もはやビジネスに不可欠な無線LAN 求められるセキュリティー対策は

適切な暗号化と認証で盗聴やなりすましを防ぐ

多くの企業において、利用が進む無線LAN。しかし利便性や運用のしやすさの裏には、「不正アクセス」や「なりすまし」「情報漏えい」などの脅威が潜んでいます。組織内部における無線LANはもちろん、モバイルワークで利用する際も、安全の確保が企業に求められています。

企業内外で活用が進む無線LAN、想定される脅威は？

LANケーブルでネットワークへ接続する代わりに無線通信でデータの送受信を行う無線LAN。通信速度の向上とともに、モバイルパソコンやスマートデバイスを活用する企業も増加しており、業務において無線LANは欠かせないものになりつつあります。今後は、IoT機器の増加でますます無線LANを活用する場面が増えていくと予想されます。

LANケーブルの敷設が不要なためメンテナンスしやすく、ネットワークの再構築も容易など、有線LANより運用が楽というメリットも後押しし、近年は工場やプラント、倉庫など利用シーンが拡大しました。また企業内において会議室など別室に移動しても気軽にネットワークが利用できるのはもちろん、従業員が作業する座席を固定しない「フリーアドレス」といった新しいオフィス環境にも柔軟に対応できます。

＜無線LANと有線LANのメリット、デメリット＞

	無線LAN	有線LAN
特徴	電波を用いてアクセスポイント経由により端末をネットワークへ接続する方法。ノートパソコンのほか、スマートフォン、タブレット、IoT機器など、主にクライアント機器の接続に用いられている。	LANケーブルを用いてネットワークに接続する方法。デスクトップパソコンのほか、プリンターや複合機、サーバ、基幹システムなど広く利用されているが、タブレットなど有線LANのインタフェースを搭載しない端末も増えている。
メリット	・LANケーブルを敷設していなくとも、電波が届く範囲であれば利用できる。 ・ネットワークの構築、再構築を比較的容易に行うことができる。 ・モバイル端末、IoTなど、機器の追加へ柔軟に対応できる。	・高速な通信環境を利用できる。 ・接続環境や電波の干渉などの影響を受けにくく、安定した通信が可能。 ・接続できる端末を物理的に制限できる。
デメリット	・有線LANと比較すると低速で、接続環境や電波の干渉などの影響を受ける。 ・アクセスポイントの性能や設置状況により、通信距離、同時接続数などが変化する。 ・電波の届く範囲内であれば誰でも通信を傍受できる。	・LANケーブルを敷設する必要があり、ネットワークの構築や再構築などコストがかかる。 ・接続できる機器が機器の物理的なポート数やネットワークの敷設状況により制限される。 ・ケーブルの断線などのリスクがある。

では、企業内にアクセスポイント（以下、AP）を構築して無線LANを利用する場合、どのような脅威が想定されるでしょうか。

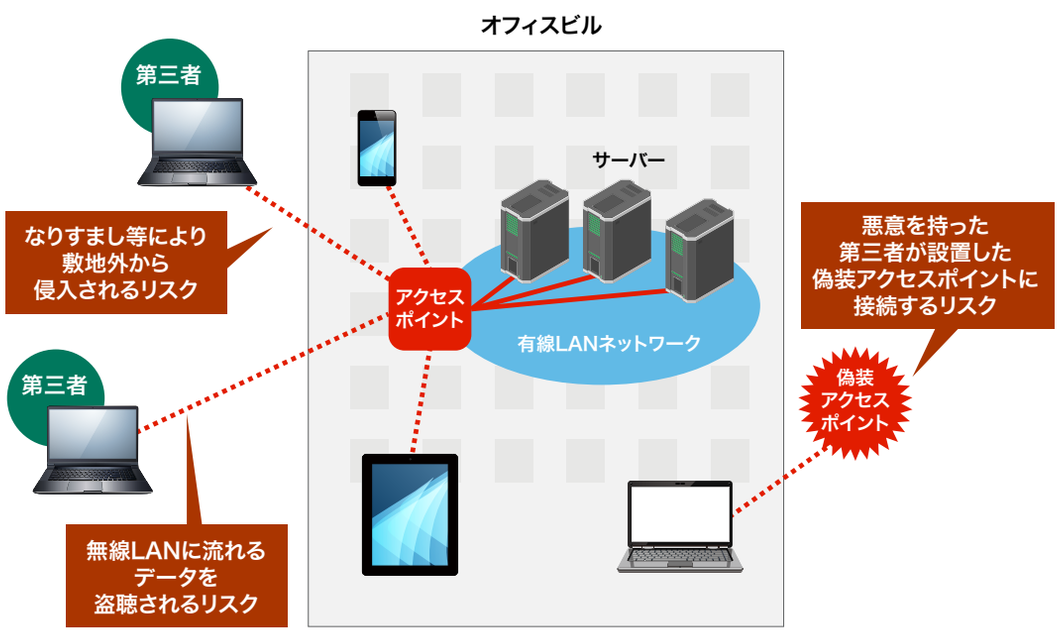
無線LANでは電波が届く範囲にいるユーザーであれば基本的にネットワークへのアクセスが可能です。つまり、電波の届く範囲であれば、企業内に設置されたAPに敷地外からもアクセスできるのです。そのため、厳重なセキュリティー対策を講じなければ、通信内容の盗聴や改ざん、ネットワークへの侵入、正規利用者へのなりすましなど、さまざまな脅威に直面します。侵入可能な無線LANを街中で探す「ウォードライビング（War Driving）」と呼ばれるリスクがかねてから指摘されています。

実際に無線LANが原因となり、不正侵入される事件も発生しました。最近では佐賀県の公立校や教育情報システムが不正アクセスを受けた事件がありました。同事件では、2016年6月に当時17歳の少年が逮捕されましたが、セキュリティーが甘い公立校のAPを探索し、外部から学内にアクセスしていました。

特に通信が「暗号化されていない」「暗号化方式が危殆化している」場合、通信内容が容易に盗聴される恐れがあります。また強度が高い暗号化であっても、事前共通キーが容易に予測できれば、暗号化していても、意味がありません。

もし企業のネットワークへアクセスを許せば、内部のパソコンやファイルサーバーにアクセスされ、保管された個人情報や機密情報を窃取されたり、データの破壊や改ざんなどの被害に遭う恐れがあります。また、LAN内からインターネットへアクセスできる場合、迷惑メール送信や外部への不正アクセスの踏み台に悪用されかねません。被害者とはいえ、事件の発端となれば企業イメージや信頼性の低下は免れないのです。

＜無線LANを用いた企業ネットワークが抱えるリスク＞



十分な暗号化と機器の認証が重要

企業内の無線LANを安全に保つには、どのようなセキュリティー対策を講じるべきでしょうか。
まずは通信の暗号化です。これによって、ネットワークへの不正な接続、通信内容が第三者に漏れてしまうことを防ぎます。

ただし、暗号化方式によって強度が変わるため注意が必要です。普及しているのは「WEP」「WPA」「WPA2」の3種類ですが、そのうち「WEP」は短時間で解読が可能であり、大変危険です。

「WPA」と「WPA2」では、暗号化プロトコルとして「TKIP（Temporal Key Integrity Protocol）」とより安全な「CCMP（Counter Modewith Cipher Block Chaining MAC Protocol）」のいずれかを選択できます。

同じ暗号化プロトコルを用いればセキュリティーは同等とされていますが、「CCMP」を標準とする「WPA2」と認証プロトコル「EAP（Extensible Authentication Protocol）」を組み合わせた「WPA2-EAP」を選択すると良いでしょう。「WPA2エンタープライズ」とも呼ばれています。

小規模なネットワークであれば、認証に事前共有キーを利用する「WPA2-PSK」を用いるケースもあります。ただし、事前共有キーは共通の文字列を用いますので、暗号化キーが企業外部へ漏れてしまえば、部外者が自由にアクセス可能となってしまいます。

多数がアクセスする企業の無線LANであれば、ネットワークへ接続した際に、ブラウザーから認証を求める「ウェブ認証」や、認証サーバーにより大規模な組織の管理にも対応する「IEEE 802.1X認証」などを活用します。「WPA2-EAP」では「IEEE 802.1X認証」をサポートしています。

加えて近年、個人端末を業務に利用するBYOD（Bring Your Own Device）が広がりを見せていることから、従業員が許可を得ずに私物の端末を無線LANに接続するケースも想定しておかなければなりません。本来接続する必要がない端末経由でマルウェアが持ち込まれ、組織内へ感染が広がるといったリスクも考えられます。企業においては、不用意に接続しないようセキュリティーポリシーを定めることはもちろん、端末認証を導入し、技術的に接続できないよう制限します。

また、APの管理にも注意を払います。管理者用パスワードは、初期設定から必ず変更し、類推できるようなパスワードや、簡易なパスワードは避けて、文字数が長く大文字や小文字、数字、記号を組み合わせた複雑なものを設定します。また脆弱性が存在しないよう、定期的にファームウェアのアップデートを確認することも重要です。

公衆無線LANに潜む「盗聴」リスク

無線LANの利用シーンは、企業内部に限りません。外出先で公衆無線LANを利用してインターネットに接続するケースも増えています。

情報処理推進機構（IPA）が、2016年12月に公表した「2016年度情報セキュリティの脅威に対する意識調査」によると、スマートデバイス利用者の31.5%が無料で提供されている「公衆無線LAN」を利用すると回答しました。2014年度は8.8%ほどでしたが、ここ数年で急激に利用が拡大しています。

さらに驚くことに、同調査ではプライベートやビジネス（学業）で無線LANを利用するユーザーのうち、38.0%が公衆無線LANへ接続していました。またビジネス（学業）のみで無線LANを利用している回答者も21.6%が公衆無線LANを活用していました。

公衆無線LANは主に交通機関や飲食店、コンビニエンスストア、観光地などで提供されています。2020年の東京オリンピック・パラリンピックの開催を見据え、訪日外国人が利用できるよう、国でも公衆無線LANの整備、拡大に取り組んでおり、今後ますます利用が進むことが予想されます。

暗号化されていない、または暗号の強度が弱い公衆無線LANでは、通信内容が盗聴される恐れがあります。ただし、暗号の強度が高ければ安全というわけではありません。公衆無線LANのように暗号化キーを不特定多数の利用者が共有しているケースでは盗聴の危険性があります。

第三者に通信が盗聴されれば、機密情報の漏えいなど生じる恐れがありますが、なかでもIDやパスワードなどのアカウント情報が窃取されれば厄介です。社内ネットワークや各種サービスへアクセスされれば、さらなる大きな被害へ発展する恐れがあります。

またAPには、悪意を持って設置されたAPも存在します。実在する正規のAPと同一のSSIDや暗号化キーが設定されており、端末にも接続情報が保存されている場合、悪意のAPを認識すると自動的に接続してしまう場合もあります。

公衆無線LANを利用してマルウェアへ感染させる「Darkhotel」と呼ばれるサイバー攻撃もセキュリティーベンダーによって確認されました。ホテルにおいて宿泊客が公衆無線LANに接続すると、パソコンへ偽のログイン画面を表示して情報を収集し、さらにソフトのアップデートに見せかけてマルウェアをインストールさせていました。Darkhotelの国別の検知数では日本がもっとも多く、主な標的になっていると見られています。

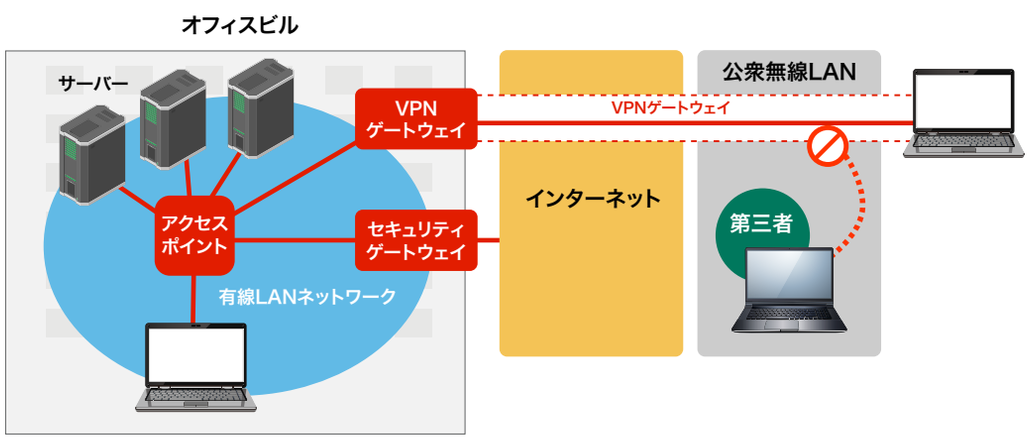
公衆無線LANを利用するならVPNの活用が不可欠

公衆無線LANにはさまざまな脅威が潜んでいます。暗号化に対応しているAPであっても、前述したように、公衆無線LANという性質上、SSIDと暗号化キーが公開されていることがほとんどで、暗号化された通信であっても、安全とは言えません。

悪意あるAPへアクセスすれば、DNSの改ざんなどをはじめ、偽の認証画面を表示する、偽サイトへ誘導されるといったリスクもあります。HTTPSに対応したウェブサイトなど、SSL/TLSにより暗号化されていれば、通信内容の盗聴は防げますが、電子証明書のエラーなどに気が付かず、悪意を持って設置されたウェブサイトへアクセスしてしまえば、データの漏えいなどが生じることになります。

業務で公衆無線LANを使用する場合は、すべての通信を端末と拠点間で暗号化する「VPN（Virtual Private Network）」を検討するとよいでしょう。VPNを利用して社内ネットワークへ接続すれば、中間者攻撃のリスクを排除できるだけでなく、インターネットへアクセスする場合も企業ネットワークを経由することで、マルウェア検査やフィルタリングなど、セキュリティー対策を実施できます。

＜VPNを用いた、外部から社内ネットワークへのアクセス＞



またMDM（モバイルデバイス管理）により、接続を許可するAPを指定できる製品やサービスもあります。許可していないAPへ意図せず接続するのを防ぐことが可能です。

無線LANは、目に見えない電波により通信が行われており、ついリスクを見落としてしまいがちです。そのような「隙」こそ攻撃者の狙い目となっています。

組織における無線LANの利用状況を可視化し、リスクへ十分な対策を講じているか ― 今、無線通信の安全を見つめ直さなければならない時が来ています。

NTTコムウェア株式会社
URL：http://www.nttcom.co.jp/
WEB 掲載：2017.2