



無線LANは簡単、
セキュアな無線LANはチャレンジ

目次

無線LANは、あらゆる分野への拡大	3
無線LAN導入が拡大している理由	4
無線LANネットワークを狙う11のセキュリティの脅威:	
1. Wi-Fiパスワード解読	6
2. 不正ホットスポット	6
3. マルウェアの拡散	6
4. 盗聴	6
5. データの不正取得	6
6. 不正・違法使用	6
7. 悪意ある近隣ユーザー	7
8. 中間者攻撃 (MiM)	7
9. 無線LANに対するDoS攻撃	7
10. なりすまし攻撃	7
11. APの構成ミス	7
業種別の問題	8
小売業	8
観光業	9
医療機関	10
教育機関	11
今すぐ実行すべき対策	12
エンタープライズグレードセキュリティへのステップアップ	13
ウォッチガードのセキュア無線テクノロジー	14

無線LANは、あらゆる分野へ拡大

あらゆる業種の企業が、顧客、取引先、従業員から無線アクセスの提供を求められるようになっていきます。無線LANサービスを提供することにメリットがある反面、提供側にとっては、モバイル環境の提供や利用状況の分析、ホットスポット、IoT（モノのインターネット）といった検討すべき多くの課題が存在します。

このeブックでは、無線LANニーズ急増の現状をふまえ、重要度の高い無線ネットワークの保護について解説します。



**全世界の
インターネットトラフィックの
63% が
2019年¹までに
無線LAN 経由になる**



無線LAN導入が 拡大している理由

iPassは2014年に**2千3百万**だった
ホットスポット数が**2018年²⁾**に
3億に増加すると予測



作業生産性

無線LAN接続のスループットが802.11acに高速化したことで、イーサネット接続なしでも仕事ができるようになりました。モバイル環境を活用することで、柔軟な作業環境が実現するだけでなく、以前にはボトルネックとなっていた生産性低下も回避できます。



優れた投資対効果

従来の有線LAN環境には、柔軟性の欠如や導入コストの高さといった問題があります。有線のためのインフラを構築する場合には、セットアップやメンテナンスのコストだけでなく、配線、壁面コンセント、スイッチなどの費用も必要です。組織が拡大し、ユーザ数が増えると、さらに追加コストが発生します。しかし、無線LAN環境を用意すれば、はるかに少ないコストで高いスケーラビリティを提供でき、ユーザが施設内で自由に移動できるため、柔軟性と効率性が各段に向上します。



顧客満足度の向上とリピート客の獲得

多くの業種でゲスト用無線LANが提供されるようになりましたが、サービスを提供する場合に、高解像度動画や音楽のストリーミングにも対応できる高速なネットワーク環境が必要となる場合も検討しなければなりません。旅行者がホテルを選ぶ際に、無料の無線LANサービス利用が高い優先順位となっているため、ホテル・観光業においては特に、Wi-Fi接続の提供が重要となります。



モバイルエンゲージメント

無線LAN環境の提供により、企業はさまざまな方法でゲスト用無線LANネットワークに接続した顧客とコミュニケーションができるようになります。シンプルなトップページだけでなく、魅力的で目を引くページを表示し、顧客にとって有益な情報を最適なタイミングで提示できます。



顧客分析

パッシブスキャン、アクティブスキャン、無線LANネットワークによるユーザ接続などにより収集される大量の顧客データにより、ゲストの行動、特性、トレンドなどの有益な情報が収集可能です。これらの情報をSNSのログイン分析と併用することで、顧客の性別、年齢、購買傾向などの有益な情報を視覚化し、効果的にマーケティング戦略の策定に活用することが可能となります。



モノのインターネット(IoT)

インターネット接続されるデバイスの数が急増しています。IDCは、自動車や冷蔵庫などのIoTエンドポイントのデバイス数が2020年には2014年の3倍になると予測し、同期間にグローバルのIoT市場規模が65億8千万ドルから17兆ドルへと150%も増加すると予測しています。

無線LANを狙う 11のセキュリティの脅威



1. Wi-Fiパスワードクラック

WEPなどの古いセキュリティプロトコルがいまだに使用されている無線アクセスポイントは、パスワードを簡単に解読できてしまうため、簡単に標的にされてしまいます。



2. 不正APとクライアント

サイバー犯罪者がホットスポットの近くで偽装したSSIDのアクセスポイントを用意すれば、ユーザは疑うことなく簡単にログインしてしまうでしょう。そして、不正APによる不正コードインジェクションの被害者となってしまったことに気付くユーザは少ないでしょう。



3. マルウェアの拡散

ゲスト用の無線ネットワークの利用者は、近くにいる悪意あるユーザが送り込むマルウェアの影響を知らぬ間に受けることになります。ハッカーが良く使う方法の1つに、バックドアを仕込んで後から機密情報を盗むという手口があります。



4. 盗聴

セキュリティ対策が不十分なネットワークを悪用して私的なやり取りを盗聴されたり、パケットを傍受されたりする恐れがあります。



5. データの不正取得

ユーザは、無防備な無線ネットワークにアクセスした瞬間から、極秘情報が含まれる私的文書がネットワーク経由で送受信されたり、データが傍受されサイバー犯罪者の手に渡るリスクにさらされます。



6. 不正・違法使用

ゲスト用のWi-Fiが違法性や有害性の疑われる通信に悪用されるリスクがあります。成人向けや過激なコンテンツは周りのユーザに不快感を与える恐れがあり、著作権で保護されたメディアの違法ダウンロードは著作権侵害の訴訟に発展する可能性があります。



7. 悪意ある近隣ユーザー

無線LANネットワーク上のユーザ数が増えれば、マルウェアに感染した端末が同一ネットワーク上で活動している可能性も高くなります。AndroidのStagefrightなどのモバイル攻撃では、被害が表面化する前にゲスト間での感染が広がっていることもあります。



8. 中間者攻撃(MiM)

無線LANを経由の日常的なやり取りでも、犯罪者が密かに傍受して、正規の違法性のない内容が書き換えられてしまうことで、データ流出につながる可能性があります。



9. 無線LANに対するDoS攻撃

攻撃者が正規のアクセスポイントに意図的に大量のトラフィックを送信し、アプライアンスを使用できなくすることで、正規ユーザがWi-Fiにアクセスできなくするものです。



10. なりすまし攻撃

Wi-Fiのセキュリティを攻撃するサイバー犯罪者は一般的に、MACアドレスを偽装することで正規あるいは既知のデバイスであるかのように装います。



11. APの構成ミス

ワイヤレスセキュリティのベストプラクティスに従わずにアクセスポイントを導入すると、構成ミスによって、セキュリティリスクにさらされる危険性が高まります。



業種別の問題

60%の中小規模企業が、データ流出の発生から6か月以内に廃業に追い込まれている。

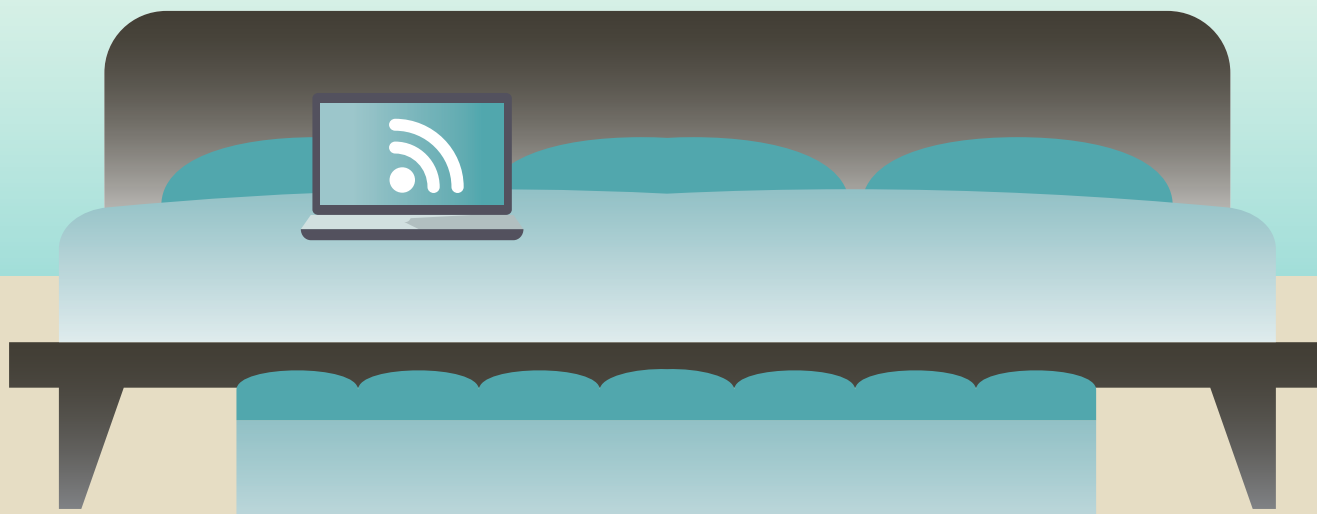


小売業の課題

モバイルPOS(販売情報管理システム)の導入が進んでいます。有線・無線LAN経由でクレジットカードでの処理を受け付ける企業は、カード会員情報の保存や個人情報の通信を保護する責任があります。金融機関グループは、PCI DSS(ペイメントカード業界データセキュリティ基準)と呼ばれる、支払情報保護の規格を定義しており、このガイドラインでは、小売業者や消費者の情報を保護するよう設計されています。このガイドラインに従わない企業には、多額の罰金が課せられます。

小売業の業種において、無線LAN経由で顧客情報を可視化しようとする場合、もう1つの大きな課題があります。オンラインビジネスでは古くから、マーケティングROIや成約率などの多くの重要な指標を改善するためのデジタルマーケティングの手法が利用されてきました。しかし、それらのツールを実店舗での活動でビジネスの最適化につながる保障が得られるわけではないのです。

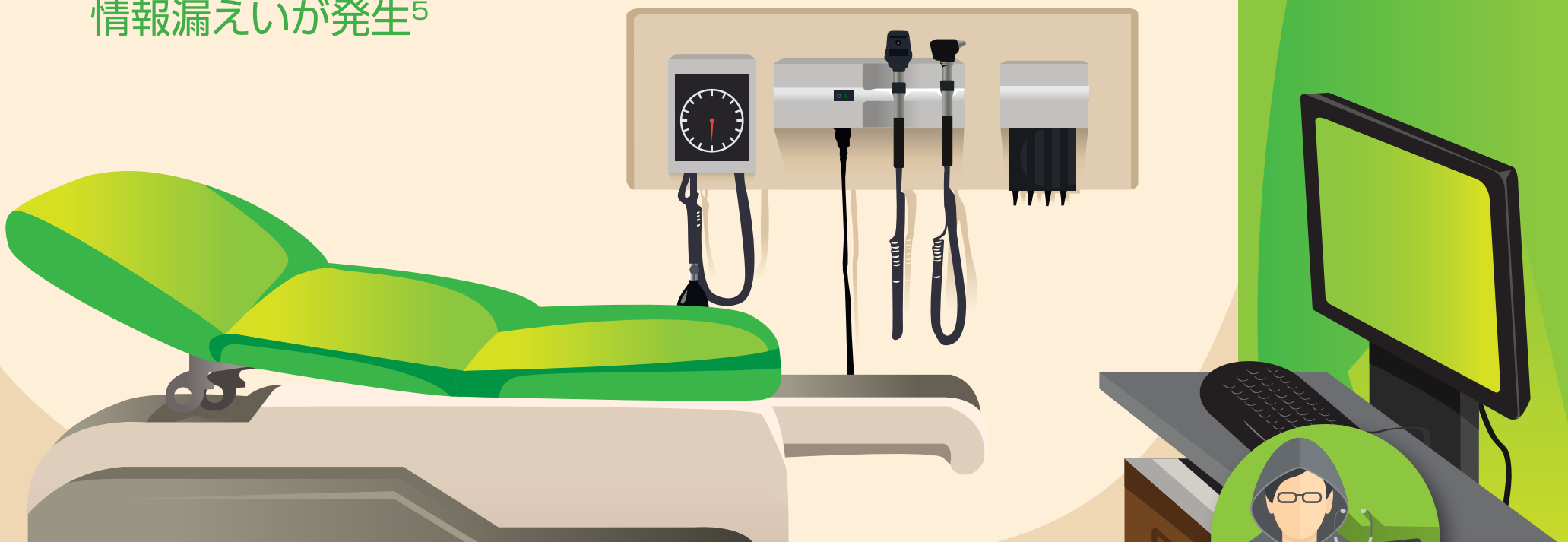
49%のビジネス出張者は宿泊先ホテルの選択肢として
無料の無線LANサービスの有無を検討している⁴



観光業の課題

PMS（ホテル・旅館の管理システム）は、宿泊者のクレジットカード情報の管理を含む、フロント業務からバックオフィス処理まで複数の業務内容を自動化し、調整するためのソフトウェアアプリケーションです。POS システムや予約システムと統合されている場合が多いことから、PMS システムもまた、サイバー犯罪者にとって価値の高い標的となります。多くの大規模ホテルチェーンが、PMS やPOS を攻撃されてデータが流出し、罰金、訴訟、信用低下に追い込まれています。観光業の企業にとっては、高速無線LAN環境を提供し、同時にゲストと自社の両方のリソースを保護することが大きな課題です。また、カスタマーエンゲージメントのためのオンラインプラットフォームも必要となります。そして、これらのツールを自社ブランドでカスタマイズし、顧客満足度の向上やリピート客の獲得にも活用することが可能です。

医療・ヘルスケア業界では過去3年間に
42.5%の情報において
情報漏えいが発生⁵



医療機関の課題

医療機関でのやり取りされる情報は機密性、情報価値が高いため、無線LAN環境のセキュリティ対策においては、他の業種にはない課題を解決する必要があります。HIPAA(医療保険の携行性と責任に関する法律)や関連する基準では、患者のデータを取り扱う機関に対して、厳格なセキュリティ対策を求めています。医療機関におけるITの進化により、無線LAN経由でデータが交換されるようになり、医療機器などの在庫管理などのプロセスが合理化されましたが、脆弱性の問題が同時に発生しています。IoT(モノのインターネット)と呼ばれるこのトレンドは、医療分野にも効率化と変革をもたらし、医療関連のデバイスもサイバー攻撃の標的となっています。

医療機器では古いOS(オペレーティングシステム)が使われていることが多く、多数の脆弱性が存在します。顧客や患者の情報にモバイルデバイスからアクセスできれば、業務の効率性は向上しますが、同時に適切なセキュリティ対策がなければ、データ流出のリスクが増大する事になります。



教育機関の課題

モバイルデバイスは教育機関にも変革をもたらしました。全生徒にタブレット端末が貸与され、Webベースの教材への高速無線LANアクセスが必要とされるようになりました。しかしながら、役に立つ情報システムの活用にはリスクが伴います。小中高校生の場合には特に、不適切なWebコンテンツのフィルタリングが必要です。ハッカーの巧妙な手口に慣れていない小学生は、マルウェアに感染するリスクが特に高いと言えるでしょう。外部の脅威に加えて、不正行為や改ざんなどのプライバシーの問題のリスクを最小限に抑えるためには、学生が利用するネットワークを管理者が正しくセグメント化する必要があります。

今すぐ実行すべき対策



WPA2 – 最新の安全なプロトコルを有効にしましょう



強力なパスワード – デフォルトのパスワードをそのまま使わずに、パスワードを定期的に変更しましょう。



ネットワークの理解 – 不正APをスキャンし、可能であればMACアドレスのホワイトリストを使用しましょう。



無線LAN利用範囲の制限 – 利用可能範囲を限定しましょう。



常に最新のファームウェアにアップデートしましょう。

エンタープライズグレードのセキュリティの導入



セキュリティ Security

無線LANを有効にするのは簡単ですが、セキュリティの実現は簡単ではありません。賢明なセキュリティ管理者であれば、無線LANを含むすべてのトラフィックに対して、AV、IPS、Webフィルタリング、スパムメール対策、アプリケーション制御、レピュテーションセキュリティ、標的型攻撃対策、情報漏えい防止などのセキュリティ機能を有効にするはずです。

パフォーマンスや効率性を低下させることなく、すべてのセキュリティ機能を単一のインターフェースで一元管理できるようにし、WIPS (特許取得：ワイヤレス侵入防止システム) が有効なアクセスポイントを使用するようにします。WIPS により、機密情報の保存や送受信を保護し、ネットワーク管理者が未承認デバイス、DoS攻撃、不正APなどから無線LAN環境を保護する上で不可欠のシステムです。

WIPS は、無線LANアクセスで検知されたデバイスを自動的にリアルタイムで承認済み、不正、外部のいずれかに分類します。セキュリティ管理者は、不正な無線デバイスを特定するための複雑なルールを定義したり、手動でデバイスを調査したりする必要もありません。

可視性 Visibility

現在、無線LAN環境は、多くの組織において最も見過ごされやすい盲点です。ITセキュリティの専門家は、リアルタイムに過去のトラフィックも含め可視化でき、ネットワークの傾向の分析とレポートが提供され、無線LAN環境においては、ゲストユーザの挙動や不正APを検知できるソリューションが必要だと考えています。

管理 Management

ネットワーク機器の構成ミスは、ネットワークセキュリティ侵害の原因として最も多い原因の1つです。有線・無線LANのネットワーク管理が統合することにより、構成ミスのリスクは低下します。IT管理者の多くが、クラウド、Windows、Web、CLIベースのシステムを利用して、効率的なセキュリティ管理を可能にする柔軟な管理ツールを求めています。

WatchGuard Secure Wireless Technology

クラウド対応のアクセスポイント

クラウド対応の無線LANアクセスポイントを導入することで、既存のファイアウォールを強化しつつ、無線LAN環境を構築することができます。AP120は小規模無線ネットワークに適し、AP320は中規模以上の複雑な無線LAN環境に最適です。

ネットワークセキュリティアプライアンス

無線LANのすべてのトラフィックをセキュリティアプライアンス経由にすることで、セキュリティが強化され、ビジネスとそのユーザの両方の保護が可能になります。

WatchGuard Dimension™

WatchGuard DimensionとWatchGuard Wi-Fi Cloudの統合によって、無線LANトラフィックが1つのソースに統合されます。このリアルタイムの情報をダッシュボードやカスタマイズ可能なレポート機能で活用することにより、IT担当者がベースラインを作成してネットワークの利用傾向を理解し、無線LAN環境での悪意ある挙動を早期に検知し、ビジネスへの影響を防止できます。

WatchGuard Wi-Fi Cloud

WatchGuard Wi-Fi Cloudは、無線LAN環境の完全な可視化を可能にします。カスタマイズ可能なダッシュボードとアラートでビジュアル化されたビューを提供し、さらに、トラフィックとセキュリティの状況をドリルダウンして詳細情報を確認できます。

Wi-Fi Cloudは、革新のWi-Fi テクノロジーの活用によって、顧客の行動特性などの重要なマーケティングデータも可視化します。これらのインサイトをモバイルエンゲージメント機能に活用すれば、ソーシャルネットワーク内で、顧客ごとにカスタマイズして、より直接的なコミュニケーションも可能になります。

ウォッチガードのSecure Wi-Fi製品



1. Cisco VNIグローバルIPトラフィック／サービス導入予測、2014年～2019年
2. <http://www.marketwired.com/press-release/ipass-wi-fi-growth-map-shows-1-public-hotspot-for-every-20-people-on-earth-by-2018-nasdaq-ipas-1963515.htm>
3. <https://www.staysafeonline.org/stay-safe-online/resources/small-business-online-security-infographic>
4. Hotels.com「Free Wi-Fi Reigns but Wanes as Top Hotel Amenity(ホテルの無料Wi-Fiは普及したが、1位に挙げる人は減少)」2015年5月6日
5. USA Today紙「Another Health Care Data Breach(相次ぐ医療データ流出)」(2015年7月25日付)
6. Websense Security Labsブログ「Today's Lesson(現代社会の教訓)」2015年7月7日



ウォッチガード製品はすべて、セキュアワイヤレスを考慮して構築されています。それは、ネットワークファイアウォールからクラウド対応アクセスポイントまでのどの製品も重要な要素であり、高速で信頼できる安全な無線LAN環境がビジネスには不可欠であるからです。

ウォッチガードのセキュアワイヤレス技術を活用することで、エンタープライズグレードで確実なネットワークセキュリティを実現できます。また、革新的なRapidDeployテクノロジーにより、各拠点に専門知識のある技術者を置く必要もなくなります。クラス最高のセキュリティが容易に実現し、クラウドWi-FiソリューションであるWatchGuard Wi-Fi Cloudによって、ワイヤレスセキュリティと脅威対策をエンゲージメント・分析のあらゆる機能を備えたインタラクティブツールと組み合わせて利用するため、エンタープライズグレードのセキュリティと最高の無線LAN環境を中堅・中小規模や分散型の企業でも活用できます。

www.watchguard.co.jp/wifi

ウォッチガード・テクノロジー・ジャパン株式会社
TEL: 03-5797-7205

Web: <https://www.watchguard.co.jp>
Mail : jpnsales@watchguard.com