

無線LANについて ～無線LANを安全に使うための対策～

無線LANについて ～無線LANを安全に使うための対策～

Part2: 従業員としての対策 — No. 9

導入



最近では、様々な場所に設置されている無線LAN。
通信データの使用量を気にする利用者にとっては非常に便利ですが、無線LANを利用する場合の危険
を認識しておく必要があります。

導入



適切なセキュリティ設定が施されていない無線LANや、悪意を持った攻撃者が設置した無線LANに接続してしまうと、通信内容を読み取られる、偽のウェブサイトへ誘導される、犯罪行為に悪用される、といった被害を受ける可能性があります。また、適切なセキュリティ設定を施していない無線LANを社内に設置してしまうと、部外者に無断でネットワークやインターネット環境を使用されてしまうかも知れません。

導入




街中にある無料の公衆無線LANも、使う際には注意が必要です。
安易に使用するとこんな危険な目に遭うかもしれません・・・。

事例

失礼します。

事例

A woman with long brown hair and bangs, wearing a dark blue business suit over a light pink shirt, is standing in front of a wall made of glass blocks. She has her arms raised high in the air and is smiling broadly, appearing to be celebrating. A black shoulder bag is visible on her left side. The background shows a bright, sunny outdoor street scene with trees and buildings.

あー終わったー。さあ早く
帰って次の仕事を……。

事 例


あー！！



事例

いっけなーい！〇〇時までに
送らなきゃいけない大事なメール、
忘れてた！！

事例



打合せが押しちゃったから・・・
どうしよう、会社に戻ったら
間に合わなくなっちゃうし・・・。

事例

そうだ！
近くのカフェにあるかな？
無線LAN。




事例

よかった、間に合った。
もう一息入れたら会社戻ろっと。

数十分後。

事例



本当に助かったのよ、
そのお店に無料で使える無線LANがあつて。

1時間後。

事例

へー、斉藤さんにしては機転が利いたね、
無料の無線LANを使うなんて。

事例

でしょー！？
ノートパソコンの無線LANの機能を
思い出して使えるかなー？って。



事例

仕事とは言え、
社外の公衆無線LANを
使ったのはよろしくなかったな。


事例

たしかに、街中には
無料で使える無線LANが
増えていて便利にはなった。

しかし、安易に仕事で使っている
パソコンを接続して使用するのは
危険が多すぎるよ。




事例



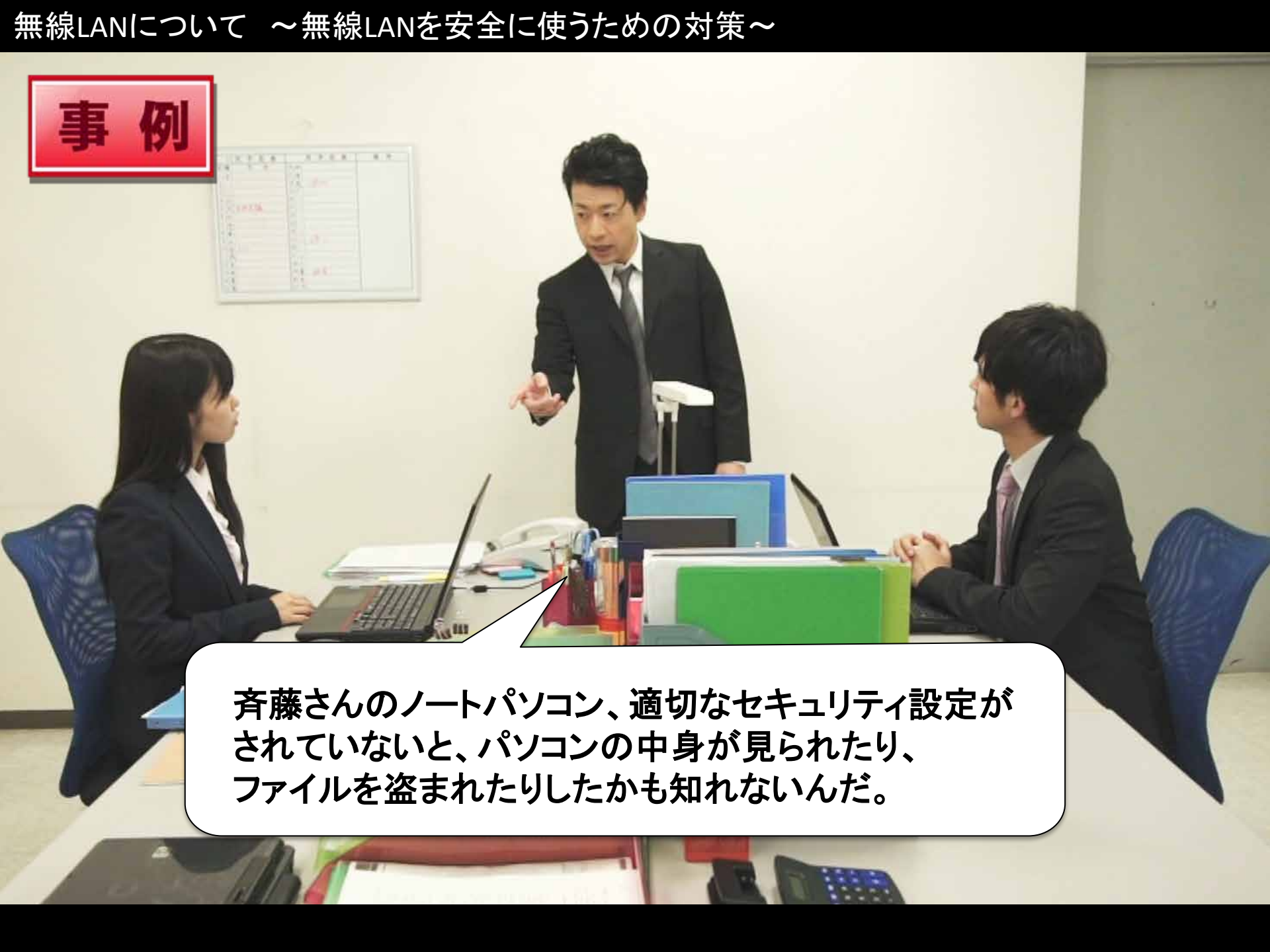
危険で…
なんですか？

事例

A man in a dark suit and tie stands in the center of an office, gesturing with his right hand as he speaks. He is facing two colleagues seated at a large white table. On the left, a woman with long dark hair, also in a dark suit, is looking towards the man. On the right, a man with dark hair, wearing a dark suit and a pink tie, is also looking towards the man standing. The table is cluttered with various office supplies, including blue and green folders, a laptop, and a calculator. In the background, a whiteboard with some writing is visible on the wall.


斉藤さんが使用した無線LANの
セキュリティ設定が疎かだったとしたら、
斉藤さんが送ったメールの内容が覗き見
されていたかも知れない。

事例

A man in a dark suit and tie stands in the center of an office, gesturing with his right hand as he speaks. He is facing two colleagues seated at a desk. On the left, a woman with long dark hair, wearing a dark blazer, sits with her back to the camera, looking towards the man. On the right, a man with dark hair, wearing a dark suit and a pink tie, sits with his hands clasped, looking at the standing man. The desk is cluttered with various items: a laptop, several colorful folders (blue, green, red), a pen holder with pens, a calculator, and some papers. In the background, a whiteboard with some writing is visible on the wall.


齊藤さんのノートパソコン、適切なセキュリティ設定が
されていないと、パソコンの中身が見られたり、
ファイルを盗まれたりしたかも知れないんだ。

事例



ええ～！？
メールを1通送るのに使っただけなのに、
そんなに危険なことだったなんて…。

学習の意図



スマートフォンやタブレット、携帯型ゲーム機の普及に伴って、使用できる所が多くなってきた公衆無線LANですが、中にはセキュリティ設定が疎かなものや、悪意を持った攻撃者が設置したものがあるかも知れません。使用する際はパスワードや個人情報を入力したり表示したりするサイトは見ないなどの注意が必要です。

学習の意図

通信の暗号化がされていないものや、暗号化の強度が低いものなど、セキュリティ設定が疎かな無線LANを使用すると、通信のやり取りを覗き見されてしまいます。

学習の意図



また、悪意を持った攻撃者が設置した無線LANに、誤って接続してしまうと、通信のやり取りを覗き見される、偽のウェブサイトへ誘導される、接続してきた機器の中身を覗かれてしまう、などの行為を攻撃者から受けてしまいます。ただし、このような無線LANを見分けることは難しいと思ってください。

学習の意図



社内で無線LANを設置して使用する場合も、セキュリティ設定を怠ってはいけません。誰でも簡単に接続可能な設定にしておくと、部外者が無断で接続して、ネットワークやインターネット環境を勝手に使われてしまいます。

学習の意図

「無線LAN」について、以下を学習しましょう。

1. 無線LANは通信の暗号化がされているものを使用する。
2. 設置した無線LANに他人を無断で接続させない。

正しい対処法



無線LANを使用する際、かならず通信の暗号化が施されているものを選びましょう。暗号化の中でも強度の高い、「WPA3」または「WPA2」の「AES」や「PSK」、「WPA」の「AES」や「PSK」を選んで下さい。脆弱性が発見されていて、簡単に暗号が解読されてしまう「WEP」は使用しないで下さい。接続する機器によっては、無線LANの一覧表示時に「セキュリティの保護」や、鍵マークが表示されますので、こうした表示を目安に選びましょう。

用語解説

●WPA

WPA（Wi-Fi Protected Access）は、無線LANの業界団体 Wi-Fi Alliance によって発表された無線LANの暗号化方式の規格。WEPより暗号化鍵の鍵長を長くする、ユーザの認証方式を強化する、などWEPの弱点が補われ、セキュリティが向上している。WPA3は、WPAやWPA2をさらに強化したもの。セキュリティ強度の高いWPA3またはWPA2を使用することが望ましい。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著者：独立行政法人情報処理推進機構

発行：実教出版株式会社

用語解説

●AES

Advanced Encryption Standard。2001年、米国政府によって選定された米国政府標準のブロック暗号。ブロック長（情報の処理単位）は128bitで、鍵長は、128bit、192bit、256bitの3種類がある。国際標準ISO/IEC18033の共通鍵暗号アルゴリズムの1つとして標準化された。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著者：独立行政法人情報処理推進機構

発行：実教出版株式会社

●WEP

Wired Equivalent Privacy。無線LANの暗号通信機能。WEPキー（40bitまたは104bit）と呼ばれる共通の暗号鍵を無線LANカードとアクセスポイントに事前に設定しておき、暗号化通信を行う。複数の重大かつ深刻な脆弱性（ぜいじゃくせい）が報告されているため、使用すべきではない。

【出典】

情報セキュリティ読本 IT時代の危機管理入門（六訂版）

著者：独立行政法人情報処理推進機構

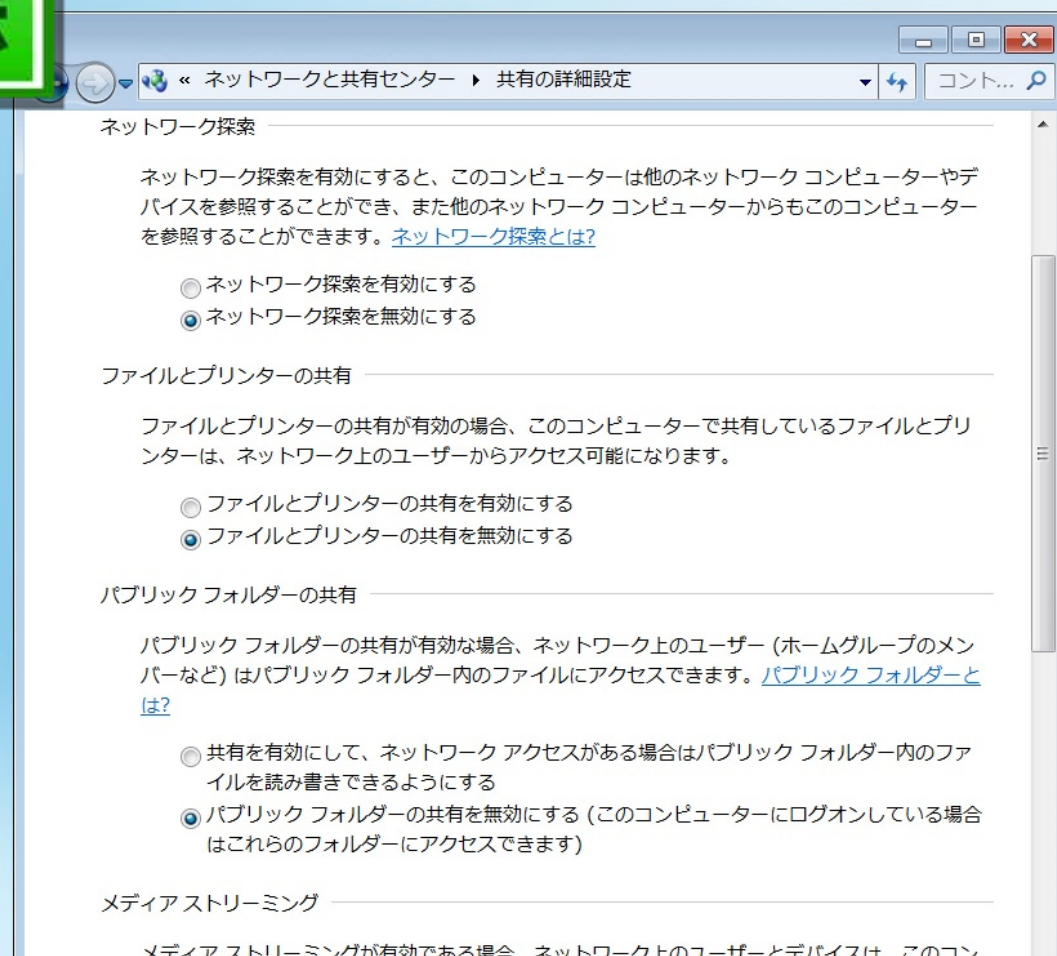
発行：実教出版株式会社

正しい対処法



社内で無線LANを設置して使用する場合も、強度の高い通信の暗号化を設定しましょう。また、無線LANと接続する際に設定するパスワードは、辞書に載っていない、それだけでは意味をなさない、推測困難な文字列にしましょう。

正しい対処法



無線LANにパソコンを接続する場合、ファイル共有機能を有効にしていると、同じ無線LANに接続している他人から、パソコンの中身を覗かれてしまいます。無線LANに接続する際は、ファイル共有機能は無効にしておきましょう。

正しい対処法



悪意を持った攻撃者が設置した無線LANを、見抜くことはまず無理でしょう。接続するのに少しでも不安があれば、接続をしないことです。それでも無線LANを使う場合は、他人に見られては困る内容の入力や表示は行なわないことです。無線LANは、他人と共有して使うため、たとえセキュリティ設定が施されている無線LANでも、通信の内容が他人に見られている可能性があることを自覚して使うべきです。

確認テスト 問題

No.9 無線LANについて ～無線LANを安全に使うための対策～

Q1

無線LANについて、不適切なのはどれでしょうか。

選択肢

- | | |
|--|---|
| | 1. 無線LANは、暗号化が施されているものを選ぶのはもちろん、暗号強度の高いものを選ぶ。 |
| | 2. 急ぎの仕事があったので、街中の無線LANを使って顧客とメールのやり取りを行なった。 |
| | 3. 無線LANに接続する時は、他人に見られないよう、ファイル共有機能を無効にする。 |
| | 4. 社内などで設置した無線LANは、暗号強度の高いものを設定し、パスワードを推測困難な文字列にする。 |

次のページで正解と
解説を確認しましょう

確認テスト 正解と解説

Q1

無線LANについて、不適切なのはどれでしょうか。

正解	選択肢
	1. 無線LANは、暗号化が施されているものを選ぶのはもちろん、暗号強度の高いものを選ぶ。
●	2. 急ぎの仕事があったので、街中の無線LANを使って顧客とメールのやり取りを行なった。
	3. 無線LANに接続する時は、他人に見られないよう、ファイル共有機能を無効にする。
	4. 社内などで設置した無線LANは、暗号強度の高いものを設定し、パスワードを推測困難な文字列にする。

【解説】

街中にある無線LANは、暗号化が施されていないものや、悪意を持った攻撃者が設置したものがあるかも知れません。個人情報や秘密情報など、他人に見られたくない内容の情報をやり取りすることは、情報漏洩(ろうえい)の危険がつきまとうので控えましょう。