ZDNet Japan

Wi-Fiのセキュリティ事情

- WPA2の脆弱性「KRACKs」公開、多数の Wi-Fi 機器に影響の恐れ
- MWC 開催のバルセロナで公衆Wi-Fi を使ったハック実験
  -- セキュリティ企業が危険性を指摘
- Wi-Fi にありがちな 5つの致命的ミス
- 中国の無線LAN セキュリティ事情の今

ZDNet Japan

Wi-Fiのセキュリティ事情

WPA2の脆弱性「KRACKs」公開、多数のWi-Fi機器に影響の恐れ

Wi-Fi認証の「Wi-Fi Protected Access II」（WPA2）に関する脆弱性の詳細な情報が10月16日、特設サイトで公開された。脆弱性は全部で10件あり、この脆弱性には「KRACKs」（key reinstallation attacks：鍵再インストール攻撃）という通称が与えられた。

情報を公開したベルギーのルーヴェン・カトリック大学のセキュリティ研究者、Mathy Vanhoef氏によると、一連の脆弱性はクライアント機器がWi-Fiのアクセスポイント（AP）と接続する際における「4ウェイ・ハンドシェイク」という処理に起因する。

4ウェイ・ハンドシェイクでは、クライアント機器がAPとの間で暗号化通信を行うために、認証や暗号鍵などに関するメッセージを複数やりとりする。その際にメッセージが失われたり、削除されたりする場合があり、APからクライアントに対してメッセージを再送信する。この時、クライアントが受信する暗号鍵が再インストールされ、やりとりしたパケットなどの情報がリセットされる。

攻撃者は、この仕組みを悪用して細工したメッセージを送り付ける手法などにより、暗号化されたパケットを復号して内容を盗聴したり、攻撃コードを埋め込んだり、ユーザーを不正サイトに誘導したりするといった、さまざまな攻撃を実行可能だという。

WPA2は、現在のWi-Fi暗号化通信における認証でセキュリティレベルが高いとされていることから、世界中で広く利用されている。Vanhoef氏は、この問題がWPA2の仕様によるものであり、個別の製品やその実装が原因ではないと解説。WPA2をサポートする大半の機器に影響が及ぶ可能性があり、WPA2が正しく実装された機器では影響を受ける可能性が高いという。

初期調査では、AndroidやLinux、Apple、Windows、OpenBSD、MediaTek、Linksysなどの製品で攻撃の影響を受けることが判明した。Vanhoef氏は、Android 6.0（Marshmallow）を搭載するデバイスで脆弱性の悪用を実証し、特にLinuxで広く普及しているWi-Fiクライアントの「wpa_supplicant」のバージョン2.4以上が致命的だと指摘。Android 6.0以降のバージョンは、Android全体の約41%を占めている。

脆弱性に関する情報は、今回の公表に先立って米US-CERTなどに提供され、8月下旬にUS-CERTからWi-Fi機器メーカーなどにも提供されている。脆弱性を修正するには、各メーカーが機器ごとに提供するパッチを適用しなければならないが、多くの機器で提供されるまでに、長い時間がかかるとみられる。

Vanhoef氏の見解では、現状でユーザーは、WPA2を介したWi-Fiの利用を慎重に行い、メーカーからパッチが提供されれば、速やかに適用すべきとしている。また今回、WPA2の危険性が指摘されたからといって、既にクラッキングが可能なWEPなど古い認証方式を利用すべきではないともアドバイスしている。

Vanhoef氏らの研究者グループは、脆弱性悪用の概念実証のためのスクリプトも公開している。Wi-Fi Allianceは16日、今回の脆弱性問題についてスクリプトを活用した脆弱性検査テストの準備を進めていることを明かし、機器メーカーらと協力して迅速に対処すると表明した。

こちらは、2017/10/16に公開された記事（https://japan.zdnet.com/article/35108859/）を再録したものです。仕様等は公開時点のものです。

ZDNet Japan

Wi-Fiのセキュリティ事情

MWC 開催のバルセロナで公衆Wi-Fiを使ったハック実験 -- セキュリティ企業が危険性を指摘

チェコのセキュリティベンダーであり、ウイルス対策製品を手がけている AVAST Software はスペインのバルセロナで開催中の「Mobile World Congress」（MWC）で現地時間 2 月 22 日、公共の場所で無料提供されているセキュアでない Wi-Fi アクセスポイントの危険性について警鐘を鳴らした。

セキュリティ事業を手掛ける AVAST は、同カンファレンスの参加者が数多く到着するバルセロナ空港で、複数の公開 Wi-Fi ネットワークを設置した。

同社の研究者らは、「Airport_Free_Wifi_AENA」（編集部注：「AENA」は Aeropuertos Españoles y Navegación Aérea（スペイン空港・航空管制公団）のこと）や、「MWC Free WiFi」「Starbucks」といった名前を用いてネットワークを設置した。するとわずか数時間のうちに2000人以上のユーザーが、このハニーポットネットワークに接続してきたという。

AVAST は以下の要点を伝えている。

- 50.1%は Apple 製品を使用し、43.4%は「Android」搭載機器を使用していた。
- 61.7%が Google 検索あるいは Gmail の電子メールにアクセスした。
- 14.9%が米 Yahoo にアクセスした。
- 2%が Spotify を利用した。
- 52.3%が Facebook アプリを、2.4%が Twitter アプリをインストールしていた。
- 1%がデートアプリ（Tinder または Badoo）を利用していた。

そして恐ろしいことに、63.5%で端末情報やユーザー情報を確認できた。

Avastのモバイル担当プレジデント Gagan Singh 氏は「オープンな Wi-Fi を使ってネットにアクセスすることは危険を伴うことを多くの人が承知している。しかし、このように認識していても、設定を変えない限り Wi-Fi ネットワークに端末が自動接続する可能性があることを理解していない人がいる」と述べる。

Singh 氏は接続にパスワードが求められるアクセスポイントのほうが安全であり、（Hotspot Shield のように）VPN サービスの一部では身元をマスクすることが可能で、プライバシーが守られるとしている。

ZDNet Japan

Wi-Fiのセキュリティ事情

Wi-Fi にありがちな 5つの致命的ミス

誰もが常に 1 台以上の Wi-Fi 対応デバイスを持ち歩くようになりました。Cisco Systems の 2016 年 VNI レポートによると、2021 年までに世界中で 5 億 4000 万を超える公共ホットスポットが提供され、スマートデバイスをサポートするようになる見込みです。ほとんどの商業施設や小売店舗が既に、来店客への信頼性の高い Wi-Fi ネットワークの提供をビジネスの基本コストと考えるようになっています。ただし、Wi-Fi をインターネット接続のための単なるツールと考えるべきではありません。無線ネットワークを設置してただ放置するだけではなく、そのメリットを最大限に活用することをお勧めします。

商業施設が来店客に無料 Wi-Fi を提供する際に犯しやすい代表的なミスを、以下にご紹介します。

1. スプラッシュページやキャプティブポータルがない

ゲスト用 Wi-Fi ネットワークを設定する際は、スプラッシュページやキャプティブポータルを忘れずに有効してください。「ここをクリックして利用規約に同意」といった、ありきたりのメッセージのページが表示されるだけで、すぐに無料 Wi-Fi を利用できるようになる例が多く見受けられます。このような方法では、来店客がメッセージを読まずにインターネットに簡単にアクセスできるようになりますが、既存や新規の顧客の貴重な情報を何も手に入れることができません。

カスタマイズ可能なスプラッシュページやキャプティブポータルを使えば、無料インターネットアクセスの提供と引き換えに、メールアドレス、携帯番号、SNS アカウントなどの貴重な顧客情報を収集できます。そして、このようなプロセスが、ターゲットを絞った販促活動を可能にし、カスタマーエンゲージメントを強化、つまり顧客との関係性を強化することができます。また、Facebook、Twitter、Instagram などの主要 SNS を認証で使えるようにすれば、出身地、出身校、購買行動の傾向などさらに多くの有益な情報を得られる可能性もあります。

最低限の情報として、性別や年齢などの基本的な人口統計データを Wi-Fi ネットワークアクセスページに入力してもらうようにするべきでしょう。

2. 顧客を犯罪やハッキングのリスクに晒している

サイバーセキュリティのベストプラクティスに従わないのは、どのような組織にとっても危険な行為であり、大きな損害を被る可能性があります。公共 Wi-Fi ホットスポットはハッカーにとって、獲物を手に入れる格好の場所です。ハッカーにとってみれば、セキュリティ保護が適切でない Wi-Fi 環境で、来店客のメールの認証情報やクレジットカード番号などの機密情報や個人情報を手に入れるのは、容易なことです。しかしながら、Wi-Fi セキュリティは、来店客だけを保護するものではありません。自らのブランドを保護する重要な方法でもあるのです。

具体的には、どのような方法で Wi-Fi セキュリティが実現すればよいのでしょうか。ワイヤレス不正侵入防止システム（WIPS）は、サイバースヌーピングから Wi-Fi

こちらは、2017/09/06 に公開された記事（https://japan.zdnet.com/article/35106545/）を再録したものです。仕様等は公開時点のものです。

ZDNet Japan

Wi-Fiのセキュリティ事情

ネットワークを保護する目的で広く利用されている無線ネットワークセキュリティソリューションです。問題は、これらのソリューションの多くが高価であり、無線環境内のハッカーを発見してブロックするのは比較的容易ではあるものの、ほとんどの WIPS ソリューションが本当に悪意のあるデバイス、アクセスポイント（AP）と近くの店舗で使われている正規の AP を確実に区別できない点にあります。この誤検知の問題によって、WIPS が近くにある無害のデバイスや AP を誤って排除してしまう恐れがあり、そのような状況が発生すると、組織の評判が悪化し、法的責任を問われる可能性もあります。そのため、このようなリスクを避けて、WIPS の対策機能を無効にしている企業も少なくありません。

朗報と言えるのは、エンタープライズグレードの Wi-Fi セキュリティソリューションが、資金の潤沢な大企業だけのものではなくなったこと、そして、WIPS の誤検出を実質的に排除できる新たなテクノロジが登場したことでしょう。接続されたデバイスと AP を自動的かつ正確に承認済み、外部、または不正のいずれかに分類して、その分類に応じて処理できる WIPS を採用し、無線ネットワークと顧客を保護することをお勧めします。

また、小売業には、PCI（Payment Card Industry）と呼ばれる誰もが知っている業界標準が存在し、毎年の厳格化にもかかわらず、その規格を順守するよう求められています。しかしながら、規格を順守すれば顧客と店舗の双方のセキュリティが保証されるわけではありません。事実、無線ネットワークのセキュリティの保護に関する、ある PCI 規格で求められているのは、四半期に 1 回、不正 AP の定期スキャンを実行することだけです（90 日にたった 1 回です）。したがって、繰り返しになりますが、コンプライアンスは重要ではあるものの、同時に、WIPS の全機能を常に有効にしておくことが重要なのです。

3. ネット通販大手に売上を奪われる

実際の店舗がネット通販サイトのショールーム同然となってしまうことを防ぐには、どうすれば良いのでしょうか。さまざまなモバイルエンゲージメント技術を使えば、Wi-Fi ネットワークに接続した来店客とやり取りが可能になります。そして、このようなツールを使えば、スプラッシュページを離れた後もやり取りが可能になり、来店客ごとにカスタマイズしたカスタマーエクスペリエンスを提供できるようになります。

例えば、URL を読み取るツールを利用して、来店客が通販サイトの価格と比較した際に、Wi-Fi ネットワークでクーポン、割引コード、カスタマイズされたメッセージなどを提案することもできるでしょう。また、Wi-Fi ネットワークをチャネルとして利用して、SMS、MMS、ソーシャルネットワークなどの来店客が選択した方法で直接やり取りすることもできるでしょう。アンケートや投票を Wi-Fi で配信して、顧客の好みや意見を直接的かつ正確に測定･判断し、マーケティングやビジネスの戦略に反映させる方法も考えられます。

4.Wi-Fi のデータ分析機能を活用できていない

実店舗の来店客とウェブサイトの訪問客に大きな違いはありません。訪問のきっかけ、滞在時間、購入商品などの情報は、短期的･長期的な販売促進やビジネスの意思決定の重要な指標となる可能性があります。ところが、多くの場合に Wi-Fi ネットワークの分析ツールが有効活用されておらず、来店客の足取りや滞在時間などの店舗の最適化やレイアウトに役立つ指標を得られていないようです。無線ネットワークでは、パッシブスキャン、アクティブスキャン、Wi-Fi ネットワークの内部と

こちらは、2017/09/06 に公開された記事（https://japan.zdnet.com/article/35106545/）を再録したものです。仕様等は公開時点のものです。

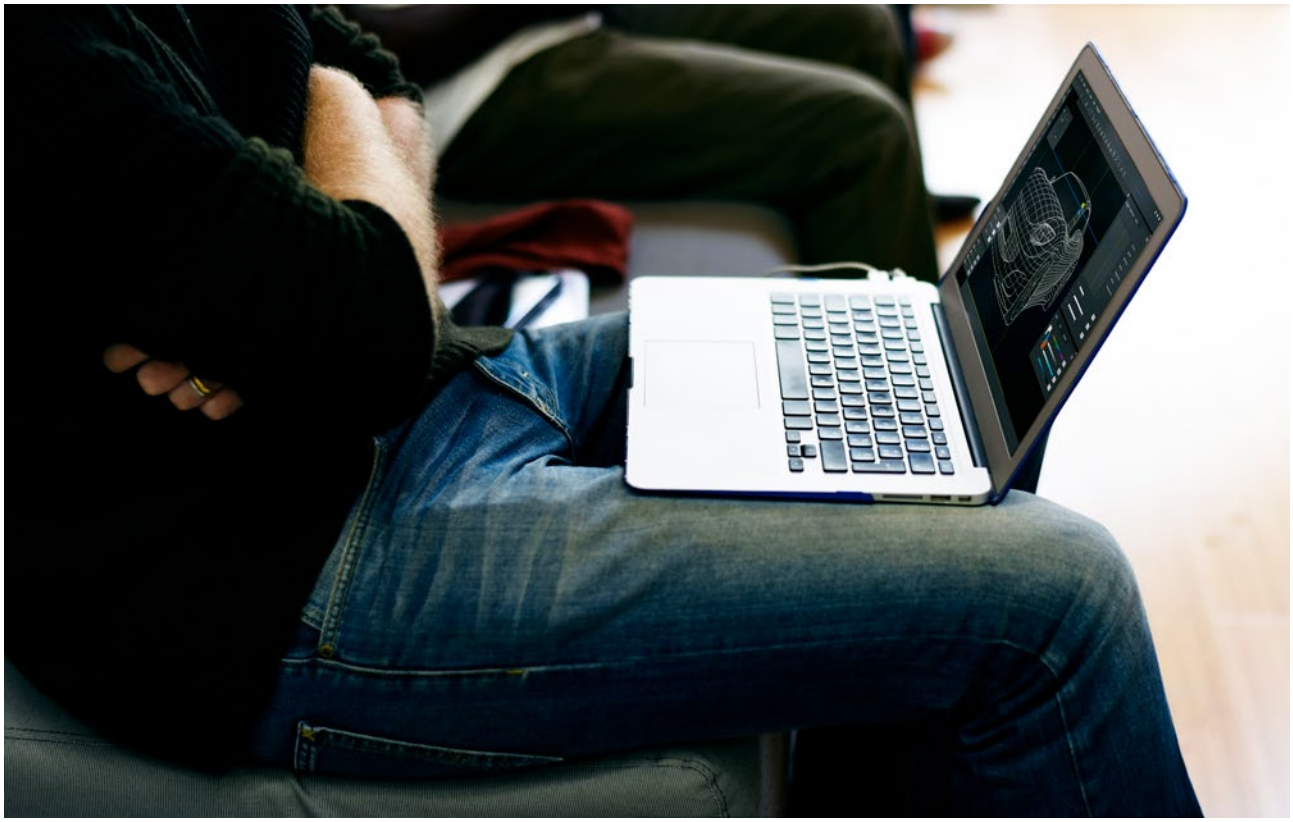
Wi-Fiのセキュリティ事情

周辺のユーザー接続から、膨大な顧客データを収集して利用することができます。これらのデータを正しく分析することで、Wi-Fi ユーザーのトラフィックパターン、行動、人口統計的データが明らかになり、店舗のフロアプランやサービスの最適化に役立てることができるでしょう。

5. 家族連れや子供にとってのインターネットの安全性が十分に考慮されていない

Wi-Fi 環境を利用する来店客をハッカーから保護するだけでなく、十分な予防措置を講じて、あらゆる年齢層の来店客が、不快なコンテンツを目にすることなく、快適にインターネットアクセスを楽しめるようにする必要があります。公共 Wi-Fi におけるインターネットの安全性と有害コンテンツの排除を目的とする「Friendly WiFi」という優れた団体があります。安全な Wi-Fi を提供していると認められた企業の施設や店舗には、Friendly Wi-Fi マークが目印として表示されています。

Wi-Fi には、良くも悪くも、ビジネスを大転換させる力があります。適切な保護無しに Wi-Fi 環境を提供してしまうと、ゲスト用 Wi-Fi ネットワークから顧客の個人情報がハッカーによって外部に持ち出されてしまう可能性があります。その反対に Wi-Fi ネットワークを適切に保護し、それを正しく活用すれば、安全で効率的なオンライン環境というメリットお客様にもたらされるだけでなく、顧客満足度と売上の向上という企業側のメリットにもつながります。



こちらは、2017/09/06 に公開された記事（https://japan.zdnet.com/article/35106545/）を再録したものです。仕様等は公開時点のものです。

ZDNet Japan

Wi-Fiのセキュリティ事情

中国の無線 LAN セキュリティ事情の今

ロジテック製無線 LAN ルータから ID とパスワードが流出し、中国ユーザー向けプロキシサーバが日本へのサイバー攻撃に悪用された事件があった。PC によるインターネットがはじめに普及し、その後にスマートフォンが普及した中国では、無線 LAN ルータは多くのインターネットユーザーが所有している。そして中国でも無線 LAN がハッキングされ、悪用されるケースが多数報告されている。その問題は、影響力のある全国テレビ「CCTV（中国中央電視台）」でも特集で報じられた。

国家信息安全漏洞共享平台（CNVD）の分析によれば、Cisco をはじめ、中国でどこの電脳街でも見る D-LINK、Linksys、Netgear、Tenda などのメーカーの製品にバックドアが存在するという。ロジテックだけの問題ではなく、あらゆる無線 LAN ルータで起こりうる問題といえよう。日本のユーザーも海の向こうの話と思わず、無線 LAN ルータのファームウェアを最新に更新するように努めたい。

今夏、360 互聯網安全中心が発表したルータに関するセキュリティレポート「中国家用路由器安全報告」によれば、2014 年 6 月末の時点で、1000 機種超、約 1 億台の無線 LAN ルータが稼働していて、その 68.5%が家庭、12.7%が学校の宿舎、9.3%が職場で使用されているという。無線 LAN ルータの利用人数について「1 人」というのは 1.6%しかなく、「2 ～ 3 人」は 55.8%、「4 ～ 5 人」は 32.7%、「6 ～ 8 人」は 7.3%となっている。

つまり「1 人暮らしの人」や「家族の中で 1 人っ子の若い世代」が、1 人だけで無線 LAN ルータを占有し、PC なりスマートフォンなりを利用することは極めてレアだということだ。では青年世代だけでなく、年配の人や子供も無線 LAN ルータを利用するのかというと、18 歳以下は 5.6%、46 歳以上は 1.3%しかなく、その間の世代に利用者は集中する。家に人を呼ぶのを躊躇しない中国人は、しばしば同僚や旧友を呼ぶが、そうした訪問客が、「家で無線 LAN ルータを利用する複数人のうちの 1 人」と解釈すべきだろう。

まだスマートフォンが普及しなかった 2008 年以前は、パスワードを設定していない無線 LAN ルータを見かけた記憶がある。普及した今、セキュリティ意識の向上と、製品自体にデフォルトでパスワードが設定されていることから、無線 LAN ルータの多くにパスワードがかけられている。レポートによれば、稼働する約 1 億台の無線 LAN ルータの多くが WPA/WPA2 PSK 方式によるパスワードを利用し、パスワードをかけていないのは 80 万台、WEP 方式を利用するのは 330 万台にすぎない。

しかしパスワードをかけているとはいえ、少なくない無線 LAN ルータで、8 が好きな中国人は「12345678（1 から 8 まで）」や「88888888（8 つの 8）」という定番のパスワードを設定している。また「admin」や「ROOT」などのルータの初期設定のパスワードもよく利用されている。とはいえ、最近ではルータ絡みのセ

こちらは、2014/12/16 に公開された記事（https://japan.zdnet.com/article/35057916/）を再録したものです。仕様等は公開時点のものです。

Wi-Fiのセキュリティ事情

キュリティの問題提起を各メディアで行っていたからか、2013年第3四半期には98.6%のルータに「わかりやすいパスワード」が採用されていたが、2014年第2四半期には24.3%まで減り、だいぶ改善したという。

パスワードが脆弱な無線LANルータのうちの61.1%のルータが、「ぼくはまちちゃん」騒動などで知られる「CSRF (Cross-Site Request Forgeries。リクエスト強要)」の脆弱性がある。また75万台の無線LANルータがDNSハイジャックされているという。危険なサイトにアクセスした結果被害にあうことが主な原因だが、それは中国では、日本でもありがちなポルノ広告だけでなく、オンラインショッピングサイトで、店が儲けるために仕掛けたリンクやQRコードによるリンクによるものもあり、仕掛けられた罠は多い。

加えて中国は、他国と比べてiOS機器のJailBreak率や、Android機器のroot率が特に高いことが知られている。そのために無線LANを通じて、スマートフォンやタブレット内の写真やショートメールなどの個人情報が盗まれる案件が非常に多いという。

こちらは、2014/12/16に公開された記事（https://japan.zdnet.com/article/35057916/）を再録したものです。仕様等は公開時点のものです。