

メディア

無線LANの利用 個人情報漏れ注意

グーグル問題で表面化

総務省は先月、米インターネット検索大手のグーグルが昨年5月まで、無線LAN経由で個人の通信データを収集していたとして、再発防止策を報告するよう文書で指導した。同社は誤って収集していたとするが、第三者にデータが流出しやすい無線LANの危険性が浮き彫りになった。利用方法によってはメールやパスワードなどの個人情報が他人に見られる危険性がある。

【岡礼子】

◆世界で問題に

住所を打ち込むだけで町並みの画像がインターネットで見られるグーグルの人気サービス「ストリートビュー」。同社はこのサービス向けの撮影車で、無線LANの電波を利用して位置情報を収集。別のサービスの精度向上に役立てていた。ところが、暗号で保護されていない通信本文(ペイロードデータ)も誤って収集していたことが判明、昨年5月に公表して謝罪した。

日本を含む34カ国・地域で、収集地点で送信されたメール本文や、ID、パス

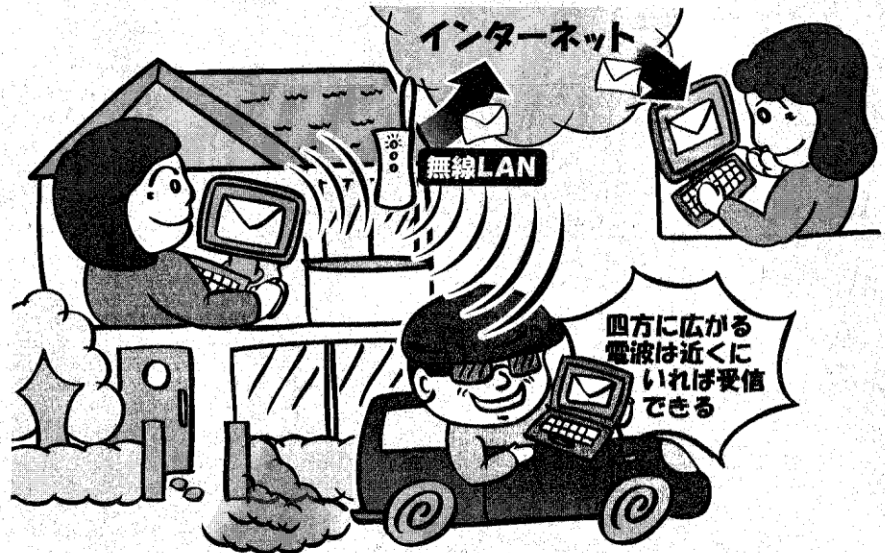
ワードなどの情報が含まれていた可能性があるという。韓国警察庁がグーグルコリアを家宅捜索するなど、各国で問題になり、無線LANデータの収集について調査を求める国が相次いだ。グーグルは撮影車による収集をやめ、昨秋、研修強化などの防止策を発表。今年11月には位置情報サービスに無線LANのアクセスポイント情報を使うことを拒否できる仕組みを導入した。

日本でも07年12月から通信を受信し、その一部を記録していたが、「閲覧、使用はしていない」とする。総務省は電気通信事業法

(4条)の「通信の秘密」を侵害するおそれがあったとして先月11日、同社に対して該当する記録の削除と再発防止策を早期に実施し

誰でも傍受が可能

グーグルが収集していた無線LANの基地局情報は、スマートフォン(多機能携帯電話)向けの「位置情報」を使ったソフトなどにも利用されている。現在



え・菅野庸平

地からの道案内や紛失した端末を探すサービスなどは人気。位置を特定するのにGPS(全地球測位システム)や通信各社の携帯電話

用基地局情報が使われるが、それだけでは精度が保てないため、個人が使っている無線LANの情報なども併用されることがある。電波は10〜100メートル

ため、その範囲内では誰でも電波の受信が可能だ。さらに、使っている機器の種類、通信速度、暗号化の方式などと同時に、通常は通

信内容も記録されてしま
う。データは断片化されて
おり、通常は暗号化されて
いるため、そのままで意味
を読み取ることができな
い。

しかし、森井昌克・神戸
大学教授(情報通信工学)

によると、暗号化されてい
ないデータを読める形に
「復元」するツールはネ
ット上で無料で公開され
ており、「無線LANに接
続できるパソコンがあれば
可能で、特別な装置は
必要ない」という。メール
の送信先、内容、閲覧して
いるウェブサイトなど、他
人がインターネットで送
受信している内容は、いわ
ば、誰でも「傍受」できる
状況といえる。

①自宅でも外出先でも、セキュリティ確認

市販の無線LANルーターは購入時点に、どのような暗号
化機能があるか確認する。外出先でも注意が必要。セキュリ
ティーがかかっていないネットワークに自動で接続してしま
う場合がある。

②URLが「https」で始まるウェブサイトを使う

通常のホームページのURLが「http」で始まるのに対し、
「https」で始まるサイトは、暗号化されており安心。

③複数のサービスで、同じパスワードを使わない

オンラインショッピングや、会員制交流サイト、メールサ
ービスなど、複数のサービスを使う場合、異なるパスワード
を使用する。

④重要な情報は別の認証システムで

ID、パスワード以外にデジタル証明書を発行したり、乱数
表などその場限りのパスワードを使う方法がある。オンライ
ンショッピングなどは別認証を採用したサイトを。

⑤たえず安全対策をアップデート

パソコンの基本的な安全対策を欠かさない。スマートフォ
ンやタブレット型端末で通信事業者以外が製造したアプリケ
ーションを使う場合には、端末内のどのような情報を利用す
るか、確認する。

◆無線LAN「安全使用」の5カ条

また、暗号規格の一つ、
「WEP」は簡単に解読で
きることがすでに分かっ
ている。最新の機種は「W
PA」など新しい暗号方式を
使うが、古い機器の中には
WEPしか使えないものが
ある。

電波法では、無線通信を
傍受すること自体は法律違
反にならないが、「その存
在性」は内容を漏らし、
またはこれを窃用(通信内
容を窺って、何か行動を起
すこと)することは禁止

スマートフォンも

あるインターネットブラ
ウザー向けに昨年、暗号化
されていない無線LANを
通してログイン状態を管理
する情報を盗むツールが公
開された。このツールを使

ている。森井教授は「無線
LANは簡単に傍受されて
プライバシーが侵されるだ
けでなく、成りすまして不
正メールを送ることなども
可能で、危険性が高い。必
ず暗号化し、推定されなく
いパスワードにすること
が、安全に使うためには必
要だ」と警告する。自分が
被害を受けるだけでなく、
第三者によって犯罪に利用
され、たどるとはサイバー犯
罪などに加担したとみなさ
れる可能性もあるのだ。

うと、同じ無線LANを使
っているパソコンが接続し
ているサイトを、近くで同
じように閲覧したり、本人
に成りすまして使うことが
できる。例えばSNS(ソ
シャル・ネットワークキン
グ・サービス)に投稿したり、
オンラインショッピングサ
イトで買い物することも可
能になる。このツールは世
界で約190万人がダウン
ロードしたとみられる。

メール暗号化サービスZ
enlock(ゼンロック、
東京都渋谷区)のアミール
・アヤロン社長は「カフェ
で、近くでパソコンを使っ
ている人の情報を盗むこと
が簡単にできてしまう」と
指摘する。また、無線LAN
N基地局を偽装し、接続し
たパソコンのパスワードな
どを盗むツールまで公開さ
れている。

大人気のスマートフォン
でも注意が必要だ。スマー
トフォンには、無線LAN
通信の基地局があると自動
的に接続する機能があり、
事前に設定しておかないと
暗号化されていない通信に
接続して気づかないケース
があるためだ。「無線」で
ネットを利用する際には細
心の注意と対策が必要だ
別項参照。アヤロン社長は
「非常に簡単に使える解読
ツールが無料公開されてい
る。WEPなら1分程度で
解けてしまう。侵入されて
も気づかない人が多く、表
面化することは少ない」と
指摘している。