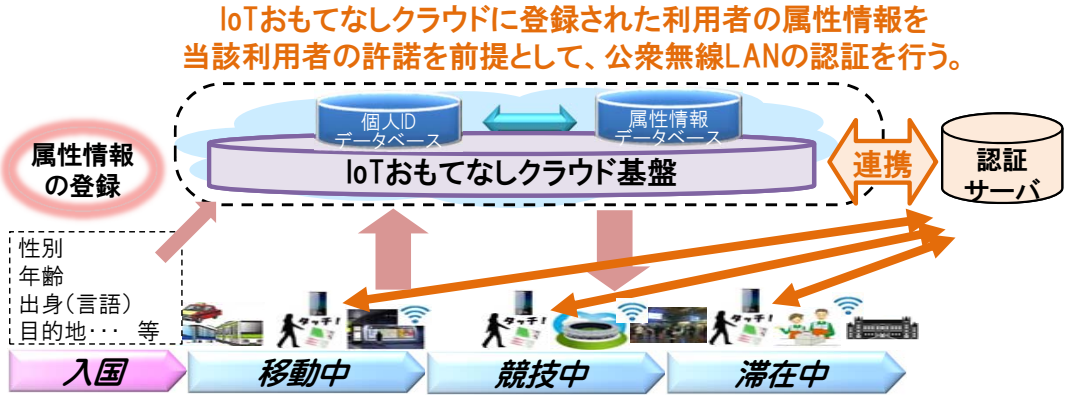
（民間事業者における取組）

- 暗号化の有無を識別可能な公衆無線LANサービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

2. データ利活用施策との連携

（国・民間事業者における取組）

- 公衆無線LANサービスとIoTおもてなしクラウドとの連携推進（2019年中を目途に実用化）



3. 優良事例の普及

（国・民間事業者等における取組）

- 自治体に対する公衆無線LAN環境整備支援事業の継続的推進（2019年度まで継続）及び優良事例の普及促進（優良事例の調査・公表及びこれを踏まえた所要の政策支援については、2018年夏以降に実施）
- デジタルスタジアムの実現に向けたセキュアな公衆無線LAN環境の整備及び公衆無線LANサービスのSSID等の情報や接続アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018年度以降に実施）