平成29年度あいち無料公衆無線LAN推進協議会
講演資料

総務省

公衆無線LANのセキュリティ対策について

２０１８年３月２７日

総務省　情報流通行政局
サイバーセキュリティ課
豊重　巨之

本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．サイバーセキュリティ政策の動向

３．公衆無線LANのセキュリティ対策

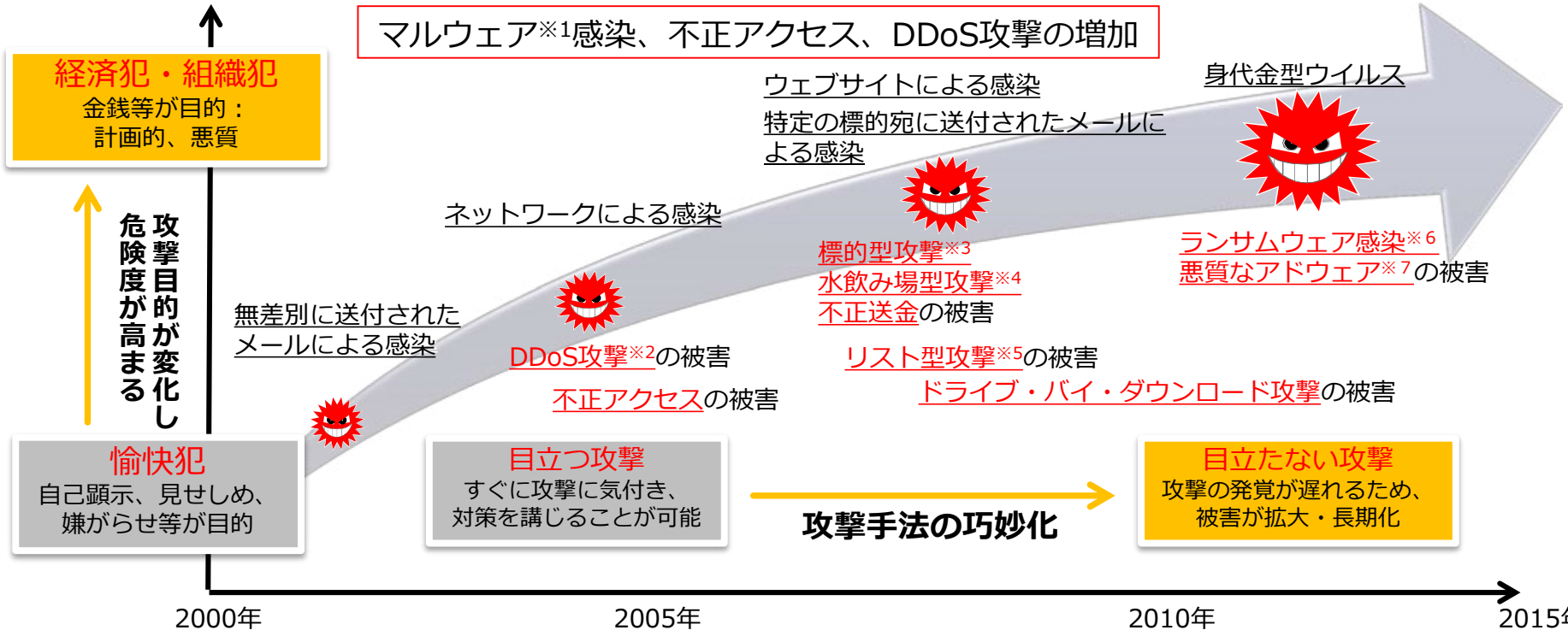
（１）　公衆無線LANの現状

（２）　公衆無線LANセキュリティ対策のあり方

（３）　セキュリティに配慮した公衆無線LANサービスの普及策

サイバーセキュリティの脅威の増大①「概況」

○　インターネット等の情報通信技術は社会経済活動の基盤であると同時に我が国の成長力の鍵であるが、昨今、サイバーセキュリティ上の脅威が悪質化・巧妙化し、その被害が深刻化。



※1 マルウェア（Malware）： Malicious softwareの短縮語。コンピュータウイルスのような有害なソフトウェアの総称。

※2 DDoS攻撃： 分散型サービス妨害攻撃（Distributed Denial of Service）のこと。多数の端末から一斉に大量のデータを特定宛先に送りつけ、宛先のサーバ等を動作不能にする攻撃。

※3 標的型攻撃： 機密情報等の窃取を目的として、特定の個人や組織を標的として行われる攻撃。

※4 水飲み場型攻撃： 標的組織が頻繁に閲覧するウェブサイトで待ち受け、標的組織に限定してマルウェアに感染させ、機密情報等を窃取する攻撃。

※5 リスト型攻撃： 不正に入手した他者のID・パスワードをリストのように用いてWebサービスにログインを試み、個人情報の窃取等を行う攻撃。

※6 ランサムウェア (Ransomware)： 身代金要求型ウイルスのこと。感染端末上にある文書などのファイルが暗号化され、暗号解除のためには金銭を要求される。

※7 アドウェア(Adware)： 広告表示によって収入を得るソフトウェアの総称。狭義には、フリーウェアと共にインストールされ、ブラウザー利用時に広告を自動的に付加するソフト。

サイバーセキュリティの脅威の増大②「国内事例」「海外事例」

国内事例

２０１５年６月・・・**日本年金機構**の職員が利用する端末がマルウェアに感染し、年金加入者に関する情報約125万件が流出（**標的型攻撃**）

２０１５年10月・・・**金融庁**の注意喚起を装ったフィッシングサイトを確認、 国内銀行のセキュリティを向上させるためと称し、口座番号、パスワード、第二認証などの情報を騙し取られるおそれ（**フィッシング攻撃**）

２０１５年11月・・・**東京五輪組織委員会**のホームページにサイバー攻撃、約12時間閲覧不能（**DDoS攻撃**）

２０１６年６月・・・**i.JTB（JTBのグループ会社）**の職員が利用する端末が、マルウェアに感染し、パスポート番号を含む個人情報が流出した可能性（**標的型攻撃**）

２０１７年５月・・・**WannaCry**による被害が発生。企業内のシステム停止などの障害が発生した。（**ランサムウェア**）

海外事例

２０１５年４月・・・**フランスのテレビネットワーク TV５ Monde** がサイバー攻撃を受け、放送が一時中断（**標的型攻撃**）

２０１５年６月・・・**米国の人事管理局（OPM）**が不正にアクセスされ、政府職員の個人情報が流出（**不正アクセス**）

２０１５年12月・・・**ウクライナの電力会社**のシステムがマルウェアに感染し、停電が発生（**標的型攻撃**）

２０１６年10月・・・**米国のDyn社**のDNSサーバが大規模なDDoS攻撃を受け、同社の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（**DDoS攻撃**）

２０１７年５月・・・アメリカ、イギリス、中国、ロシア等において、**WannaCry**による被害が発生。行政、民間企業、医療等の多くの組織に影響を及ぼした。（**ランサムウェア**）

JNSAによるセキュリティ十大ニュース

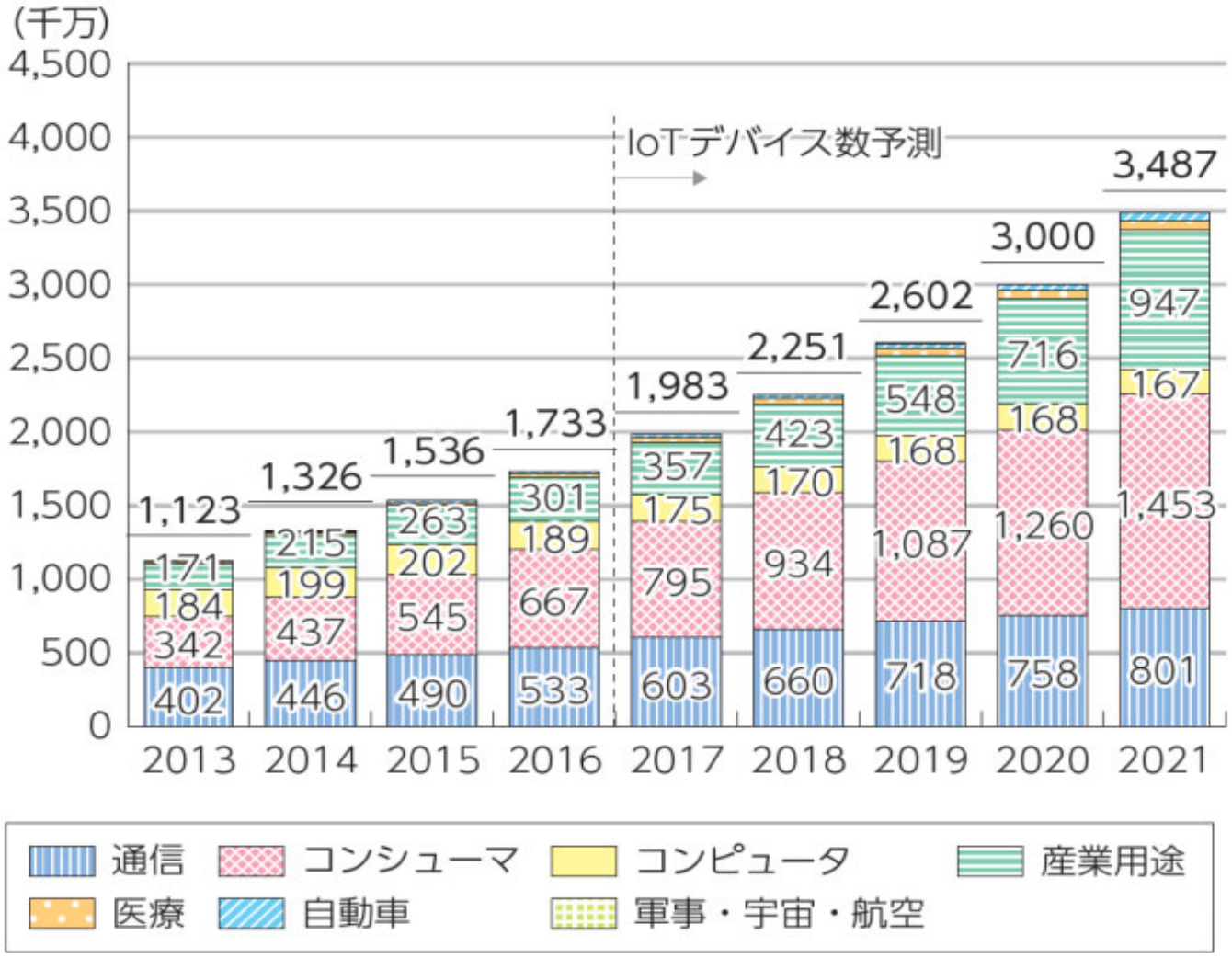
	2016セキュリティ十大ニュース
1位	**IoT機器による史上最大規模のDDoS攻撃の実態が明らかに ～防犯カメラ等のIoTデバイスのセキュリティは喫緊の重要課題～**
2位	IPAから「ランサムウェア感染を狙った攻撃に注意」と注意喚起 ～ランサムで 資料使えず キョウハクシ（今日白紙／脅迫し）～
3位	政府機関から「ポケモンGO」の利用者向けに注意喚起 ～国民全体のセキュリティ意識向上へGO!～
4位	人工知能が囲碁の世界トップ棋士に完勝 ～AIはビッグブラザーの夢を見るか？～
5位	ＩＰＡ新設国家資格「情報処理安全確保支援士」の初回申請受付を開始 ～セキュリティ人材不足の切り札となるか～
6位	防衛省と自衛隊の情報基盤へのサイバー攻撃 ～外に開かれた防衛系大学PCを踏み台に本丸へ侵入か？～
7位	アメリカ大統領選挙はドナルド・トランプ氏が勝利 ～トランプ現象は日本のセキュリティに向かい風か？～
8位	佐賀県教育委員会は不正アクセス被害を公表 ～17歳の少年の犯行、ダークサイドとゲーム感覚の狭間～
9位	JTBグループのWebサイトから大量の個人情報流出か ～巧妙化する標的型攻撃メール、問われる日頃からの備え～
10位	EU、一般データ保護規制（EUプライバシー規制）正式に採択 ～個人データの変化と脅威の遍在化に対応した新しいルール～

	2017セキュリティ十大ニュース
1位	**総務省が「IoTセキュリティ総合対策」を発表 ～攻撃者が嬉々とするIoT機器の危機的な状況～**
2位	IPAがランサムウェア「WannaCry」に関する注意喚起を発表 ～侮るなかれ、セキュリティ対策の基本の基本～
3位	米国の一私企業のミスで日本の通信インフラが混乱 ～巨人の咳一つでゆらぐインターネット～
4位	世界が狂騒したWPA2の脆弱性は狂想だった ～SNSでの不確かな憶測情報が不安を助長した～
5位	米国、サイバー攻撃に北朝鮮関与を断定 ～国家によるサイバー攻撃の常態化～
6位	長野県の高校生が不正アクセス容疑で逮捕される ～目立つサイバー犯罪の低年齢化～
7位	改正個人情報保護法が全面施行に ～個人情報の保護と利活用の両立に効果を発揮するか～
8位	米国消費者信用情報会社Equifaxで大量の個人情報が流出 ～止まらぬ大規模情報漏洩事件～
9位	IPA「情報処理安全確保支援士」累計で約7,000名に！ ～2020年までに3万人は達成できるのか～
10位	セキュリティ会社員がウイルス保管容疑で逮捕 ～セキュリティ企業が時代の要請に応えるために～

出典：NPO日本ネットワークセキュリティ協会（JNSA）ホームページ

IoT機器の推移

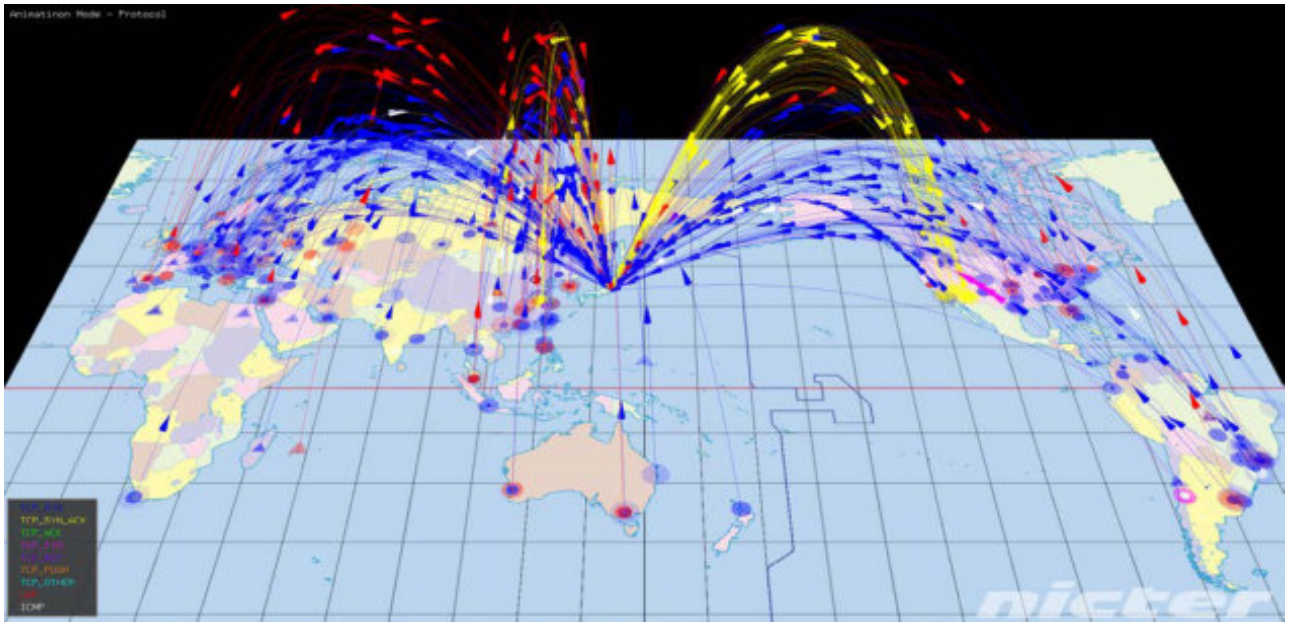
○　IHS Technology の推定によれば、2016年時点でインターネットにつながるモノ（IoT機器）の数は173億個であり、2021年までにその２倍の349億個まで増加するとされている。

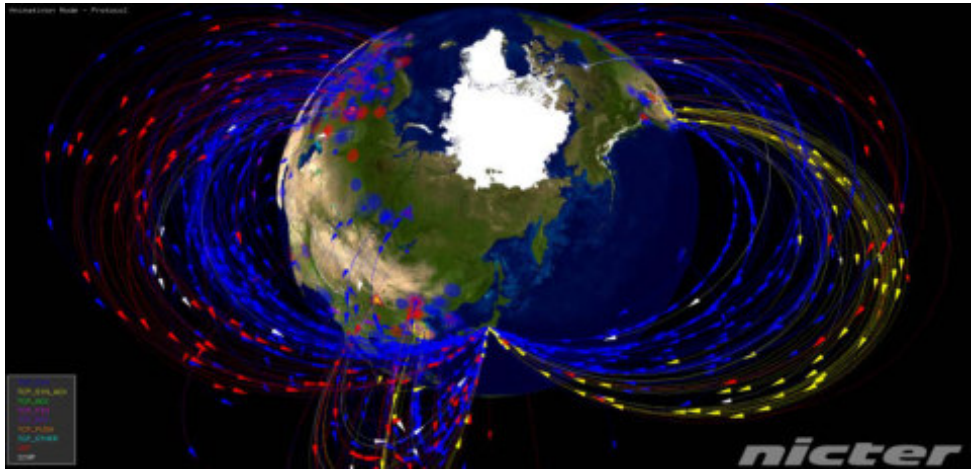


出典：IHS Technology

サイバー攻撃の状況（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。





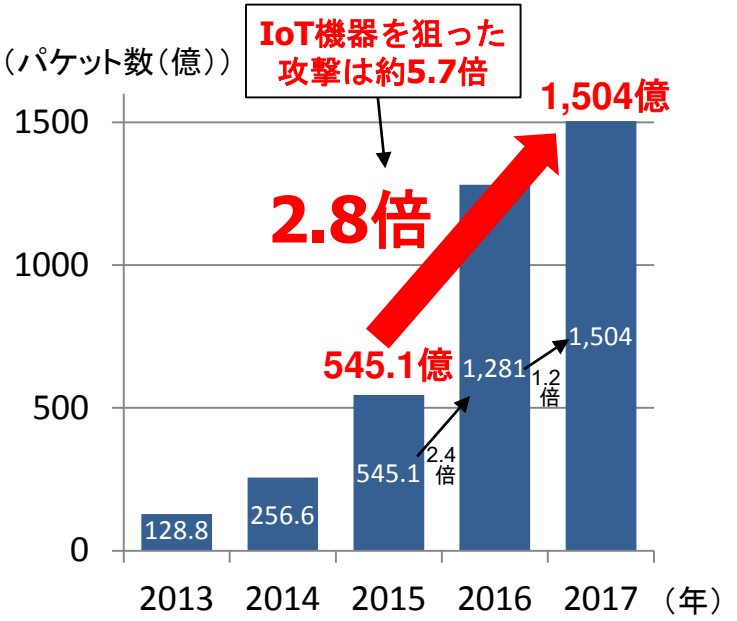
- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

・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

NITCERで１年間に観測されたサイバー攻撃回数

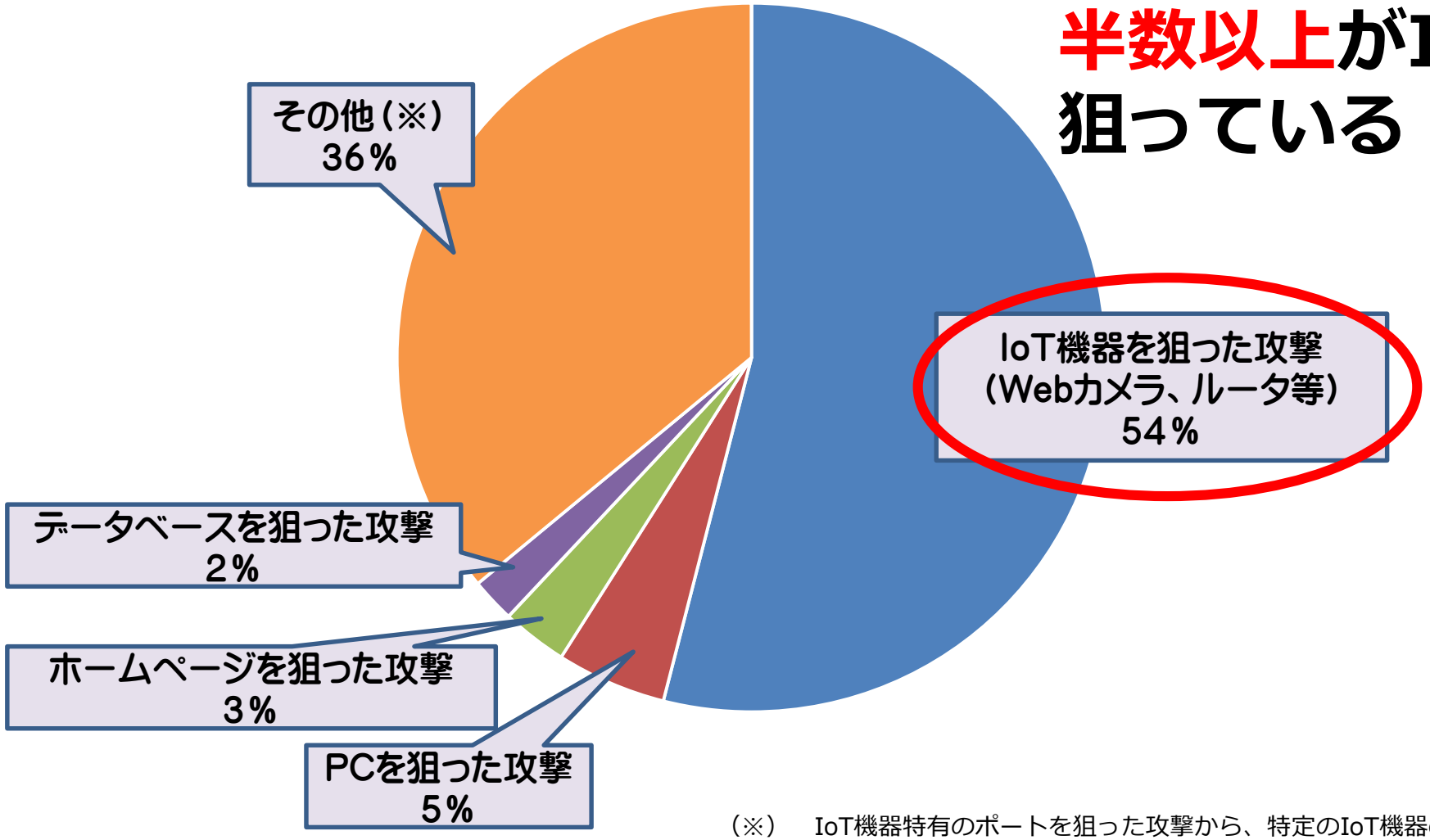
・２年間で２．８倍
（2015年→2016年：２．４倍、2016年→2017年：１．２倍）



サイバー攻撃の内訳（2017年、NICTERによる観測）

観測された全サイバー攻撃1,504億パケットのうち、

半数以上がIoTを狙っている！



（※）　IoT機器特有のポートを狙った攻撃から、特定のIoT機器の脆弱性を狙ったより高度な攻撃も観測されるようになっており、単純にポート番号だけから分類することが難しいIoT機器を狙った攻撃が「その他」に含まれている。

IoTセキュリティ対策の必要性

○　IoTでは、これまで接続されていなかった自動車やカメラなどの機器が、Wi-Fiや携帯電話網などを介してインターネットに接続されることにより、新たな脅威が発生し、それに対するセキュリティ対策が必要となった。

自動車へのハッキングによる遠隔操作

人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。
（ID，パスワードなどの初期設定が必要）

本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．サイバーセキュリティ政策の動向

３．公衆無線LANのセキュリティ対策

（１）　公衆無線LANの現状

（２）　公衆無線LANセキュリティ対策のあり方

（３）　セキュリティに配慮した公衆無線LANサービスの普及策

サイバーセキュリティ推進体制

○　平成26年11月に成立した「サイバーセキュリティ基本法」に基づき、平成27年1月、内閣にサイバーセキュリティ戦略本部が設置され、同年9月、日本年金機構の年金情報流出の事案も踏まえた新たな「サイバーセキュリティ戦略」を閣議決定。同本部を司令塔として、事務局を担う内閣サイバーセキュリティセンター（NISC）の調整の下、関係省庁が連携した政府横断的サイバーセキュリティ推進体制を整備し、本戦略を推進。

内閣　内閣総理大臣

高度情報通信ネットワーク社会推進戦略本部（IT総合戦略本部）
高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進

緊密連携

サイバーセキュリティ戦略本部（2015.1.9 ｻｲﾊﾞｰｾｷｭﾘﾃｨ基本法により設置）

本部長　内閣官房長官
副本部長　サイバーセキュリティ戦略本部に関する事務を担当する国務大臣
本部員　国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック競技大会・パラリンピック競技大会担当大臣
有識者（７名；10名以下）

閣僚が参画

遠藤　信博　日本電気株式会社代表取締役会長
小野寺　正　ＫＤＤＩ株式会社代表取締役会長
中谷　和弘　東京大学大学院法学政治学研究科教授
野原佐和子　株式会社イプシ・マーケティング研究所代表取締役社長
林　紘一郎　情報セキュリティ大学院大学教授
前田　雅英　日本大学大学院法務研究科教授
村井　純　慶應義塾大学教授

重要インフラ専門調査会
研究開発戦略専門調査会
普及啓発・人材育成専門調査会
ｻｲﾊﾞｰｾｷｭﾘﾃｨ対策推進会議（CISO等連絡会議）

緊密連携

国家安全保障会議（NSC）
我が国の安全保障に関する重要事項を審議

（事務局）

内閣官房　内閣サイバーセキュリティセンター
（2015.1.9 内閣官房組織令により設置）
内閣サイバーセキュリティセンター長
（内閣官房副長官補(事態対処・危機管理)が兼務）
副センター長（内閣審議官）
上席サイバーセキュリティ分析官
サイバーセキュリティ補佐官

政府機関・情報セキュリティ横断監視・即応調査チーム（ＧＳＯＣ）
情報セキュリティ緊急支援チーム（CYMAT）

＜重要インフラ所管省庁＞
金融庁　（金融機関）
総務省　（地方公共団体、情報通信）
厚生労働省　（医療、水道）
経済産業省　（電力、ガス、化学、クレジット、石油）
国土交通省　（鉄道、航空、物流）

＜その他関係省庁＞
文部科学省（セキュリティ教育）等

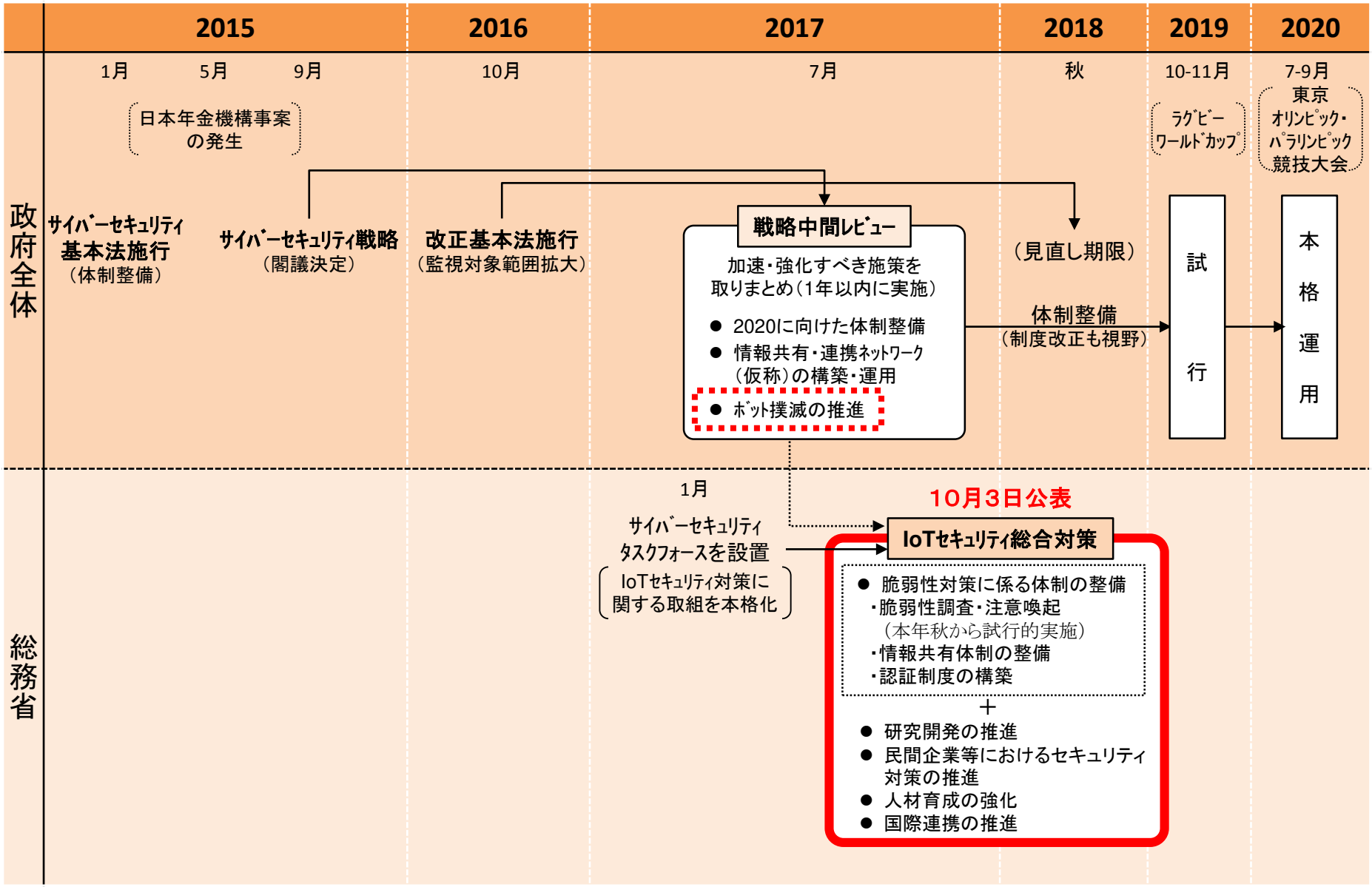
協力

協力

閣僚本部員５省庁
警察庁（サイバー犯罪・攻撃の取締り）
総務省（通信・ネットワーク政策）
外務省（外交・安全保障）
経済産業省（情報政策）
防衛省（国の防衛）

重要インフラ事業者等　政府機関（各府省庁）　企業　個人

サイバーセキュリティ戦略の推進



IoTセキュリティ総合対策（2017年10月3日　公表）

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

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

本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．サイバーセキュリティ政策の動向

３．公衆無線LANのセキュリティ対策

（１）　公衆無線LANの現状

（２）　公衆無線LANセキュリティ対策のあり方

（３）　セキュリティに配慮した公衆無線LANサービスの普及策

公衆無線LANの概要

○　公衆無線LANは、電気通信事業者や自治体等のサービス提供者が無線LANのアクセスポイントを設置して、飲食店や宿泊施設、交通機関、競技場等においてインターネット接続サービスを提供するものとして、その普及が進んでいる。（一般に、公衆無線LANを指す用語として、Wi-Fiを用いることも多い。）

利用イメージ

Wi-Fiとは

○　無線LAN技術の推進団体であるWi-Fi Allianceによる相互接続性の認定テストによって、一定レベルの相互運用性が保証されているもの

出典：「無線LANビジネス研究会報告書」（総務省）　http://www.soumu.go.jp/menu_news/s-news/02kiban04_03000093.html

無線LANの普及の三段階

○　無線LANの普及は、大きく三つの段階に分けることができる。

第1段階

家庭内・企業内の
有線ネットワークを置換
（1999年～）

○　1999年のIEEE802.11bの標準化により、家庭内・企業内において無線LANが普及

第2段階

無線LAN対応機器の
普及に伴う
公衆インフラ化
（2002年～）

○　ノートパソコンやゲーム機等にWi-Fiチップが搭載され、Wi-Fiのモバイル利用が可能となり、公共インフラ化

○　通信事業者が公衆無線LANサービスを開始し、駅・空港・宿泊施設・飲食店等において、公衆無線LANサービスが普及

第3段階

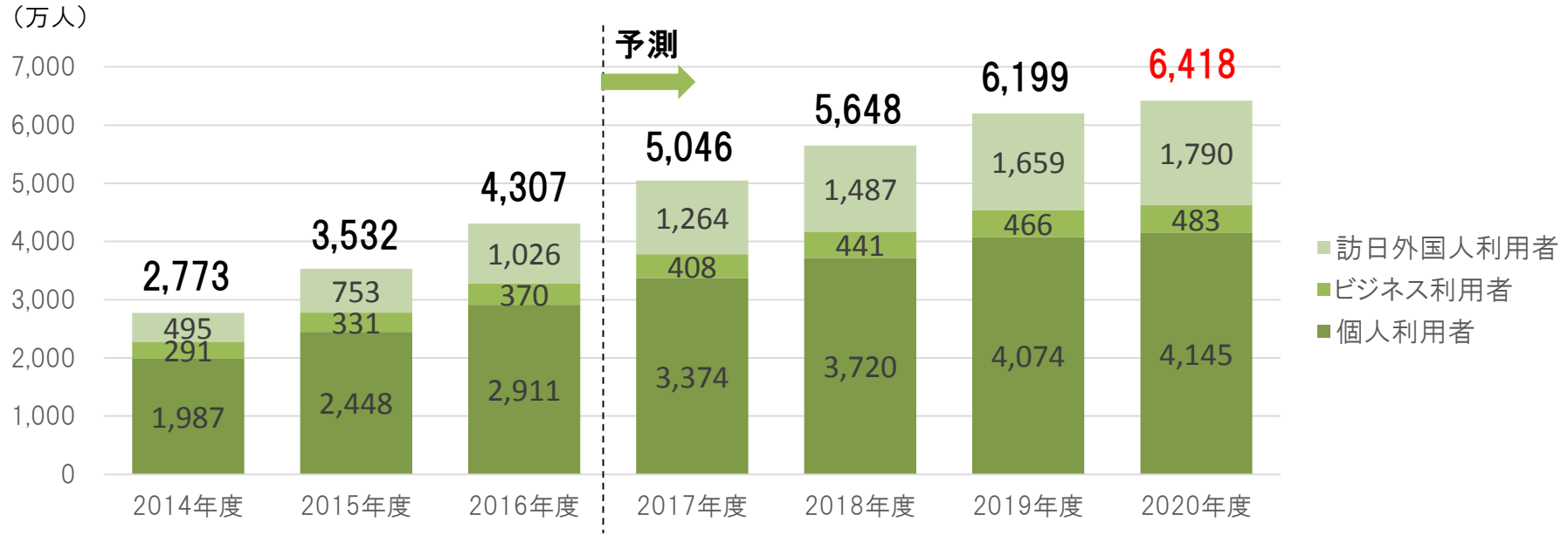
スマートフォンの普及による
オフロード対策
（2012年～）

○　スマートフォンの普及を契機として、無線通信トラヒックのオフロード対策の進展等により、公衆無線LANが急速に拡大

公衆無線LANの普及状況

○　公衆無線LANは、観光・防災等、街づくりに不可欠な社会基盤へと進化し、その利用者数は引き続き増加傾向にあり、**国内における2020年度末時点の利用者数は、約6,400万人（2016年度末時点で約4,300万人）と予測**されている。

公衆無線LANサービスの利用者数の予測



（注1）　日本在住の個人･ビジネス利用者は、各年度末の利用者数。2017年度以降は予測値。
（注2）　日本在住の個人･ビジネス利用者の定義は、1か月に1回以上利用するアクティブユーザー。
（注3）　訪日外国人利用者の定義は、訪日時に1回以上利用したユーザーの年間合計数。

「2017年公衆無線LAN利用者動向調査」(ICT総研)
http://ictr.co.jp/report/20170921.html　を基に作成。

公衆無線LANサービスの利用者のメリット

1．携帯回線のパケット通信料を削減できる

通信事業者によっては、月に一定量以上のデータを送受信すると携帯回線の通信速度が遅くなること（帯域制限がかかること）がある。公衆無線LANを時と場合に応じて上手に利用することができれば、携帯回線でのパケット通信料を抑制し、帯域制限を回避することができる。

2．通信速度が速い

サイズが大きい動画や写真を見たり送ったりするとき、混雑状況によるが、比較的通信速度が速く、短時間で再生、表示することができる。

例えば、ゲームソフト等のサイズの大きいプログラムのダウンロードも早く終えることができる。

3．簡単に設定・接続ができる

通信事業者等が提供する公衆無線LANに接続するためのアプリを利用すると、非常に簡単な設定で、街中にある公衆無線LANが利用できる。

4．災害時に役立つ情報インフラである

熊本地震の際には、携帯電話事業者等による「00000JAPAN」（ファイブゼロ・ジャパン）の提供等を通じて、被災者の通信環境が確保された。

公衆無線LANは、平時の利用だけでなく、災害発生時には被災者支援に用いることができる。

「Wi-Fi利用者向け簡易マニュアル」（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_Users.pdf　等を基に作成。

公衆無線LANサービスの提供者のメリット

1．来訪者サービスの向上

SNSの人気もあり、いつでも・どこでもインターネットを利用した人が多くなっており、また、最近ではスマートフォンで動画を見る人も増えており、無料で高速な通信を実現する公衆無線LANの導入は、来訪者のサービスの向上につながる。

2．外国人観光客の誘客

海外では無料の公衆無線LANサービスが普及していることもあり、日本でも公衆無線LANサービスを利用したいと考える外国人観光客が多くなっており、誰でも利用できる公衆無線LANを設置することは、海外からの観光誘客にもつながる。

3．店舗・施設情報の発信

公衆無線LANサービスと組み合わせて店舗や施設の情報を発信することができ、来訪者に対するPRにつなげることも可能。

4．災害時の活用

災害時には携帯電話回線が利用しにくくなることがある。公衆無線LANは災害時でも比較的つながりやすいため、代替の通信手段として活用することができる。

「Wi-Fi提供者向けセキュリティ対策の手引き」（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf を基に作成。

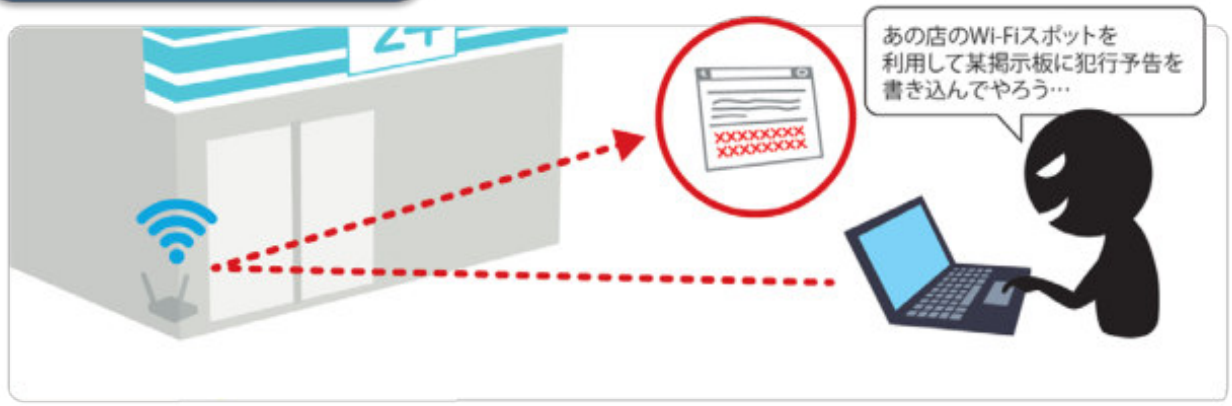
公衆無線LANにおけるセキュリティリスク

○　公衆無線LANは誰でも接続できるという利便性を有する一方、様々なセキュリティリスクが存在。

利用者のリスク例

○　利用者の通信内容が盗聴され、ID・パスワードが盗まれるおそれ　等

提供者のリスク例



○　迷惑メールの送信や掲示板への悪意ある書き込みに悪用されるおそれ　等

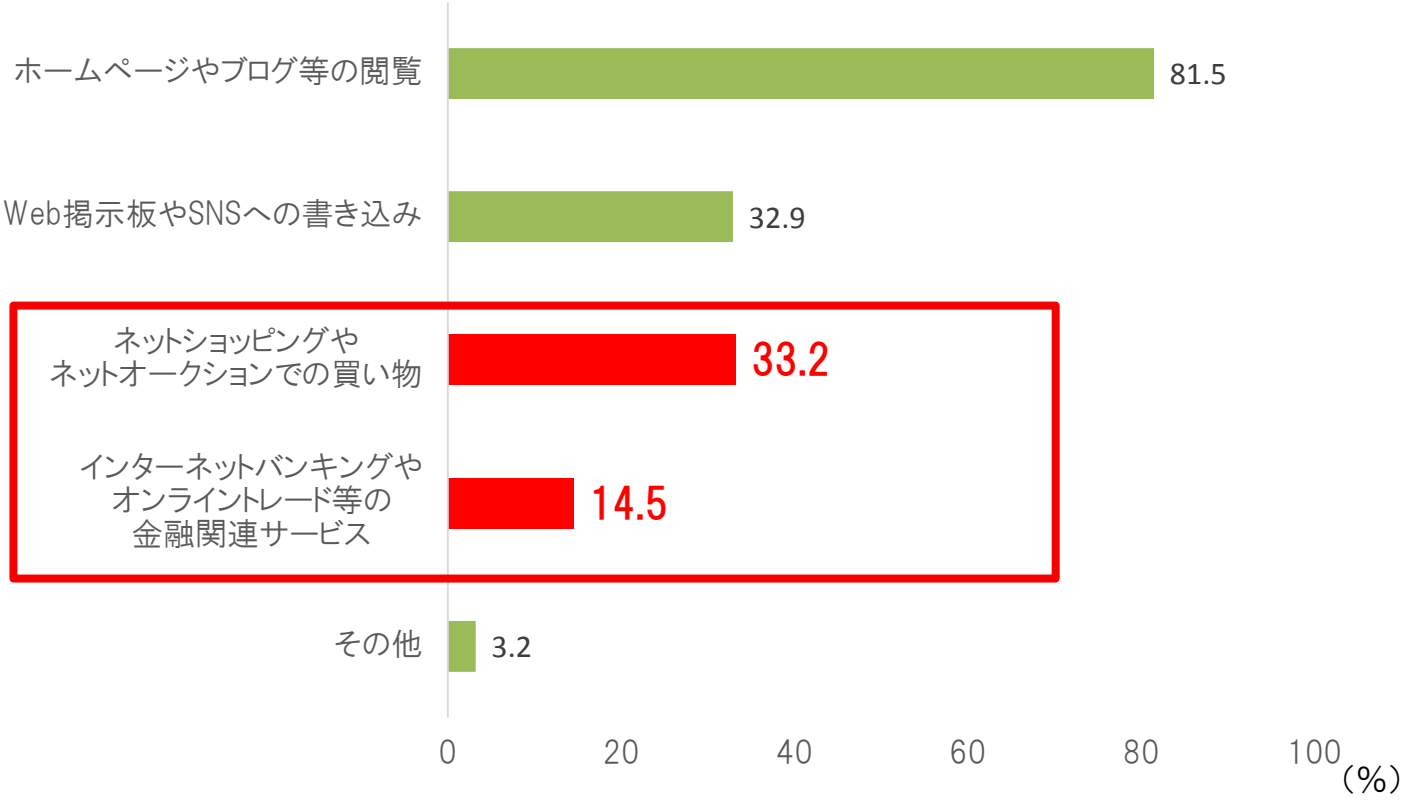
「Wi-Fi提供者向けセキュリティ対策の手引き」（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf　を基に作成。

公衆無線LANのセキュリティに関する現状

○　公衆無線LANの利用者が利用しているサービスには、ネットショッピングやネットオークションでの買い物、インターネットバンキングやオンライントレード等の金融関連サービスといった金銭に関するものもある。

○　他方、公衆無線LANサービスには、無線区間の通信が暗号化されていないアクセスポイントが存在。

公衆無線LANの利用者が利用しているサービス（2016年）（複数回答可）

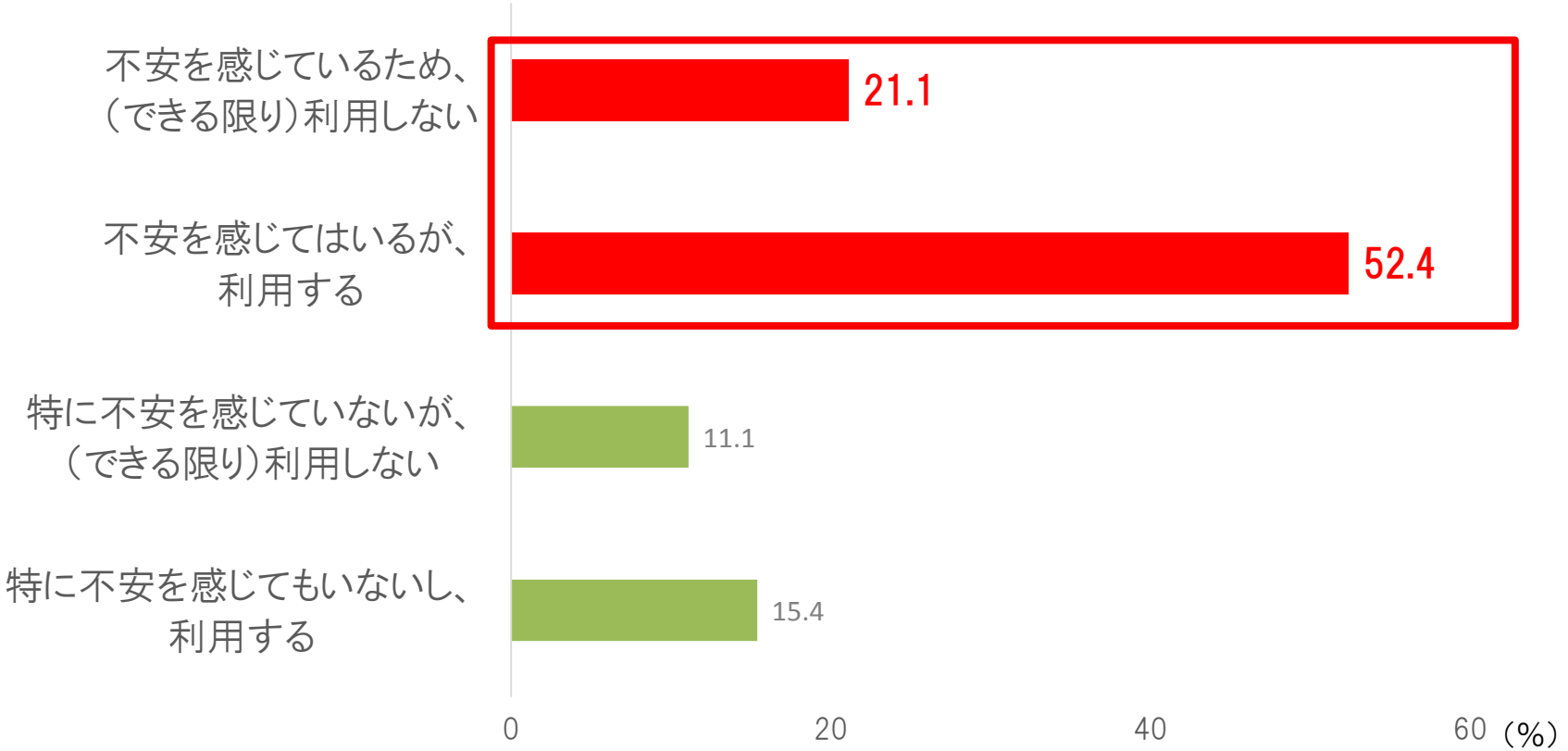


出典：「2016年度情報セキュリティの脅威に対する意識調査」（情報処理推進機構）
https://www.ipa.go.jp/security/fy28/reports/ishiki/index.html

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①

○　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

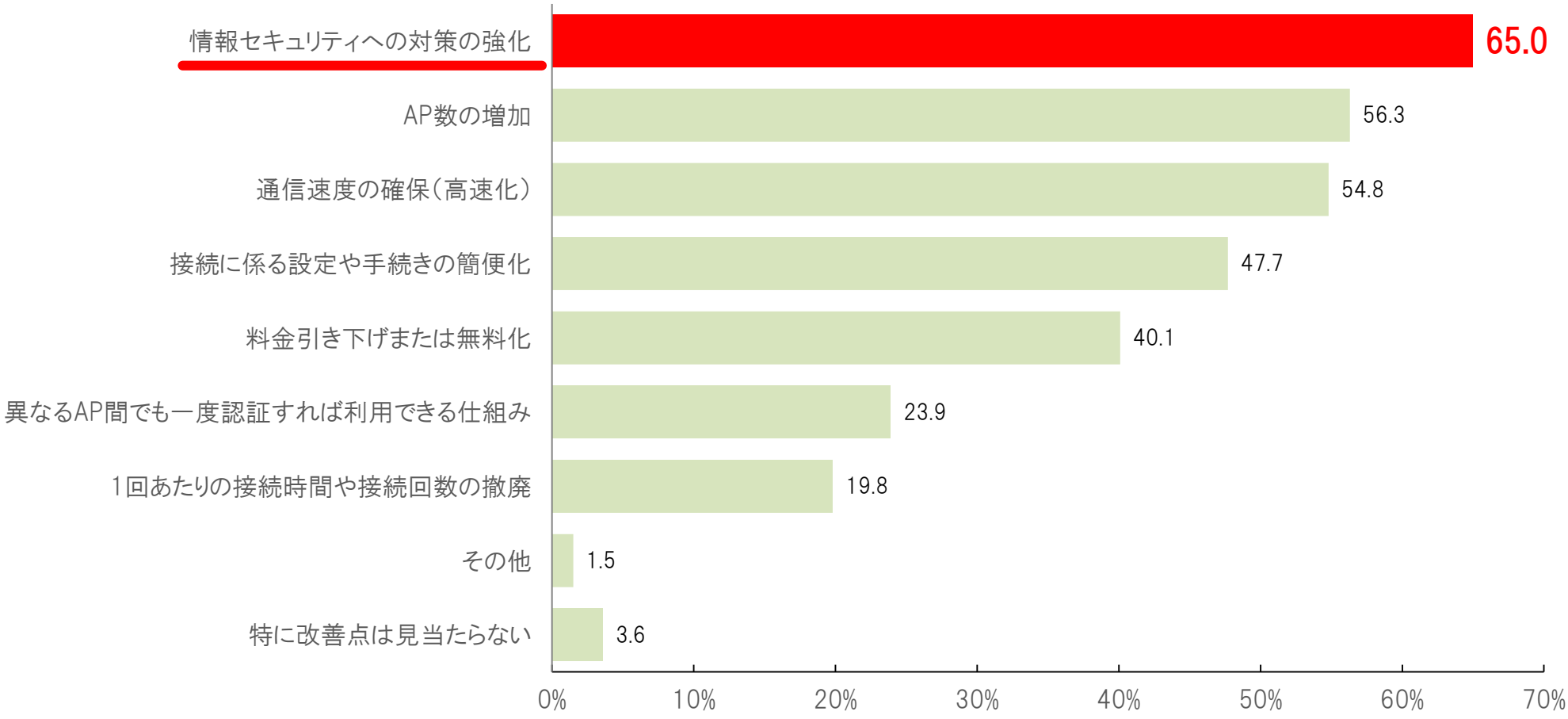


出典：「利用者の無線LANサービスに関するセキュリティ意識調査結果（2017年度）」（総務省）

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②

○　公衆無線LANの更なる普及が期待される中、**公衆無線LAN利用において利用者が求める改善点としては、「情報セキュリティ対策の強化」が最も多い**。

普段利用している公衆無線LAN利用に係る改善点について（複数回答可）



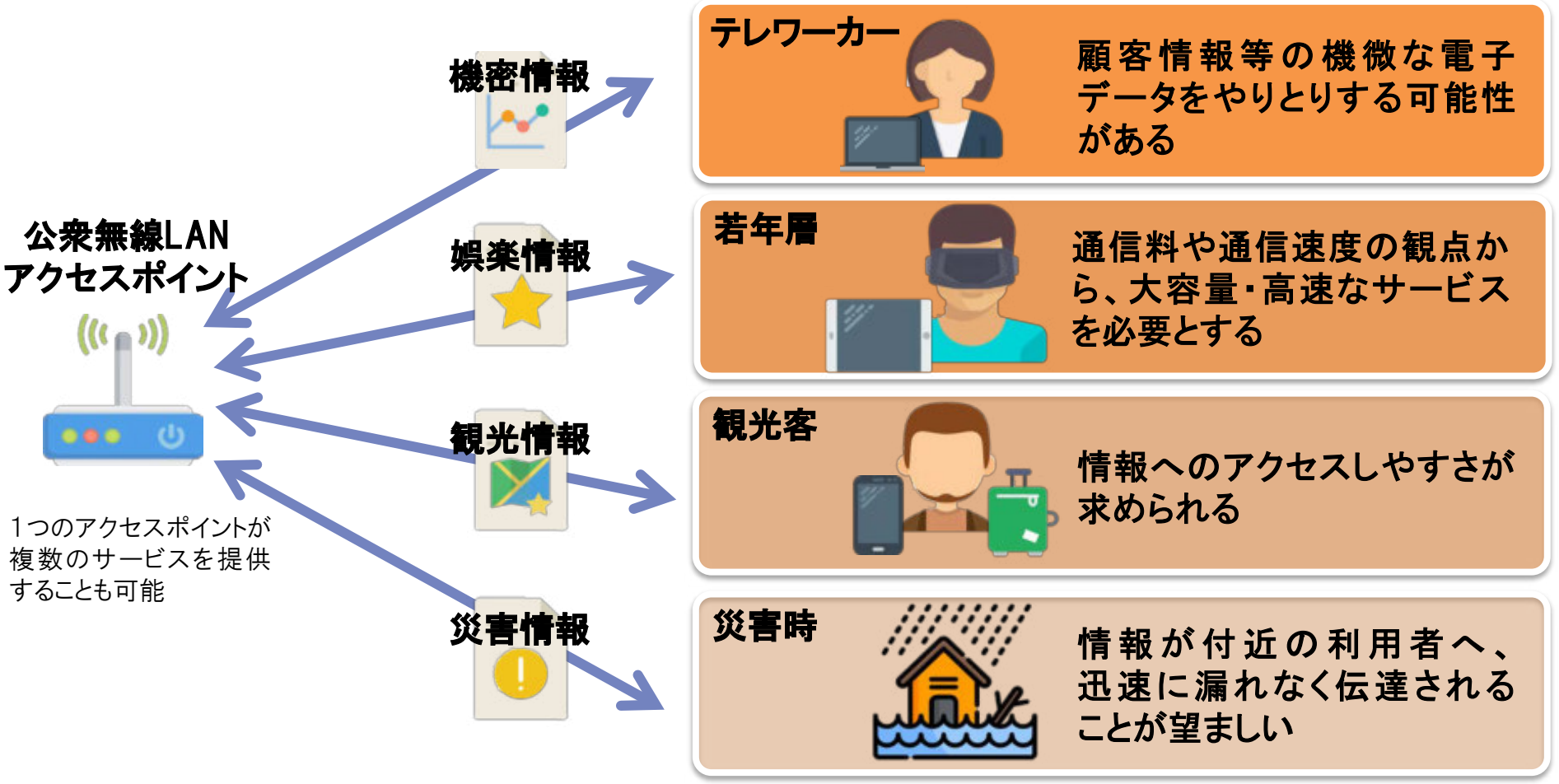
出典：「公衆無線LAN利用に関する情報セキュリティ意識調査結果」（総務省）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000091.html

公衆無線LANの利用形態を踏まえたセキュリティ対策の必要性

○　公衆無線LANの普及の阻害要因の一つに、利用者が抱えるセキュリティに対する不安がある。

○　公衆無線LANには、テレワーク環境の提供、リッチコンテンツの配信、観光客向けの観光情報案内、災害等の緊急時における情報提供といった様々なサービスの利用が期待されている。

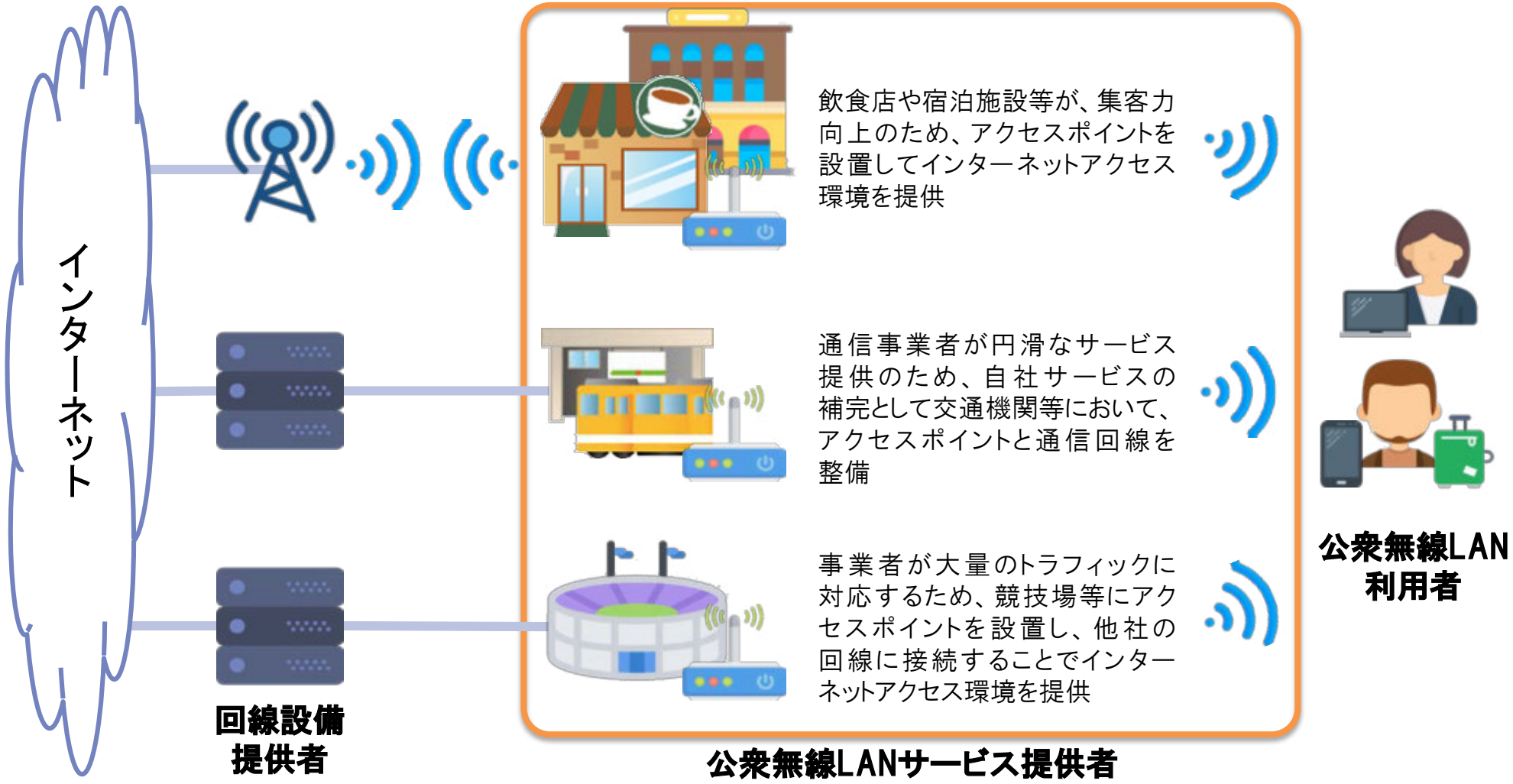
○　**利便性と安全性のバランスに配慮し、様々な利用者・利用シーンに応じたセキュリティ対策が必要**。



公衆無線LANの提供形態を踏まえたセキュリティ対策の必要性

○　サービスの範囲や課金の有無等、様々な公衆無線LANの提供形態が存在。

○　提供者のビジネス環境等を配慮し、提供形態や目的に応じたセキュリティ対策が必要。



本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．サイバーセキュリティ政策の動向

３．公衆無線LANのセキュリティ対策

（１）　公衆無線LANの現状

（２）　公衆無線LANセキュリティ対策のあり方

（３）　セキュリティに配慮した公衆無線LANサービスの普及策

無線LANにおけるセキュリティ上の脅威

○　一般に、無線LANにおけるセキュリティ上の脅威として、① 通信傍受、② 不正アクセス、③ なりすまし、④ 不正なアクセスポイントの設置等が知られている。

○　こうした脅威に対するセキュリティ対策として、無線LANにおける認証や暗号化が挙げられる。

無線通信を傍受することで、
情報の読取等を行う。

悪意のある第三者

① 通信傍受

② 不正アクセス

悪意のある第三者

利用者の端末等に不正に侵入し、
情報の読取等を行う。

悪意のある第三者

利用者

アクセス
ポイント

インターネット

③ なりすまし

正規の利用者になりすまし、不正な
サービスの利用、攻撃等を行う。

④ 不正なアクセスポイントの設置

不正なアクセスポイント

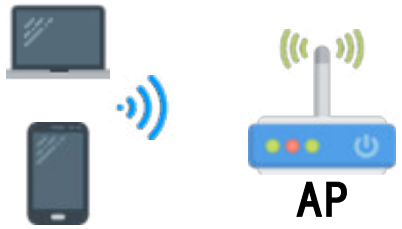
正規のアクセスポイントになりすますことで、利用者の
接続を誘引し、情報の読取等を行う。

無線LANのセキュリティ対策：認証

○　**認証とは、端末やアクセスポイントが、接続相手の正当性を確認する仕組み**であり、正当性が確認できない相手とは通信できない。

○　認証を行うことにより、接続に係る情報が記録され、不正な端末による接続試行の検知や不正利用発覚後の特定の一助となる。

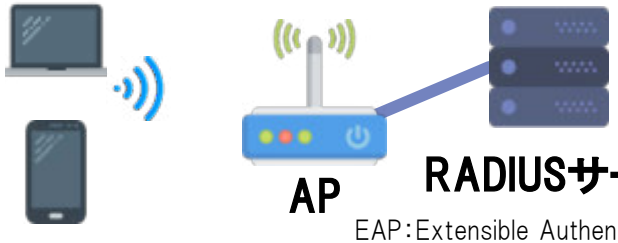
PSK方式（パーソナル）



APに設定されているパスフレーズと、利用者が入力したパスフレーズが一致することで認証。

PSK：Pre-Shared Key
AP：Access　Point

EAP方式（エンタープライズ）



RADIUSサーバが、各端末に保存された情報等を基に認証。

EAP：Extensible Authentication Protocol
RADIUS：Remote Authentication Dial-in User Service

	認証方式	認証サーバの要否	端末側の認証	アクセスポイント側の認証	特徴
パーソナル	PSK	不要	SSID・パスフレーズ	-	利用者がパスフレーズを入力する。
エンタープライズ	EAP-TLS	必要	電子証明書	電子証明書	セキュリティ強度は高いが、各端末で電子証明書を管理する必要がある。
	EAP-TTLS	必要	ID・パスワード	電子証明書	端末側の認証をID・パスワードとすることで、EAP-TLSの煩雑さに対処したもの。
	EAP-SIM/AKA	必要	SIM/USIM	乱数	SIM/USIMカードが挿入されている端末は、自動で認証される。

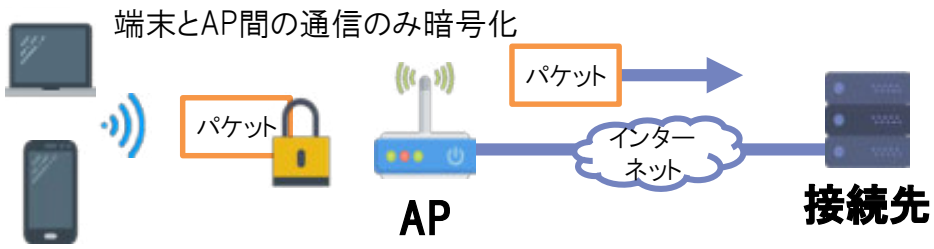
EAP-TLS：Extensible Authentication Protocol Transport Layer Security　EAP-TTLS：Extensible Authentication Protocol Tunneled Transport Layer Security
EAP-SIM：Extensible Authentication Protocol Method for Global System for Mobile Communications(GSM) Subscriber Identity Modules
EAP-AKA：Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
SIM：Subscriber Identity Module　USIM：Universal　Subscriber Identity Module

無線LANのセキュリティ対策：暗号化

○ **暗号化とは、通信の内容を容易に推定できないようにする仕組み**であり、通信の内容を秘匿化するもの。無線区間におけるネットワーク層の様々な暗号化方式には、既に脆弱性が発見されているものもあり、**利用にあわせて適切な強度の暗号化方式を設定することが望ましい**。

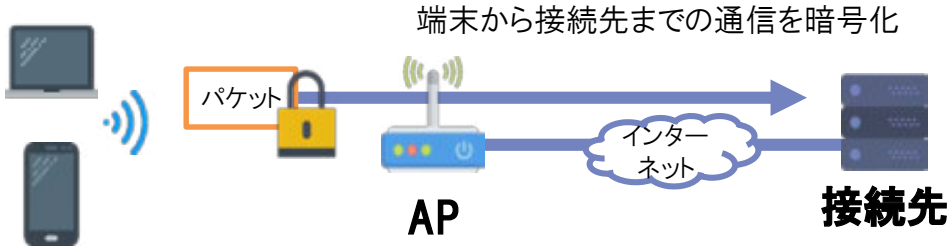
○ HTTPSやVPN等、より上位層における暗号化方式を用いて、通信の内容を秘匿することもできる。

ネットワーク層における暗号化



AP：Access Point

HTTPS及びVPN



HTTPS：Hyper Text Transfer Protocol Secure
VPN：Virtual Private Network

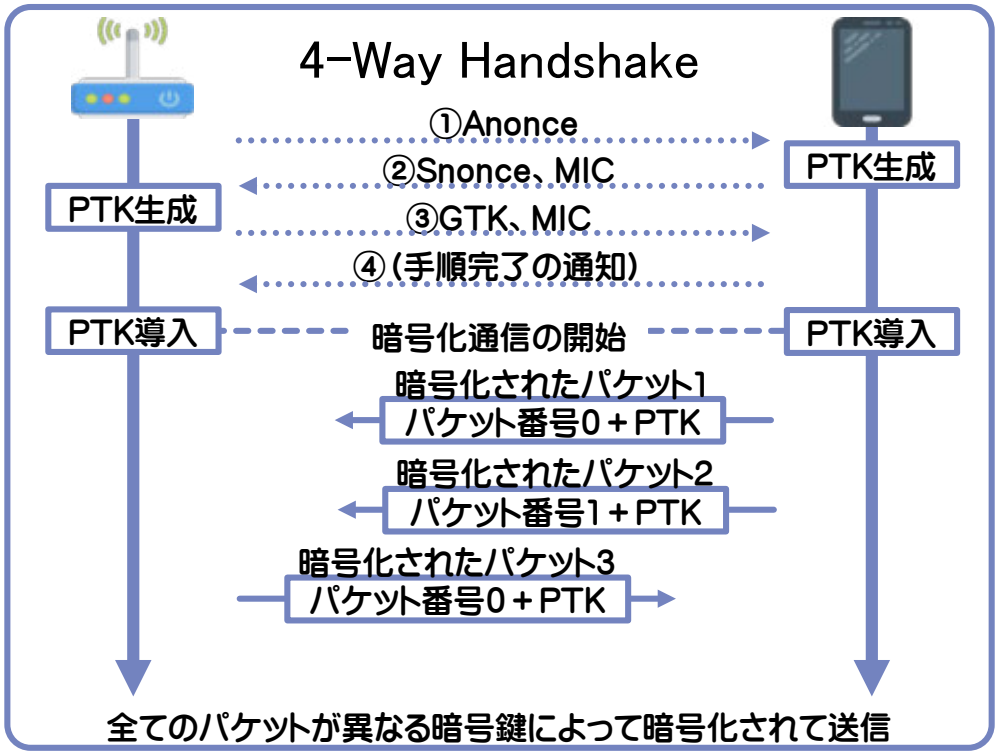
暗号化方式	特徴
WEP	○ 無線LANにおける最初の情報セキュリティ対策方式。 ○ 暗号化鍵が自動で更新されず、これを悪用した短時間で解読する方法が存在。
WPA	○ 鍵管理の方法をTKIPに変更し、WEPを拡張して策定。 ○ WEPとの互換性を有し、WEP対応の多くの端末で利用可能。
WPA2	○ 暗号化アルゴリズムや改ざん検知の方式に、より強固なもの(CCMP)を用いて策定。 ○ 現時点では無線LANにおける最も強固な暗号化方式。
HTTPS(SSL/TLS)	○ パケットのペイロード部分のみ暗号化して通信する。
VPN	○ 全体を暗号化したパケットを、暗号化された擬似的なトンネルを用いて通信する。

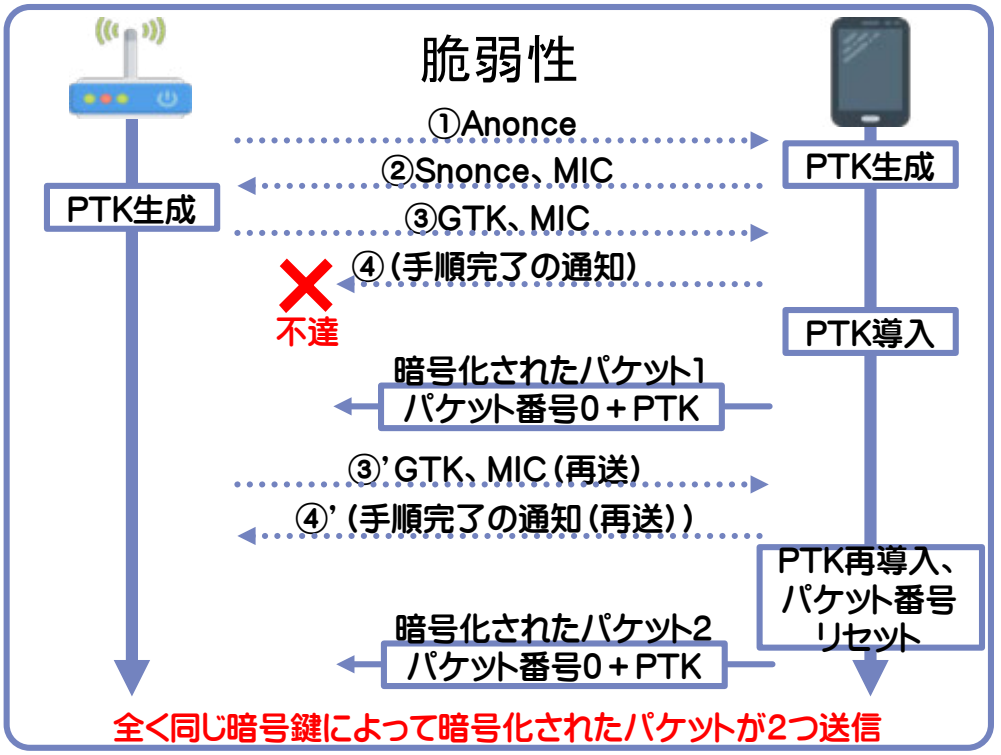
WEP：Wired Equivalent Privacy WPA：Wi-Fi Protected Access WPA2：Wi-Fi Protected Access 2
SSL：Secure Sockets Layer TLS：Transport Layer Security TKIP：Temporal Key Integrity Protocol CCMP: Counter mode with CBC-MAC Protocol

WPA2の脆弱性(KRACKs)について

○ 2017年、無線区間の通信の暗号化に用いられるWPA2に「KRACKs」という脆弱性が発見されたとの報道。

○ 本脆弱性は、WPA2の暗号化に用いる鍵を交換する仕組みである、4-Way Handshakeに起因するものであり、無線LAN接続にこの仕組みを利用する全ての機器に影響。本脆弱性を悪用することで、通信の盗聴が可能であるが、現在のところ、被害事例の報告は無し。





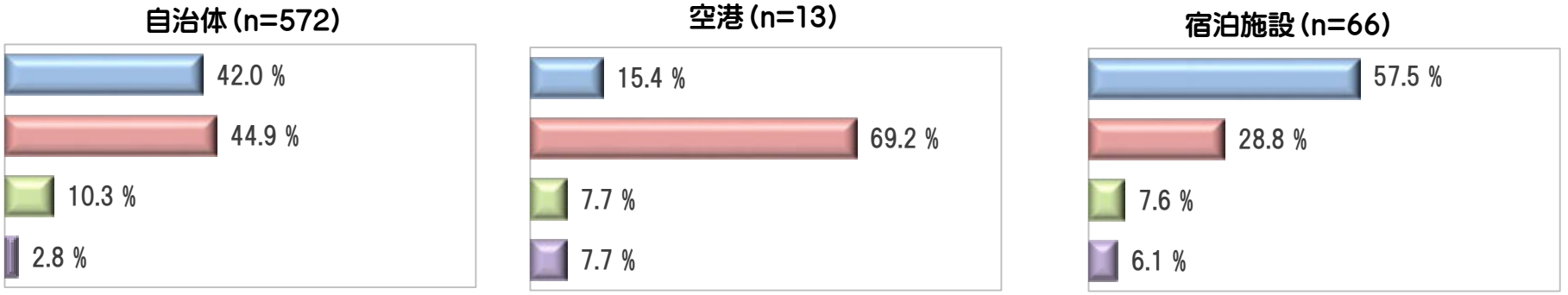
Wi-Fi Allianceは、異なる鍵交換の仕組みを採用する等、より改良されたWPA3を発表、詳細は2018年中に公表予定

小林忠男監修・無線LANビジネス推進連絡会編『Wi-Fiのすべて』(リックテレコム)、
「更新:WPA2 における複数の脆弱性について」(情報処理推進機構)
https://www.ipa.go.jp/security/ciadr/vul/20171017_WPA2.html を基に作成。

自治体等における公衆無線LANのセキュリティ対策の現状

暗号化

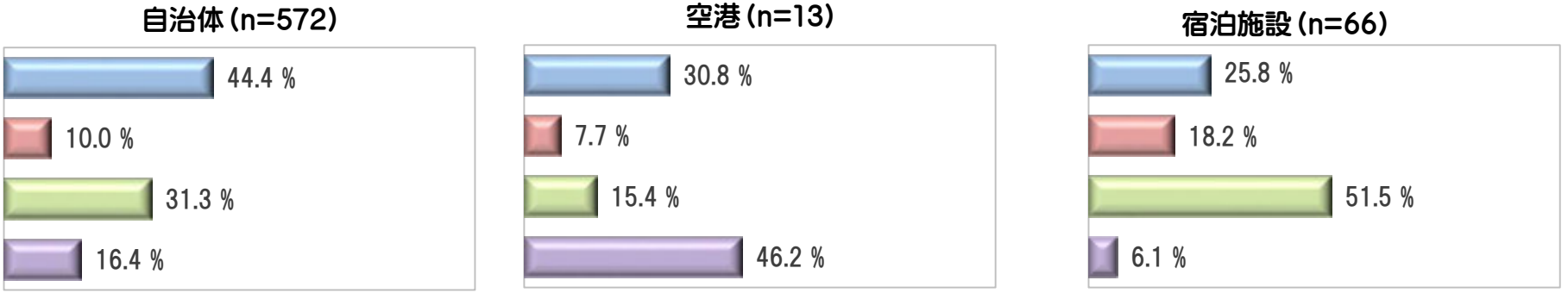
- 暗号化している
- 暗号化していない
- 暗号化しているSSIDと暗号化していないSSIDの両方を管理している
- その他（事業者が管理）



機器ファームウェアの更新

（複数回答あり）

- 都度実施している
- １年に１回程度実施している
- 実施していない
- その他（分からない、事業者が管理等）



出典：「地方公共団体が提供する「公衆無線LANサービス」の概要に関する調査結果（2017年度）」（総務省）
「企業・団体等がお客様向けに提供する「公衆無線LANサービス」の概要に関する調査結果（2017年度）」（総務省）

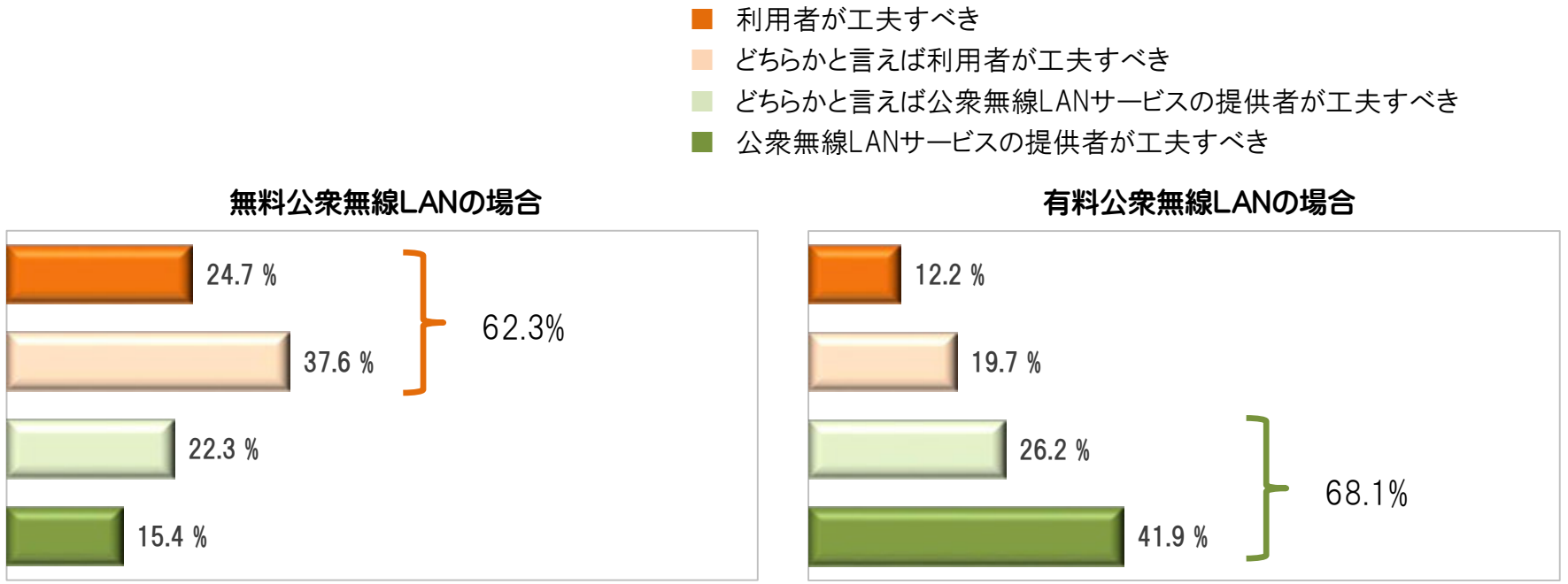
公衆無線LANのセキュリティを高める主体

○　公衆無線LANサービスの利用に当たって、**セキュリティを高めるための工夫は誰がすべきか（利用者が工夫すべきか、提供者が工夫すべきか）**という点について

・無料公衆無線LANの場合、「利用者が工夫すべき」又は「どちらかと言えば利用者が工夫すべき」と回答した割合は62.3%

・有料公衆無線LANの場合、「公衆無線LANサービスの提供者が工夫すべき」又は「どちらかといえば公衆無線LANサービスの提供者が工夫すべき」と回答した割合が68.1%

○　公衆無線LAN利用者は、**総じて無料公衆無線LANでは利用者が工夫すべきであるが、有料公衆無線LANでは提供者が工夫すべきという認識が強い**傾向にある。



出典：「利用者の無線LANサービスに関するセキュリティ意識調査結果（2017年度）」（総務省）

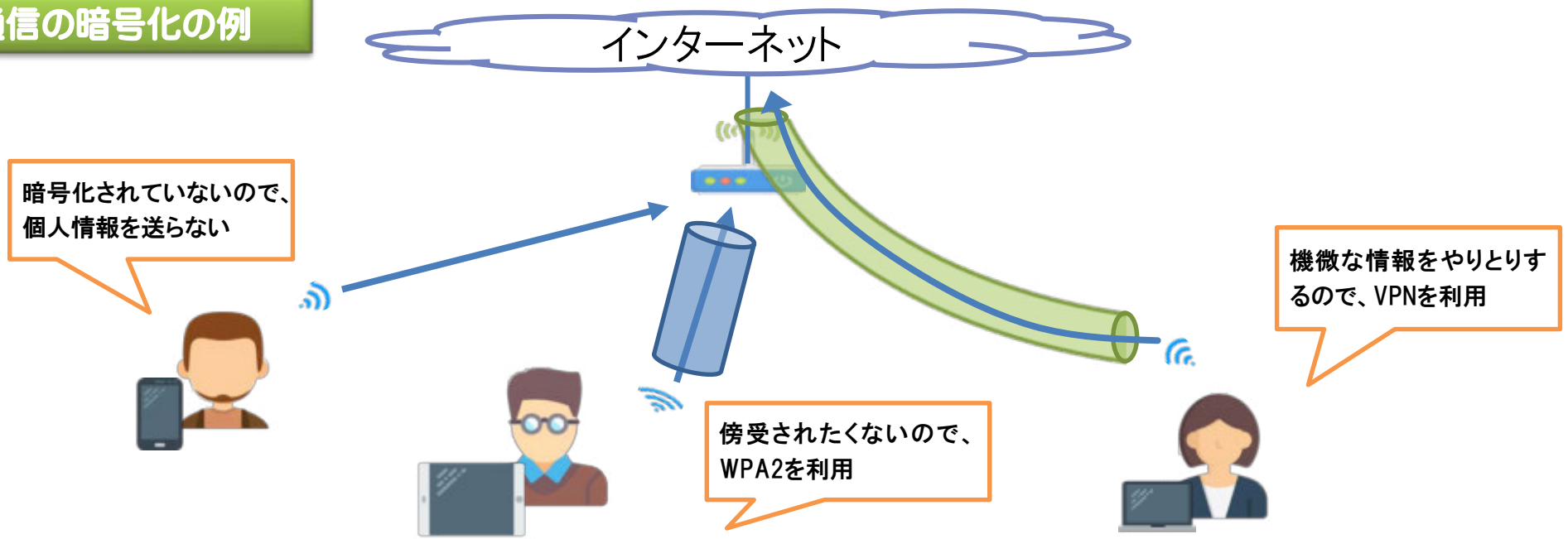
公衆無線LANセキュリティ対策の基本的考え方

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**

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**

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**

通信の暗号化の例



本日の講演内容

１．サイバーセキュリティ上の脅威の現状

２．サイバーセキュリティ政策の動向

３．公衆無線LANのセキュリティ対策

（１）　公衆無線LANの現状

（２）　公衆無線LANセキュリティ対策のあり方

（３）　セキュリティに配慮した公衆無線LANサービスの普及策

セキュアな公衆無線LAN環境の実現に向けた行動計画（2018年3月策定）

1. 利用者・提供者の意識向上

（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）

公衆無線LAN版
安全・安心マーク

（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）

公衆無線LANのセキュリティに関する周知・啓発

取組１　利用者・提供者向けマニュアル・手引きの改定

○　**「Wi-Fi利用者向け簡易マニュアル」や「Wi-Fi提供者向けセキュリティ対策の手引き」を改定**し、具体的なセキュリティ対策の事例を紹介する等、公衆無線LANサービスのセキュリティに関するさらなる周知・啓発を図る。

取組２　青少年を対象としたマニュアルの策定等

○　公衆無線LANサービスを利用する**青少年を対象としたセキュリティ対策の利用マニュアルを新たに策定**し、周知・啓発を図る。

○　**「国民のための情報セキュリティサイト」のコンテンツの充実**を図る。

取組３　オンライン教育等を活用した周知・教育等

○　**オンライン教育等**（例えば、放送大学や「gacco」）**の教育コンテンツを活用した**公衆無線LANの利活用やセキュリティに関する**周知・教育**を行う。

○　**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**公衆無線LANの利用に関する**周知・啓発等**を行う。

民間主体によるセキュアな公衆無線LANの取組

取組１　「公衆無線LAN版安全・安心マーク」制度の活用

○　インターネット接続サービス安全・安心マーク推進協議会による**「公衆無線LAN版安全・安心マーク」制度を活用したセキュアな公衆無線LANの普及**

→　現時点においては認知度が高いとは言えない状況にあるため、総務省（地方の総合通信局等を含む）においても　関係事業者団体の協力等を得ながら、「公衆無線LAN版安全・安心マーク」に関する周知・普及を図る。

一次審査（随時受付）

一般社団法人日本インターネットプロバイダー協会、
一般社団法人テレコムサービス協会、
一般社団法人電気通信事業者協会が審査項目に基づき実施。

二次審査（年３回実施）

安全･安心マーク審査委員会にて実施。

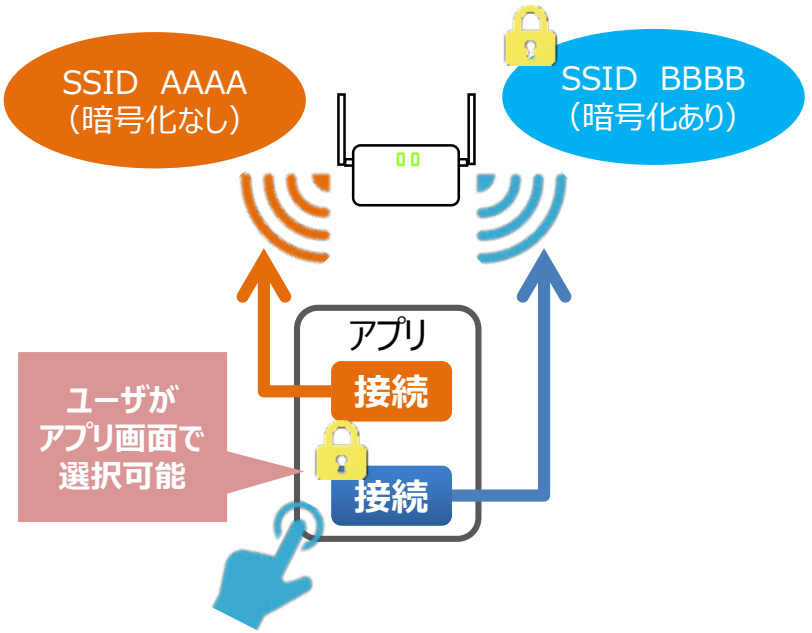
認定（有効期限は１年間）

Secured Wi-Fi

期限満了前に更新審査を実施し、合格した場合継続使用可能。

取組２　選択式のセキュリティ機能の提供

○　提供者が無線区間の暗号化を行っていない従来の無料の公衆無線LANサービスに加え、**新たに無線区間の暗号化に対応した公衆無線LANサービスを提供**することで、**利用者は暗号化あり／なしのサービスを選択**



データ利活用と連携したセキュアな公衆無線LANサービスの普及

取組１　利用者にとって利用しやすいアプリの促進

○　利用者にとって利用しやすいアプリの提供を促進することによるセキュアな公衆無線LANサービスの普及

→　公衆無線LANに接続することだけを目的としたアプリではなく、**さまざまなコンテンツサービスのアプリの機能と連携を図る。**

取組２　IoTおもてなしクラウドとの連携

○　公衆無線LANサービスとIoTおもてなしクラウドを連携することにより、例えば、**IoTおもてなしクラウドに登録された利用者の属性情報を当該利用者の許諾を前提として、公衆無線LANの認証に用いる。**

優良事例となるセキュアな公衆無線LAN環境の普及

取組１　自治体におけるセキュアな公衆無線LANの環境整備

○　総務省では、**引き続き、公衆無線LAN環境整備支援事業を行う。**

→　**こうした事業等を通じて優良事例を創出**し、自治体におけるセキュアな公衆無線LAN環境の整備を進める。その際には、例えば、**各地の優良事例を調査・公表するほか、これを踏まえ、所要の政策支援を行う**など、セキュアな公衆無線LAN環境の普及を促進する取組を行う。

取組２　東京オリンピック・パラリンピック競技大会に向けた環境整備

○　オリンピック・パラリンピック競技大会等の大規模イベントの開催時、公共施設やスタジアム等においては、悪意のある者に偽アクセスポイントを設置されるおそれがある。2020年に開催される東京オリンピック・パラリンピック競技大会に向けて、**開催地（東京等）となる自治体等において、セキュリティに配慮した公衆無線LAN環境を構築**する。

→　総務省では、「競技会場におけるICT利活用促進事業」を実施することとしており、こうした事業を通じて、**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環境を整備。**また、民間事業者等における取組として、優良事例となるセキュアな公衆無線LAN環境を実現するデジタルスタジアムを整備し、これを優良事例として全国に横展開する取組も期待される。

ご清聴ありがとうございました