参考資料

第1回公衆無線LANセキュリティ分科会
（平成29年11月24日）資料1－2

公衆無線LANのセキュリティの現状について

平成29年11月

公衆無線LANの概要

○　公衆無線LANは、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

（※）　出典：「カシマスタジアムに高密度Wi-Fiを導入…22日のセビージャ戦から各種サービスを開始へ」
https://www.soccer-king.jp/news/japan/jl/20170721/615811.html

Wi-Fiとは

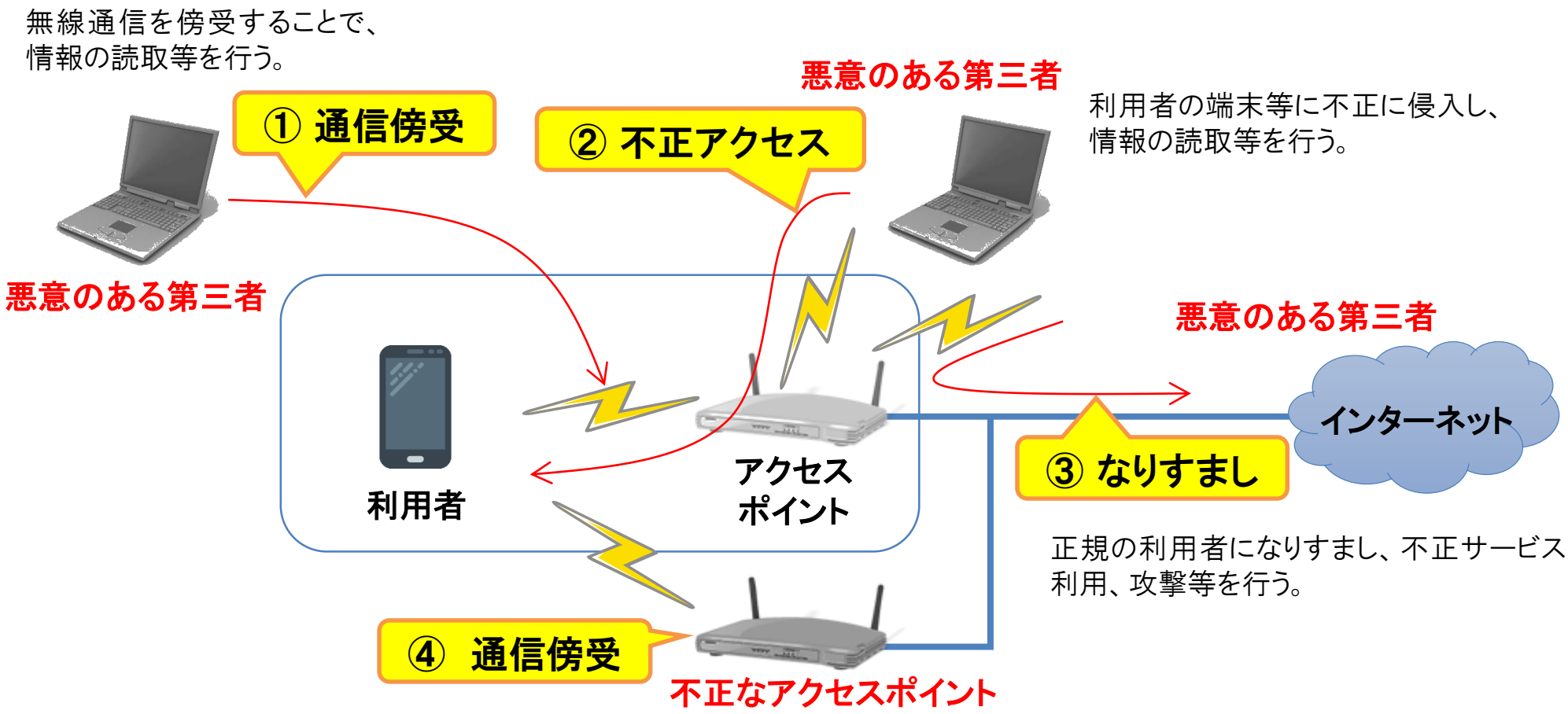
○　無線LAN技術の推進団体であるWi-Fi Allianceによる相互接続性の認定テストによって、一定レベルの相互運用性を保証されているもの

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 無線区間における通信傍受、② 他の端末からの不正アクセス、③ 利用者のなりすまし、④ 不正なアクセスポイントによる通信傍受等が知られている。

○ 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。

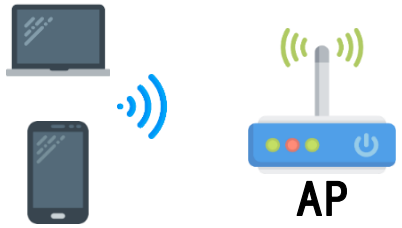


無線LANのセキュリティ対策：認証

○　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。

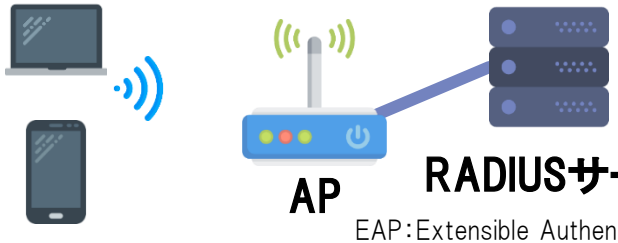
PSK方式（パーソナル）



APに設定されているパスワードと、利用者が入力したパスワード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

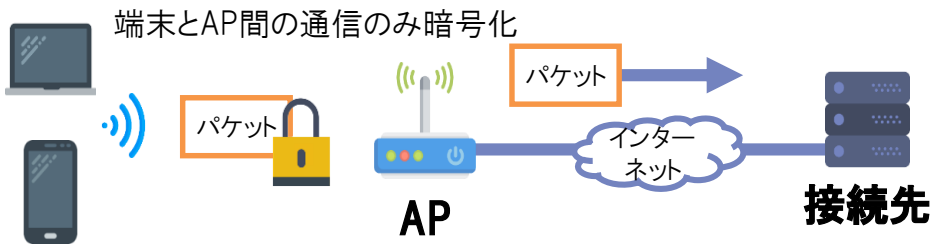
	認証方式	認証サーバの要否	端末側の認証	アクセスポイント側の認証	特徴
パーソナル	PSK	不要	ID・パスワード	-	利用者がID・パスワードを入力する。
エンタープライズ	EAP-TLS	必要	電子証明書	電子証明書	セキュリティ強度は高いが、各端末で電子証明書を管理する必要がある。
	EAP-TTLS	必要	ID・パスワード	電子証明書	端末側の認証をID・パスワードとすることで、EAP-TLSの煩雑さに対処したもの。
	EAP-SIM/AKA	必要	SIM/USIM	乱数	SIM/USIMカードが挿入されている端末は、自動で認証される。

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

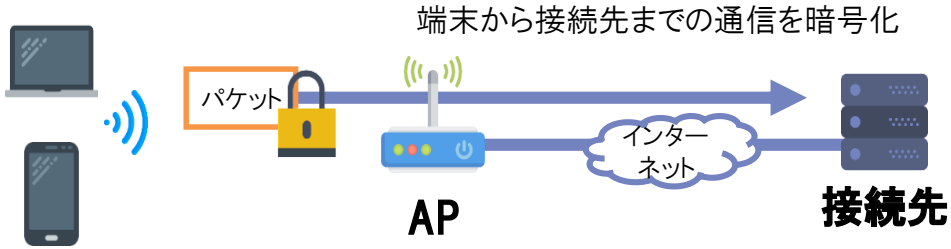
- ○ 暗号化とは、通信の内容を容易に推定できないようにする仕組みであり、通信の内容を秘匿化するもの。
- ○ 無線区間におけるネットワーク層の様々な暗号化方式には、既に脆弱性が発見されているものもあり、利用にあわせて適切な強度の暗号化方式を設定することが望ましい。
- ○ HTTPSやVPNといった、より上位層における暗号化方式を用いて、通信の内容を秘匿することもできる。

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	○ 鍵管理の方法にTKIPを採用し、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CCMPを採用。 ○ 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	○ パケット全体を暗号化して通信する。

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

公衆無線LANにおけるセキュリティリスクへの対応

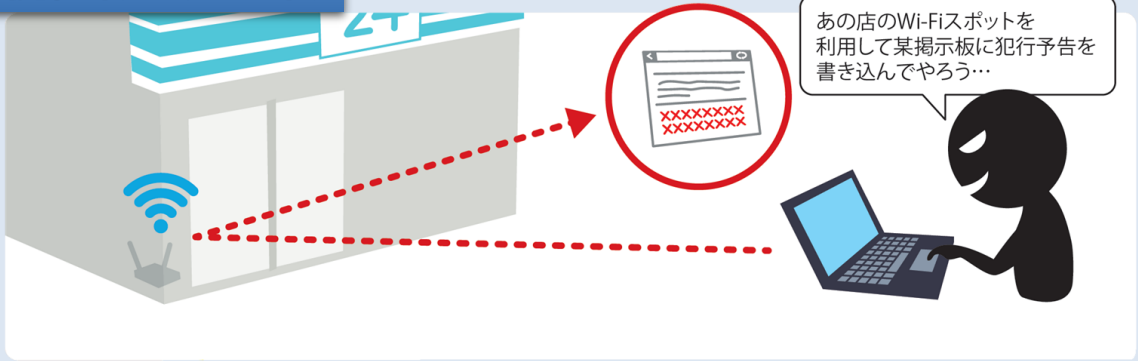
○　公衆無線LANは誰でも接続できるという利便性を有する一方、様々なセキュリティリスクが存在。

○　端末やアクセスポイントの正当性を検証する認証や通信内容の暗号化等を適切に行うことにより、公衆無線LANにおけるリスクを軽減することができる。

利用者のリスク例

○　Wi-Fi利用者の通信内容が盗聴され、IDや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

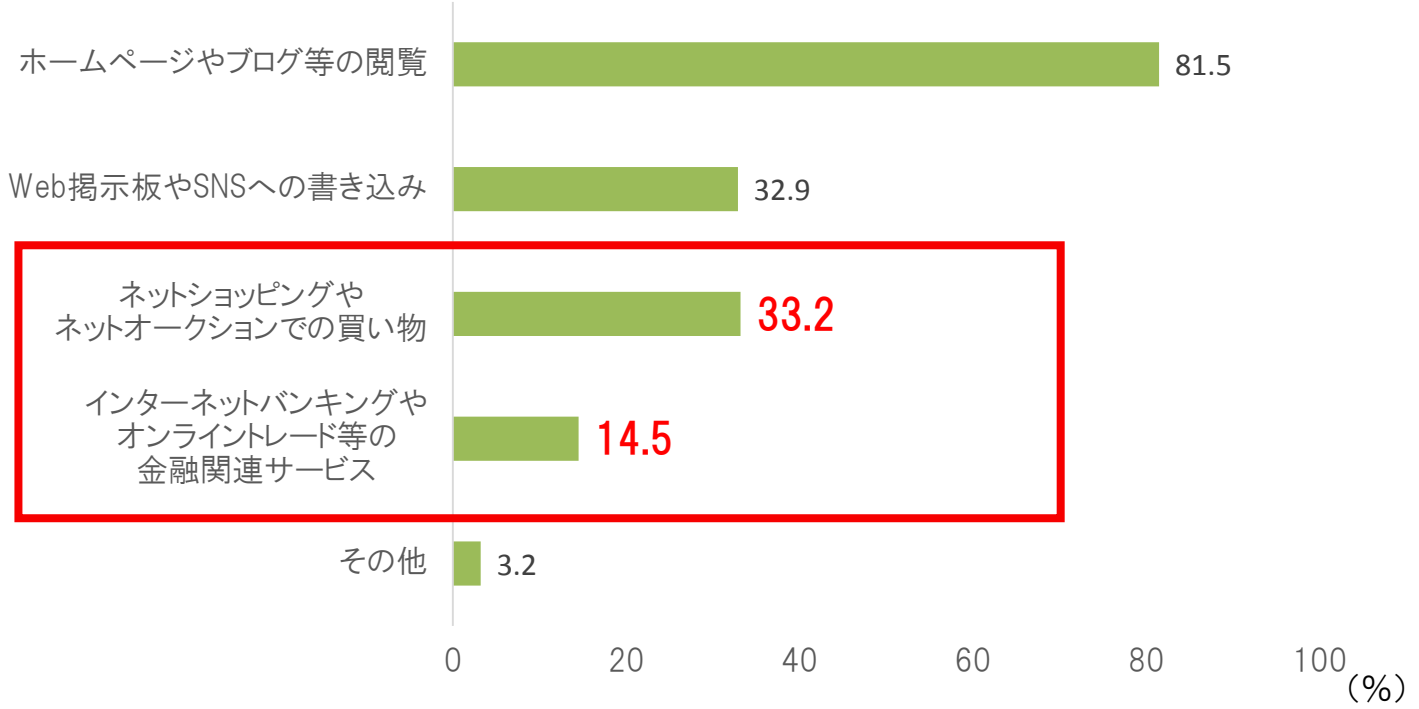
出典：「Wi-Fi提供者向けセキュリティ対策の手引き」（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_manual_for_AP.pdf

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。
- 上位レイヤで暗号化を行うSSL/TLS通信においても、様々な脆弱性が発見されている。

【最近の脆弱性の例(括弧内は発見年)】 BEAST & CRIME(2011年)、Lucky 13(2013年)、POODLE(2014年)、Heartbleed(2014年)

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)



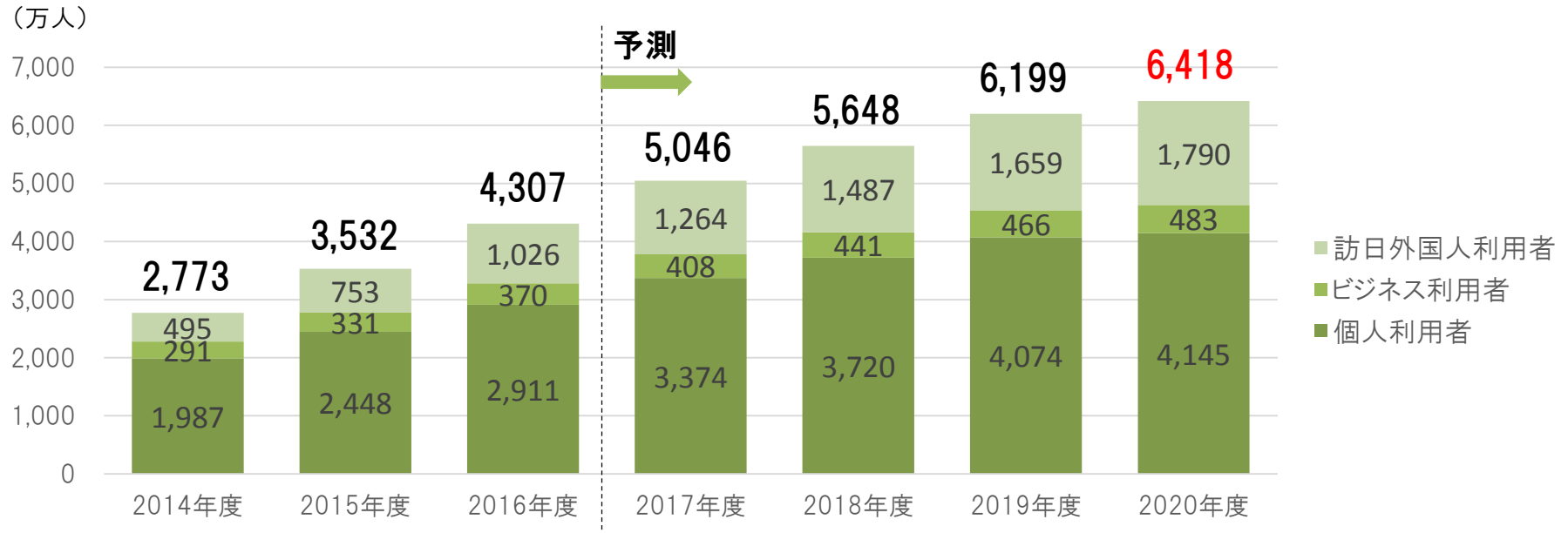
出典:「2016年度情報セキュリティの脅威に対する意識調査」(情報処理推進機構)
https://www.ipa.go.jp/security/fy28/reports/ishiki/index.html

公衆無線LANの普及状況

○　公衆無線LANは、携帯電話のオフロード対策から、観光・防災等、街づくりに不可欠な社会基盤へと進化し、利用者数は増加傾向。2020年の利用者は、約6,400万人と予測されている。

○　近年、空港、駅、ホテル、飲食店等が導入する事例が多く見られ、地方公共団体においても、地域活性化のツールとして、公衆無線LANの整備が進んでいる。また、外国人観光客にとっても、利用できる場所が十分あることが重要であり、今後、さらなる整備が求められる。

公衆無線LANサービスの利用者数の予測



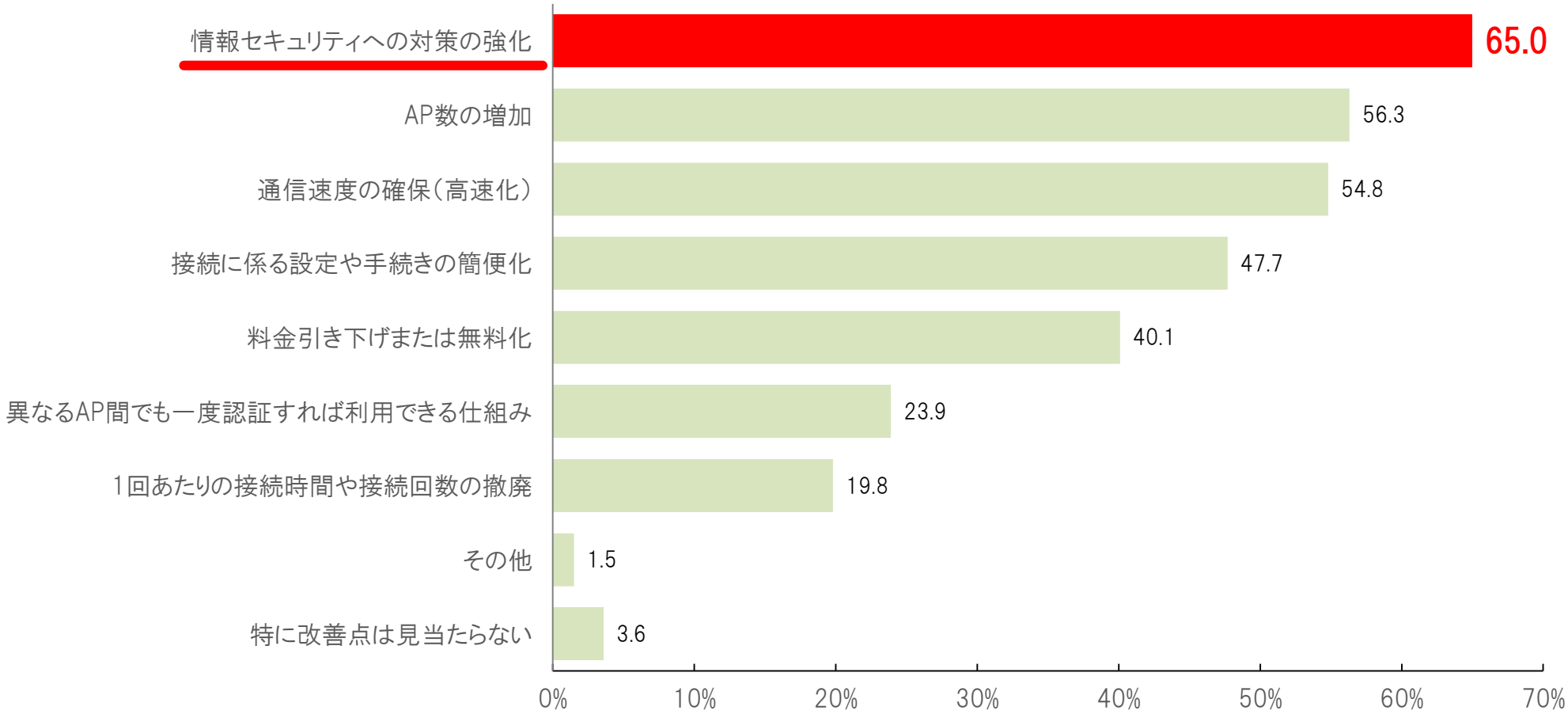
（注1）　日本在住の個人・ビジネス利用者は、各年度末の利用者数。2017年度以降は予測値。
（注2）　日本在住の個人・ビジネス利用者の定義は、1か月に1回以上利用するアクティブユーザー。
（注3）　訪日外国人利用者の定義は、訪日時に1回以上利用したユーザーの年間合計数。

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

公衆無線LAN利用におけるセキュリティに対する意識①

○　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）



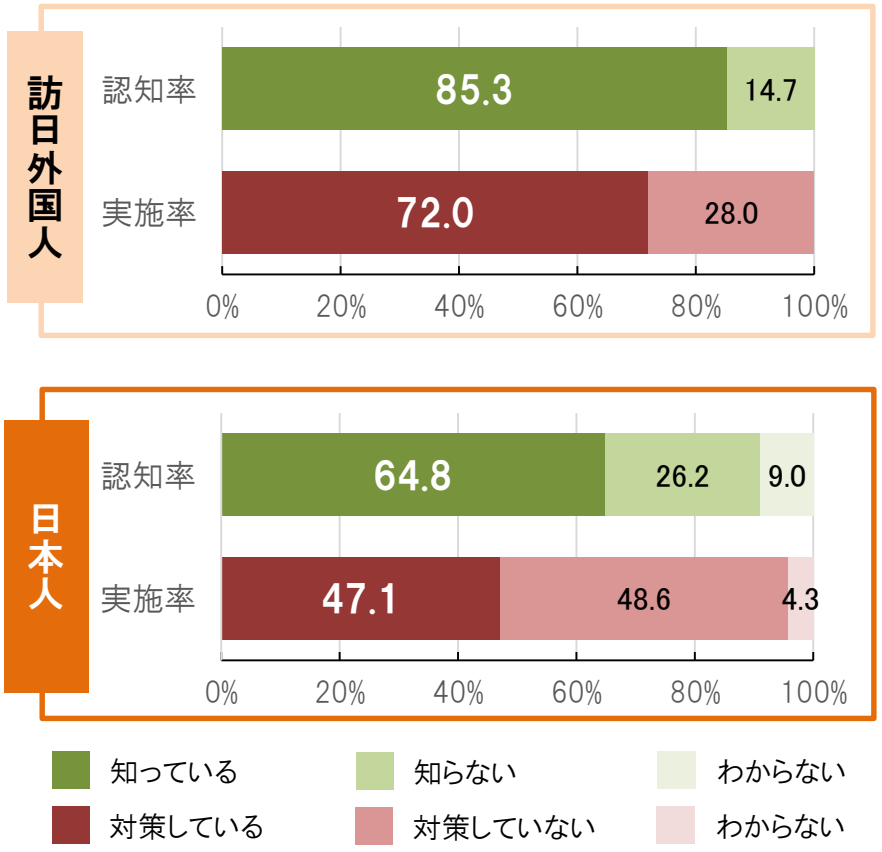
出典：「公衆無線LAN利用に関する情報セキュリティ意識調査結果」（総務省）
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000091.html

公衆無線LAN利用におけるセキュリティに対する意識②

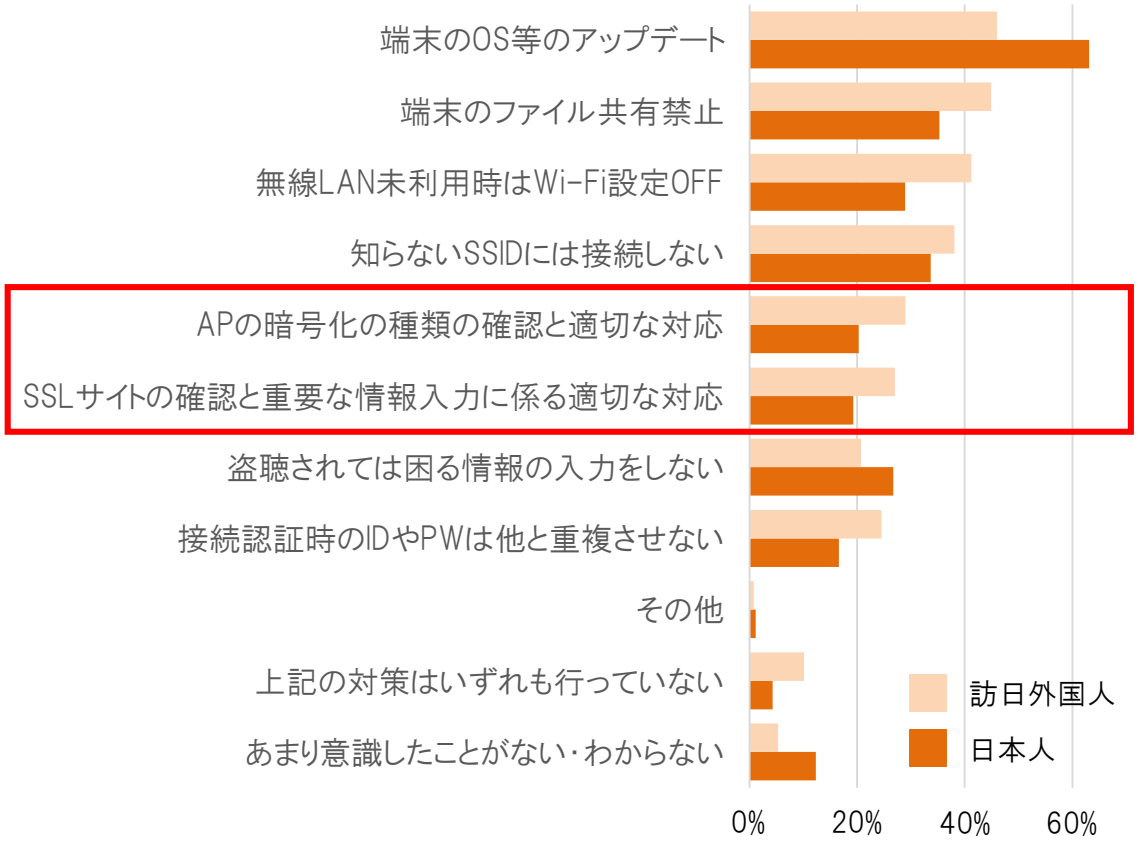
○ 公衆無線LAN利用時の脅威について、一定の認知はされているものの、セキュリティ対策の実施については低い傾向。特に、日本人についてその傾向が強い。

○ また、「AP（アクセスポイント）の暗号化の種類の確認と適切な対応」や「SSLサイト（HTTPS）の確認と重要な情報入力に係る適切な対応」といった暗号化に関するセキュリティ対策は、十分に実施されているとは言い難い。

公衆無線LAN利用時の脅威の認知率とセキュリティ対策の実施率



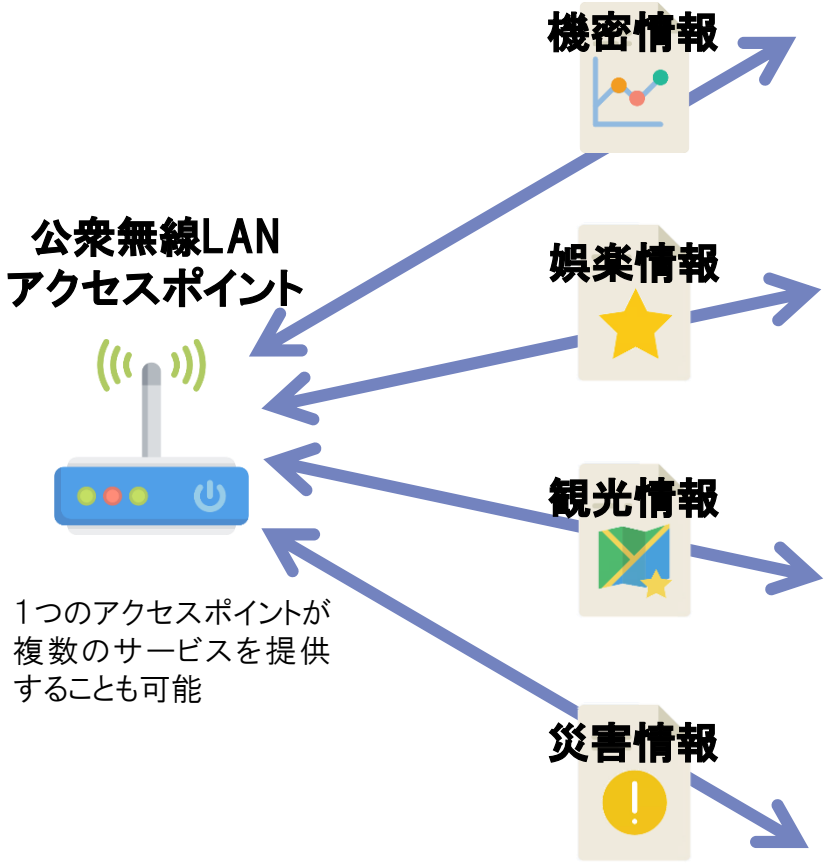
公衆無線LAN利用時に実施しているセキュリティ対策



出典：「平成26年度Wi-Fi利用に係る調査結果」（総務省）
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/cmn/wi-fi/Wi-Fi_security_survey26.pdf

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と考えられる。
○ 他方、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。



テレワーカー

顧客情報等の機微な電子データをやりとりする可能性がある

若年層

通信料や通信速度の観点から、大容量・高速なサービスを必要とする

観光客

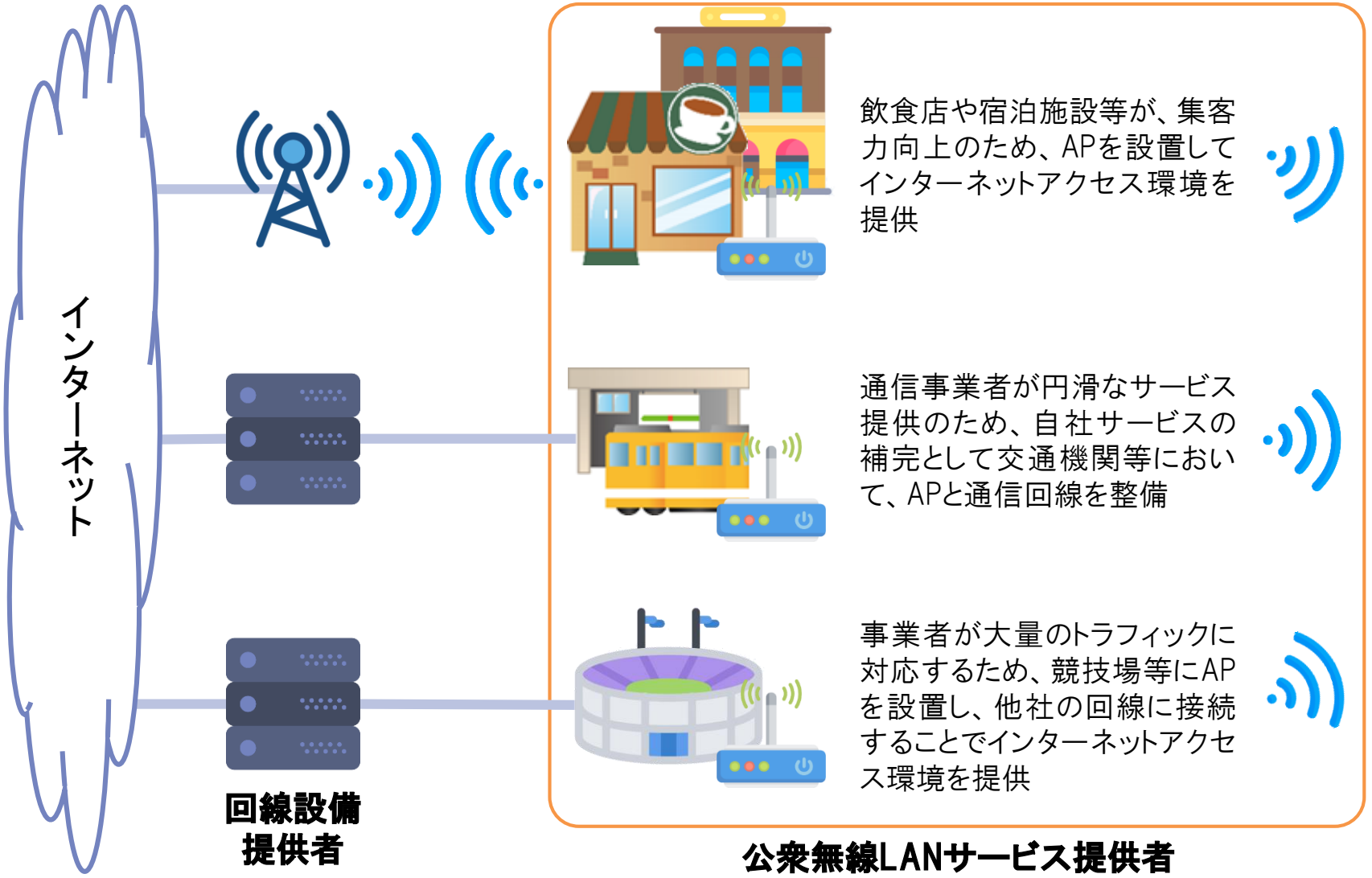
情報へのアクセスしやすさが求められる

災害時

情報が付近の利用者へ、迅速に漏れなく伝達されることが望ましい

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。



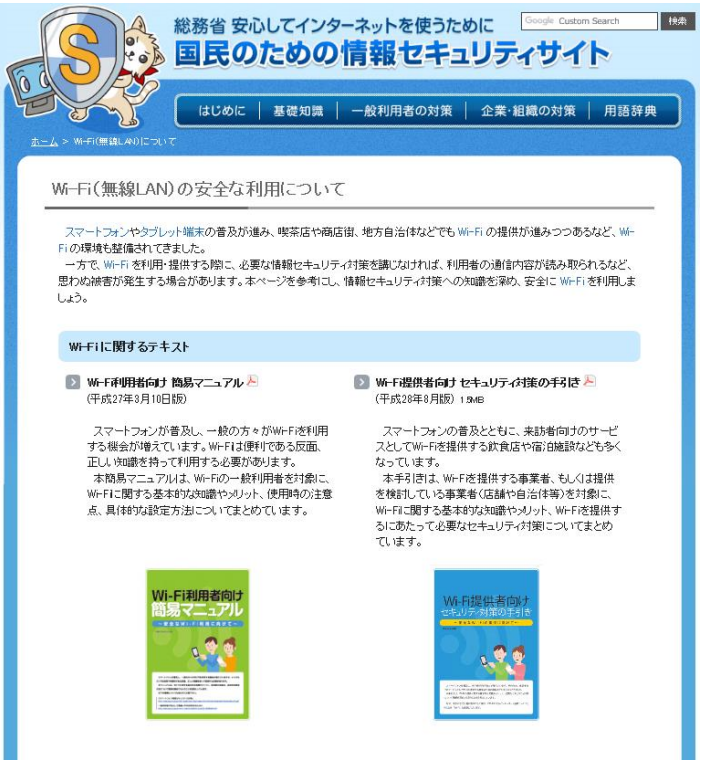
（参考） 総務省における無線LANのセキュリティに対する取組

○ 総務省は、 Wi-Fi(無線LAN)の安全な利用について「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」等を作成し、周知啓発を実施。国民のための情報セキュリティサイトにも掲載。

Wi-Fi利用者向け
簡易マニュアル
（平成26年4月策定）
（平成27年3月改定）

Wi-Fi提供者向け
セキュリティ対策の手引き
（平成26年4月策定）
（平成28年8月改定）

国民のための
情報セキュリティサイト
にも掲載



出典：国民のための情報セキュリティサイト
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html