クラウド無線LAN
Hypersonix

あなたの無線LAN、
セキュリティは大丈夫…？

これだけはやっておきたい

無線LANセキュリティ

AMIYA

Index

■ はじめに：広がる無線LANの利用 ---------- 3

■ 無線LANのセキュリティリスク

企業ネットワーク編 ---------- 4

ゲストネットワーク編 ---------- 6

■ 無線LANのセキュリティ対策

暗号化 ---------- 9

認証 ---------- 10

その他6つの対策 ---------- 11

■ 無線LAN運用の負担 ---------- 13

■ クラウド無線LAN Hypersonix ---------- 14

■ セキュリティ機能が満載！ ---------- 15

■ OneGate連携で認証の強化を ---------- 16

■ おわりに：無線LANには適切な対策を ---------- 17

本書の対象

本書は、

- **無線LANの導入を検討している方**
- **無線LANのセキュリティが気になっている方**

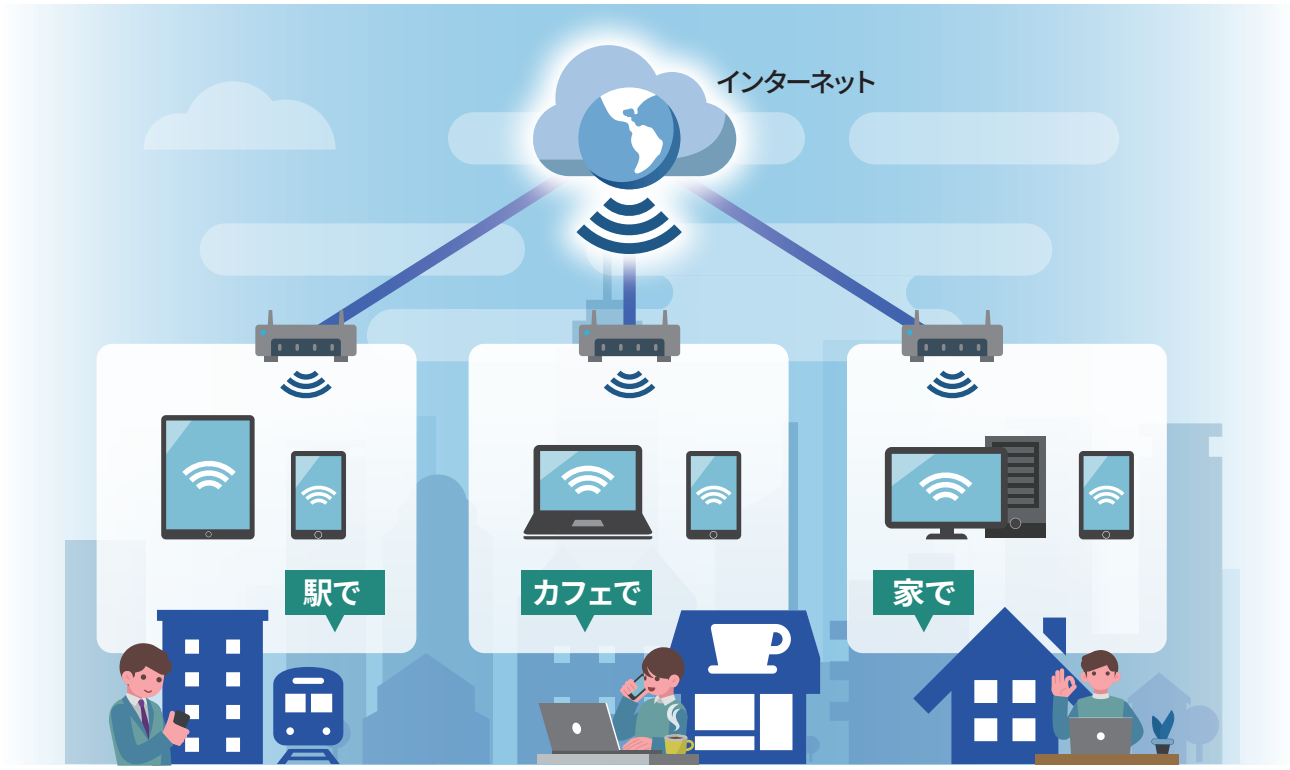
向けに、無線LANのセキュリティリスクとその対策を分かりやすく紹介するものです。
セキュリティリスクが多数存在する無線LANですが、適切なセキュリティ対策を施すことで安全に利用することができます。
本書が無線LANのセキュリティ対策の参考となれば幸いです。

広がる無線LANの利用

はじめに

近年、スマートフォンやタブレット端末、IoT家電など、インターネットを利用する様々な端末の普及を背景に、無線LANの利用が拡大しています。無線LANとは、電波を使って情報をやりとりするネットワークのことです。
無線LANの一番の利点は、端末にLANケーブルをつなぐ必要がないため、電波が届く範囲内であればどこでも好きな場所でインターネットに接続できることです。

さらには、配線を管理・整理する必要がないこと、一度に多くの端末を接続できるといったメリットもあります。
最近は公衆無線LANの整備も進み、駅やホテル、飲食店など、様々な場所で無線LANサービスを利用できるようになり、多くの人々が利用できるようになっています。



しかし、無線LANは便利である反面、情報セキュリティ対策を施さずにいると、気が付かないうちに通信内容が盗み見られたり、端末を乗っ取られてウイルスの配布などに悪用されたりするなどの被害に遭う危険性があります。

そのため、無線LANを安全に利用・提供するためには、適切なセキュリティ対策の実施が必須です。
本書では、企業ネットワークとゲストネットワークの２ケースにおける、無線LANのセキュリティリスクと、無線LANを安全に利用・提供するためのセキュリティ対策をそれぞれ紹介していきます。

無線LANのセキュリティリスク

企業ネットワーク編

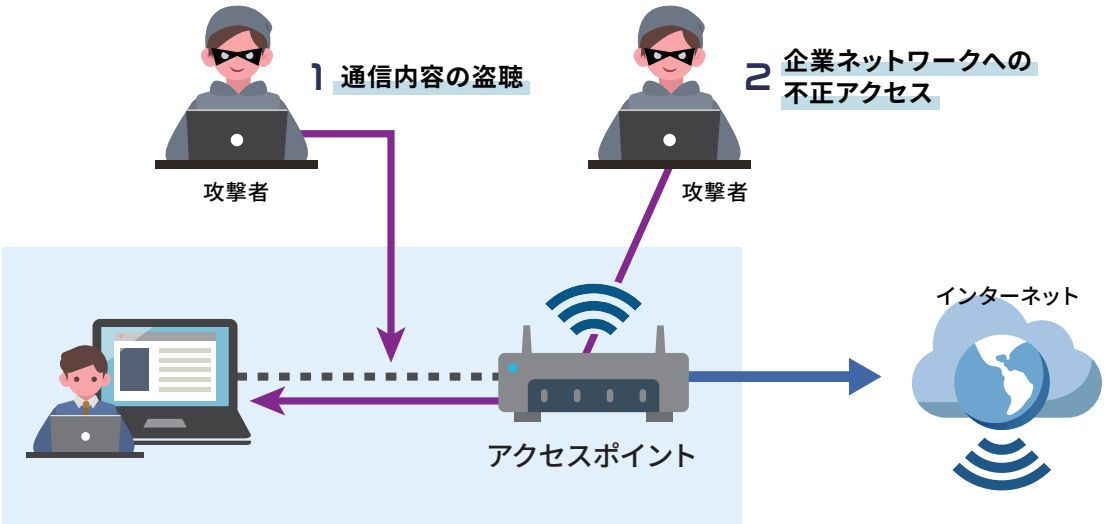
まず、**企業ネットワーク**に無線LANを導入する際、気をつけなければならないセキュリティリスクについて紹介します。

1 通信内容の盗聴

無線LANは、入退室管理の整備されたオフィス内（セキュリティエリア）に限らず、誰でもアクセスできる外部にも電波が届いてしまいます。そのため、通信の暗号化がなされていない場合や暗号強度が低い場合には攻撃者に通信内容を盗聴されてしまう危険性があります。通信内容を盗聴されると、無線LAN認証のID/パスワードや企業の機密情報などが、盗み取られてしまいます。

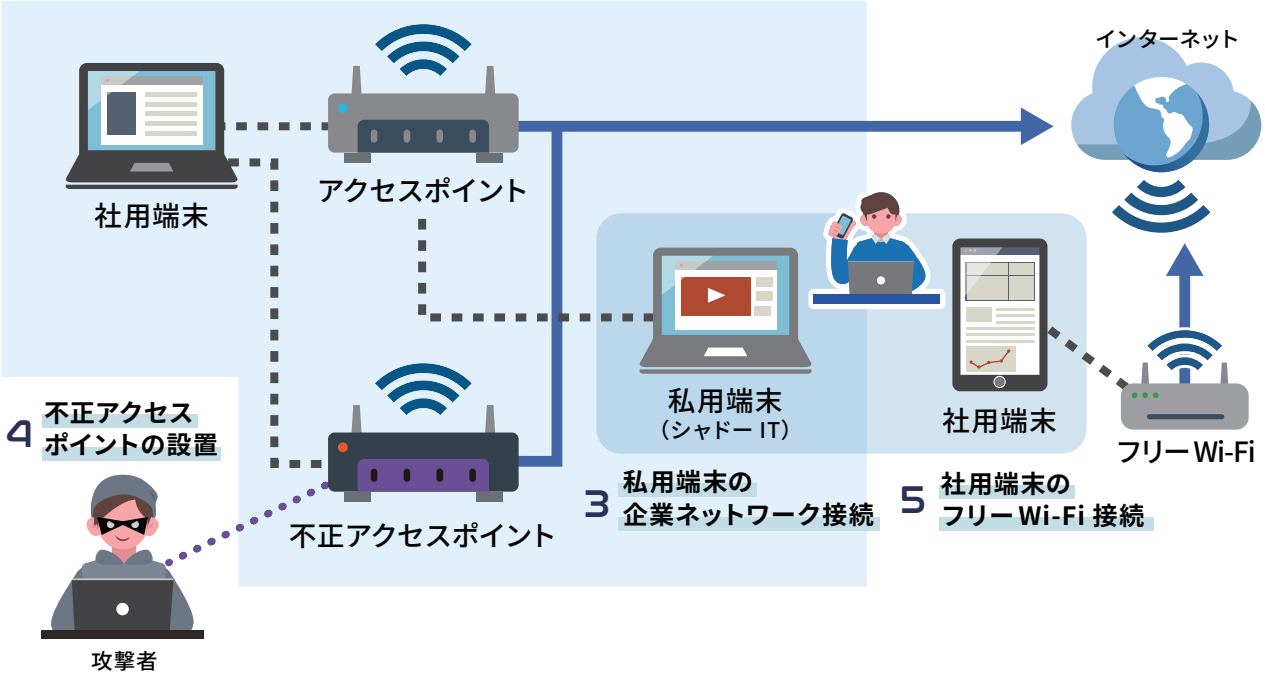
2 企業ネットワークへの不正アクセス

無線LANは、脆弱性をついた攻撃やパスワードのクラッキングにより社内ネットワークへ不正アクセスされる可能性があります。社内ネットワークへ不正アクセスを許せば、企業の重要データに不正アクセスされ、データを改ざんされたり機密情報が流出したりする可能性があります。さらには、ランサムウェアに感染させられる危険性もあり、企業に大きな悪影響を及ぼす恐れがあります。



無線LANのセキュリティリスク

企業ネットワーク編



3 私用端末の企業ネットワーク接続

無線LANの認証情報を知っている従業員は、その認証情報を使って私用端末を企業ネットワークに無断で接続する可能性があります。企業側が把握せずに従業員が業務に利用しているデバイスのことを「シャドーIT」と呼びます。

社用端末であれば適切なセキュリティ対策を施すことでリスクを低減することができますが、シャドーITは企業側で管理できません。そのようなシャドーITがマルウェアに感染していた場合、企業全体に感染が拡大してしまうなどの大きなリスクが存在します。

4 不正アクセスポイントの設置

不正な無線アクセスポイントを企業ネットワークへ接続される場合があります。例えば、従業員が電波が弱いエリアに良かれと思って無線アクセスポイントを設置する、などが想定されます。不正アクセスポイントは簡易なセキュリティ設定しか施されていないことが多いため、不正アクセスポイントを社内LANに接続されることで容易に攻撃者がアクセスできるようになってしまいます。その結果、社内サーバにアクセスをされて機密情報を閲覧されたり、奪取されてしまったりといった危険性があります。

5 社用端末のフリーWi-Fi接続

無線LANを導入すると、外出先でのWi-Fi利用についても検討が必要です。企業ネットワークの無線LANは適切なセキュリティ対策を施すことができても、外出先の無線LANのセキュリティ設定までは把握できません。適切な対策がなされていない無線LANに社用端末を接続すると、盗聴や情報を窃取されるリスクがあります。

無線LANのセキュリティリスク

ゲストネットワーク編

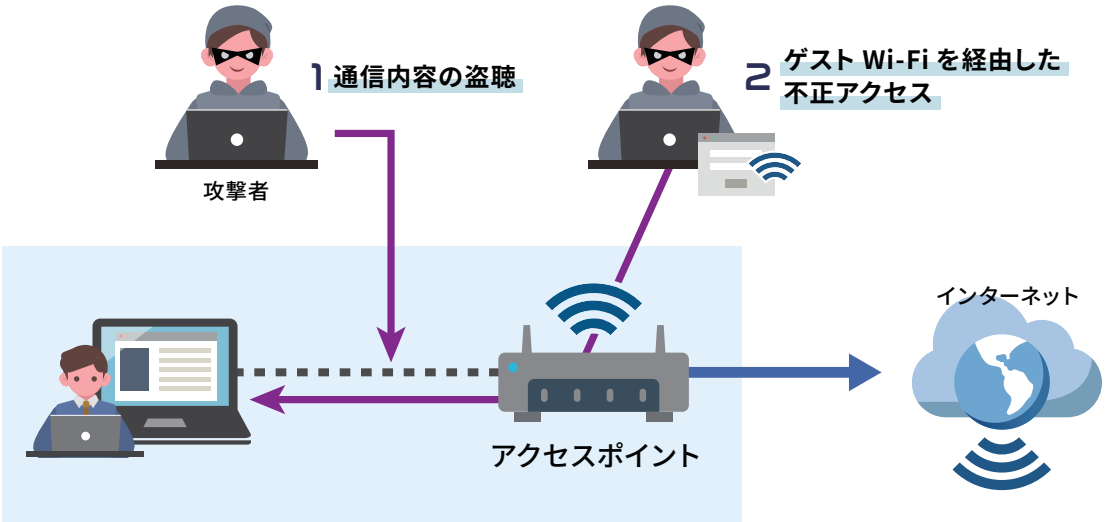
オフィスや店舗に**ゲスト用無線LAN**を導入する際、気をつけなければならないセキュリティリスクについて紹介します。

1 通信内容の盗聴

通信の暗号化がなされていない場合、暗号強度が低い場合には攻撃者に通信内容を盗聴されてしまう危険性があります。通信内容を傍受されると、メールアドレスやサイトの閲覧情報、各種パスワードなどの個人情報や企業の機密情報などが、盗み取られてしまいます。
特に、公共の無線LANは不特定多数が同じネットワークを利用でき、通信が暗号化されていないものが多いため、大変危険です。

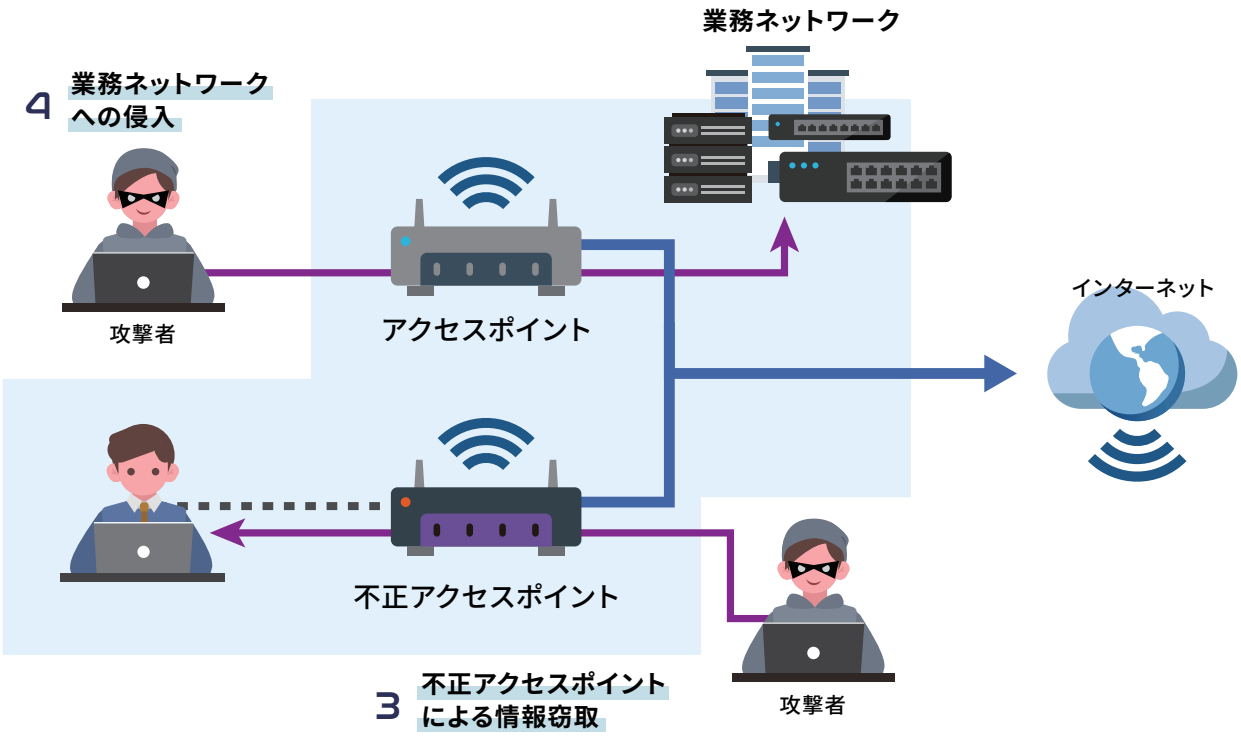
2 ゲストWi-Fiを経由した不正アクセス

無線LANはSSIDとパスワードさえわかれば接続できてしまうため、適切な対策を施されていないと、攻撃者にネットワーク内に侵入され、端末にアクセスされてしまいます。端末に不正アクセスされると、クレジットカード情報などの重要な個人情報が盗まれたり、企業の顧客情報などの機密情報が盗まれて深刻な問題に発展する可能性も考えられます。さらに、不正アクセスを通じてウイルスを送り込まれ、データを暗号化されたり遠隔操作されたりする危険性もあります。



無線LANのセキュリティリスク

ゲストネットワーク編



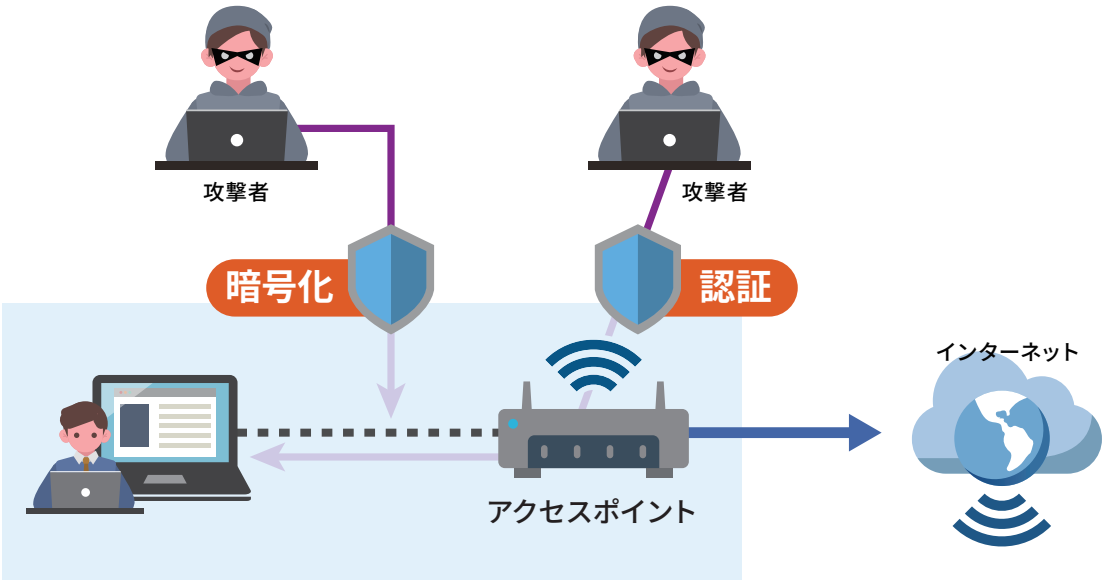
3 不正アクセスポイントによる情報窃取

ある無線LANの電波が漏れ出ている範囲に、攻撃者が偽のアクセスポイントを持ち込み、そちらに接続させることで、接続した端末が保持する情報を窃取するという手口も存在します。公共の無線LANの近くに本物と同じSSIDのついた悪意のあるアクセスポイントが設置された場合、本物との区別がつかないため、注意が必要です。

4 業務ネットワークへの侵入

提供されているゲスト無線LANが物理的もしくは論理的に業務ネットワークとは分離されていない場合、そこから業務ネットワークに侵入することが可能になってしまいます。悪意をもった第三者がそのようなゲスト無線LANに接続した場合、機密情報にアクセスして情報の改ざんや窃取が行われる危険性があります。

これらの企業ネットワーク、ゲストネットワークのセキュリティリスクは、適切な対策を施すことによって、リスクを低減することができます。まず、大きなセキュリティ強化策として、**「暗号化」**と**「認証」**の二つが挙げられます。



無線LANのセキュリティ対策 ~暗号化~

企業ネットワーク編　ゲストネットワーク編

企業ネットワーク、ゲストネットワークどちらにおいても、通信内容の盗聴を阻止するには、無線LANに安全性の高い暗号化プロトコル・暗号化方式を設定することが重要です。
最新かつ最も安全な暗号化プロトコルは「WPA3」で、従来の暗号化技術で明らかになった脆弱性を参考に対策を実装し、セキュリティ強化を実現しています。

暗号化方式は「AES」が安全で、従来の暗号化方式の弱点が強化されています。
「WPA3」と「AES」を採用することで、強固な暗号化を施すことができます。最新のWi-Fi規格である「Wi-Fi6」の機器では「WPA3」「AES」に標準対応しています。

暗号化プロトコル

セキュリティ強度	暗号化プロトコル	特徴
強	WPA3	最新の暗号化プロトコル。WPA2の脆弱性を解消しており、近年発売の機器はほとんどが対応している。
↑	WPA2	強化された暗号化アルゴリズムAESに対応。WPA3の登場まで主流であった。
	WPA	暗号化方式TKIPに対応し、WEPより安全性が強化されているが、WPA2の登場以降新しい機器で利用されることはほぼない。
弱	WEP	過去に様々な脆弱性が発見されており、安易に解読できてしまうため現在ほぼ使われていない。

暗号化方式

セキュリティ強度	暗号化方式	特徴
強	AES	WPA2から対応している暗号化方式。共通鍵方式というTKIPの弱点を補う対策が実装されており、現在主流となっている。
↑ 弱	TKIP	WPAで採用された暗号化方式。現在では脆弱性が発見されており使われていない。

無線LANのセキュリティ対策 ~認証~

企業ネットワーク編

企業ネットワークへの不正アクセスを防ぐには、認証の強化が必須です。認証方式は様々ありますが、企業ネットワークにおいては必ず「証明書認証」を行うようにしましょう
中でもおすすめなのが、数ある無線LANの認証方式の中でも最上級のセキュリティレベルである、「証明書認証（EAP-TLS）」です。

この認証方式では、クライアントとサーバの双方が用意したデジタル証明書を交換することで相互認証を行います。
そのため、クライアントのみが認証情報を送信する方式と異なり、サーバ側の詐称をも防止することができます。

認証方式

セキュリティ強度	認証方式	特徴
強	証明書認証（EAP-TLS）	IDパスワードではなくクライアントとサーバ間でのデジタル証明書のやりとりによって認証を行う方式。
↑	証明書認証（PEAP）	サーバ側がデジタル証明書を発行し、クライアントがIDパスワードを入力することで、クライアントとサーバ間で相互認証する方式。
弱	WPA	IDパスワードで認証を行う方式。

無線LANのセキュリティリスク
~その他6つの対策~

暗号化と認証の他にも、有効なセキュリティ対策が存在します。
ここでは、無線LAN運用者ができる対策を6つ紹介します。

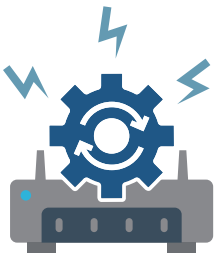
1 パスワードの適切な運用

企業ネットワーク　ゲストネットワーク

無線LANの暗号化には複数の方式がありますが、多く利用されているのが「PSK方式」です。この方式では、アクセスポイントに接続する人全員が同じ暗号化パスワードを共有することになります。手軽に利用できる一方、パスワードさえ知っていれば誰でも接続できてしまうという危険性があります。
企業ネットワークでPSK方式を採用する場合、推測されにくい、20文字以上のパスワードを設定することが基本です。
ゲストネットワークの場合、パスワードを掲示して誰もが知りうる状態にしてあると暗号化は無意味となるため、無線LANの利用者にパスワードを記した用紙を個別に配布するなど、パスワードを知りうる人を最小限に留める工夫が必要です。

2 ファームウェアの更新

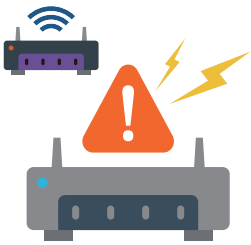
企業ネットワーク　ゲストネットワーク



ファームウェアは常に最新のバージョンに更新しておきましょう。
無線LANには脆弱性も存在します。脆弱性を放置すると、外部から攻撃を受けたりウイルスに感染する可能性もあるなど、非常に危険です。脆弱性に対しては、メーカーが更新プログラムを提供して対策を施します。そのため、こまめにファームウェアを最新のものに更新することで、脆弱性から身を守ることができます。

3 不正なアクセスポイントを対策

企業ネットワーク　ゲストネットワーク



どれだけセキュリティ対策を施した無線LANを導入しても、不正なアクセスポイントが設置されそちらに接続してしまっては元も子もありません。
対策としては、不正なアクセスポイントを検知する機能を搭載したアクセスポイントを導入し、万一不正なアクセスポイントが設置された場合、アラートで知らせてくれるようにする方法があります。

無線LANのセキュリティリスク
~その他6つの対策~

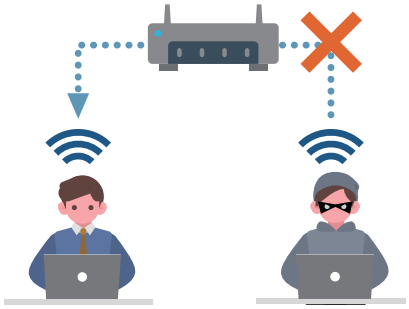
4 ステルスSSID

企業ネットワーク

ステルスSSIDとは、第三者が受信する無線LANのSSIDのリストに、自分のSSIDを掲載させない技術です。無線LANへの接続にはSSIDとパスワードを入力することが必須ですが、この機能により認証を受けていない周囲の端末からSSIDを隠すことができるので、ゲストや攻撃者からの企業ネットワークへのアクセスを防ぐことができ、一定のセキュリティを確保できます。

5 端末同士の通信禁止

ゲストネットワーク



不特定多数の人が接続するフリーWi-Fiなどのゲストネットワークでは、同じアクセスポイントに接続した端末同士が通信可能な状態であるとセキュリティ上の大きなリスクとなります。一般的なアクセスポイントには、同じアクセスポイントに接続した端末の相互の通信を遮断する機能が搭載されているため、公衆無線LANを提供する場合は必ず設定しましょう。

6 ネットワークの分離

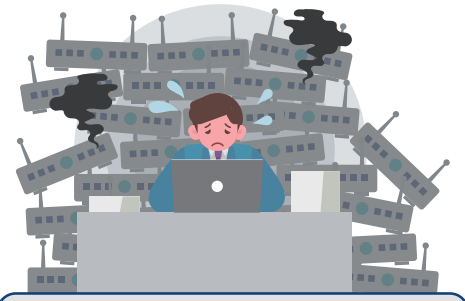
ゲストネットワーク

業務用に利用しているネットワークを公共に提供せず、物理的もしくは論理的に業務用とゲスト用のネットワークを分離しましょう。設定に不備があり、そこから業務ネットワークに接続されるケースがあります。ゲスト用に公衆無線LANを構築する場合、しっかりと業務ネットワークと分離されているかチェックしましょう。

無線LAN運用の負担

ここまで、無線LANのセキュリティ対策を紹介してきましたが、いざこれらのセキュリティ設定を施しながら無線LANを運用しようと思っても、簡単なことではありません。
多拠点に散らばる機器ひとつひとつにセキュリティ設定やファーム更新を施すために、その都度エンジニアを派遣するには、膨大な時間とコストがかかります。
また、運用すべきITシステムが増大する中で、IT人材は不足しており、運用に人材を割くことが負担になりかねません。

個別管理による無駄な工数

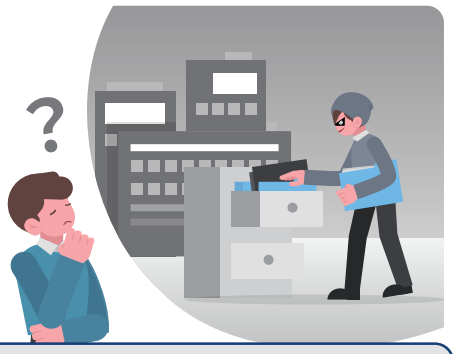


機器ごとに設定、ファーム更新、
ログ確認 etc...
何かと時間がかかる...

遠方拠点への無駄な移動コスト

遠方にエンジニアを行かせると
コストがかかり過ぎる...

セキュリティが心配



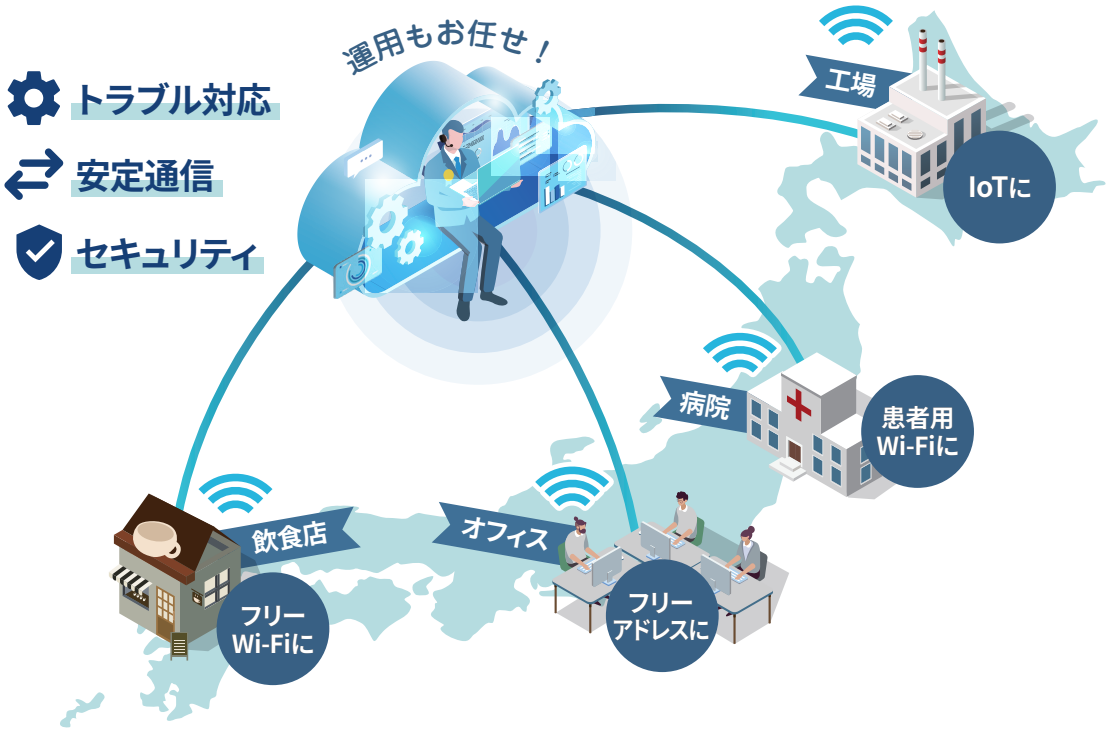
サイバー攻撃が増えてるけど、
大丈夫かな...

ITシステムの増大による人材不足

DX推進、IT運用、
セキュリティ対策etc...
人が足りない...

クラウド無線LAN Hypersonix®

網屋のHypersonix なら、無線LAN運用の負担を丸ごと解決することができます。Hypersonixは、無線LANの導入・運用を丸ごと委託できるサービス。クラウドから各種設定や運用・監視を行うので、急なトラブルや設定変更に現地にエンジニアを派遣する必要がなく、お客様のお手を煩わせることはありません。複雑なセキュリティ設定もプロが代行するため、安心してご利用いただけます。



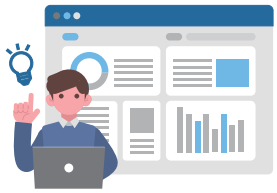
設計・構築をお任せ

- 初期設定/導入/構築
- デバイス毎の接続設定相談
- MACアドレス登録、変更、削除
- 干渉波フィルタリング
- チャネルチューニング

セキュリティをお任せ

- AD/RADIUS認証などの適用
- ステルスモードの運用
- 各種セキュリティ設定代行

運用をお任せ

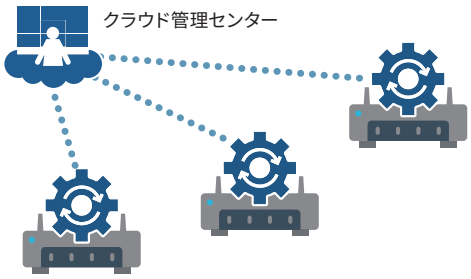


- 切断/遅延の回避
- ファームウェアのアップデート
- 無線アクセスポイントの死活監視
- 電話・メールでの障害切り分け
- ログの記録/保管
- 機器故障時の代替機器送付
  ※先出しセンドバック

セキュリティ機能が満載！

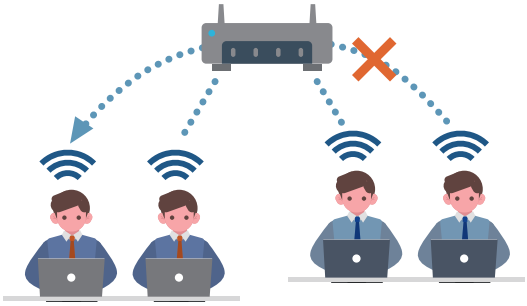
Hypersonixなら、セキュリティ機能が満載。
安心してお使いいただけます。

自動ファーム更新



セキュリティホールをふさぐファームの更新は、セキュリティに必須。しかし手が回らないことも。
Hypersonixなら、クラウド管理センターが最新のファームを自動で適用します。

セパレータ機能



同一セグメント間の通信を遮断できるため、内部デバイス間を相互通信させずに許可された端末のみ接続させることが可能です。そのため、フリーWi-Fiにも安心してお使いいただけます。

ステルス機能

SSIDが見えるだけで外部からの攻撃リスクは増大。
Hypersonixなら、ステルス機能で未承認の端末からSSIDを不可視化します。

その他のセキュリティ機能

SSID認証
アクセスポイントに接続できるユーザーを限定

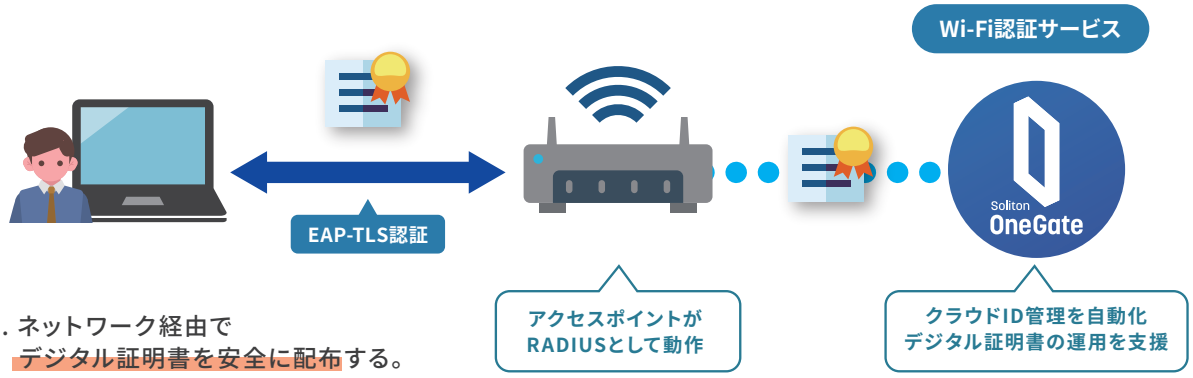
AD/RADIUS認証
認証基盤を利用して、ユーザー単位でネットワークアクセスを制御

MAC認証
許可された端末のみ無線LANへ接続を許可

VLAN機能
ネットワーク分割で業務用無線LANとゲストWi-Fiの分割も可能

OneGate連携で認証の強化を

前述の通り、企業ネットワークには証明書を使った認証がオススメです。
Hypersonix（※1※2）なら、ソリトンシステムズ社が提供する認証サービス「OneGate」と連携し、デジタル証明書による認証を実現することができます。認証機器やサーバ不要で、スピーディーに認証基盤の構築が可能。安全性と運用性の両面に優れ、悪意あるユーザーや不適切な端末の侵入を防ぎます。



1. ネットワーク経由で
   デジタル証明書を安全に配布する。
2. 無線アクセスポイントと連携して
   デジタル証明書による認証を行う。

認 証　デジタル証明書による認証

- OneGateは「デジタル証明書による認証」(EAP-TLS) に対応する認証サービスです。
- アクセスポイントがRADIUSとして動作し、ミニマム構成で認証を実現できます。

管 理　管理用Webサイト

- ユーザ/デバイスごとに発行されるデジタル証明書の管理（アカウント作成/配布/更新/失効）を低負荷で導入できます。
- 認証に使用するデジタル証明書を安全かつ効率的に配布する仕組みもあわせて提供します。

不正対策　シャドーIT対策

- ユーザ/デバイスごとに個別の情報で認証されるため、社員の持ち込みデバイスが接続されるなどのシャドーIT対策を実現します。
- 退職や異動、デバイスの紛失時にも迅速に該当アカウントの消去が可能です。

※1 ベーシックタイプを除く。
※2 スタンダードタイプは認証機器（EPS-edge）の購入が必要です。

無線LANには適切な対策を

おわりに

本書では、無線LANのセキュリティリスクと、無線LANを安全に利用・提供するためのセキュリティ対策を紹介してきました。
無線LANは便利である反面、セキュリティ対策を施さないまま提供・利用していると、多大なリスクにさらされることとなりますが、適切な対策を実装することで、多くのリスクを回避することができます。
ぜひ、本書で紹介したセキュリティ対策を実施し、安全に無線LANを提供・利用してください。

本書のまとめ

- **無線LANには多くののセキュリティリスクが潜んでいる**
- **セキュリティ対策にはまず「暗号化」と「認証」の強化**
- **暗号化と認証の強化に加え「6つの対策」を**
- **無線LANの運用はプロに任せて安心**

お問い合わせ先

株式会社網屋
ネットワークセキュリティ事業部
TEL：03-6822-9995　E-mail：infra-sales@amiya.co.jp

詳しい製品概要資料はこちら ＞

開発元

株式会社 網屋

〒103-0007 東京都中央区日本橋浜町3-3-2 トルナーレ日本橋浜町 11F
TEL: 03-6822-9999 FAX: 03-6822-9998
https://www.amiya.co.jp/

Hypersonixは株式会社網屋の登録商標です。
記載された製品の仕様・機能等は改良のため予告なく変更される場合があります。
このパンフレットの内容の一部またはすべての複写・転用・転載等を株式会社網屋に無断で行った場合、著作権の侵害になります。