



サイバーセキュリティの置き薬

2020年
第20号

「Wi-Fi提供者向けセキュリティ対策の手引き」 について総務省から改定版が公表されています

Wi-Fi 提供のリスクや具体的な対策等を確認し、実際の環境に応じたセキュリティ対策をとるための参考として、この手引きを紹介します。



適切なセキュリティ対策とは

◇利用者の安全を守るために

- セキュリティの周知啓発
- 強固な暗号化を導入する（WPA2 や WPA3 等）
- 公衆無線 LAN（Wi-Fi）端末同士の通信を遮断設定する
- 偽アクセスポイント対策（認証画面を https 化し、その URL を周知）



◇不正利用防止のために

- ネットワーク機器を厳重に管理し、最新のファームウェアで運用する
- 業務用のネットワークと Wi-Fi 提供用のネットワークは分離する
- 利用者情報の確認や認証の仕組み（下記のいずれかの利用者認証方式）を導入する
 - ・ 利用していることの確認を含めたメール認証方式
 - ・ SNS アカウントを利用した認証方式
 - ・ SMS 連携方式

◇万が一悪用された時のために

- アクセスログを長期保存する

Wi-Fi 利用者の約 3 分の 2 が、利用に不安を感じているという調査結果があります。Wi-Fi 提供者は、Wi-Fi 利用者が安心して使うための適切な情報（利用条件やセキュリティ対策の有無等）の提供をお願いします。

【参考サイト】

総務省「Wi-Fi 提供者向け セキュリティ対策の手引き」

https://www.soumu.go.jp/main_content/000690267.pdf

