埼玉サイバーセキュリティ推進会議（事務局：埼玉県警察本部生活安全部サイバー犯罪対策課）

S．C．S．C通信

H30．8．8
NO．50

★公衆無線LANのセキュリティ脅威★

急速に整備が進む公衆無線LANですが、セキュリティの脅威及びその対策について掲載しますので、サイバーセキュリティ対策の参考にして下さい。

公衆無線LANの急速な整備

無線LANは、ノートパソコン、タブレット端末、スマートフォンなどで利用する無線によるネットワーク接続のことです。その中でも商業施設、公共交通機関、店舗など、多くの人が利用できる場所に設置されているものを公衆無線LANといいます。

公衆無線LANは、Wi-Fiスポットとも呼ばれ、2020年東京オリンピック・パラリンピック開催を見据えて観光立国を推進する観点から、国内で急速に整備が進んでおり、近年は、大規模災害時における複数の通信手段確保の一環として地方公共団体などの公共施設にも公衆無線LANが導入されています。

公衆無線LANは、便利である反面、設置者のセキュリティ対策に差があるため、情報漏えいなどの危険性や犯罪行為に利用されることもあります。**※Wi-Fiは、無線LANの標準規格「IEEE802.11シリーズ」に接続保障されたものの総称**

公衆無線LANの主な脅威

〇盗聴

接続先の無線LAN（アクセスポイント）が暗号化されていない場合、接続元の機器（スマートフォンなど）との通信を第三者に盗聴される危険性があります。

無線LANの暗号化方式は、強度の順にAES、TKIP、WEPといった方式がありますが、WEPによる暗号化は既に解読されており、WEPの暗号化解析ソフトがインターネット上に出回っています。

〇悪意のAP（アクセスポイント）

通信内容の窃取などを目的として、第三者が悪意をもって、実在する正規のAPと同じ設定の無線LANを設置したもので、利用者が誤って接続した場合、通信内容を第三者に知られてしまう危険性があります。

〇なりすまし

盗聴などの手口により、第三者が不正に情報を入手し、正規の利用者のアカウント情報を悪用したり、機器情報を偽装することで、正規の利用者や機器になりすまして不正にサービスを利用される危険性があります。

〇不正利用

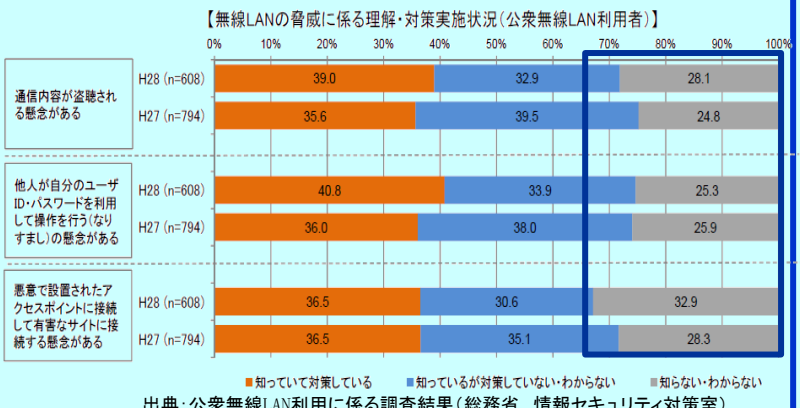
掲示板への犯行予告の書き込みや違法ダウンロードなど、公衆無線LANが犯罪に悪用されるおそれがあります。

無線LANの脅威への対策の実施状況

総務省が実施したH28年度のアンケートによると、無線LANの脅威を知らない利用者が増加しているとのことです。

無線LANの整備が進む中、こうしたアンケート結果を踏まえると、今後盗聴等の被害が増加する可能性があります。

そのため、設置者は、利用者が少しでも安心して利用できるセキュリティ対策を行うとともに、利用者に対しては、各種脅威及びセキュリティの重要性を周知していくことが重要です。



出典：公衆無線LAN利用に係る調査結果（総務省　情報セキュリティ対策室）

利用者及び設置者の被害防止対策

〇利用者

・接続先が暗号化されているものを極力使用する。
・ネットバンキングや、オンラインショッピングなど、カード情報、個人情報を入力するサイトの利用は危険性があることを認識する。

〇設置者及び今後公衆無線LANの設置を検討している企業・自治体

・機器の初期パスワードは使用せず、必ず変更をする。
・機器のファームウェア更新を適宜行い脆弱性対策を行う。
・端末認証の導入や防犯カメラの設置、通信の暗号化などセキュリティ対策の検討を行う。

STOP 立ち止まる | THINK 考える | CONNECT™ 楽しむ