

事務連絡
令和2年6月4日

各
〔都道府県
保健所設置市
特別区〕
医政主管部（局） 御中

厚生労働省医政局研究開発振興課

無線 LAN のセキュリティに関するガイドラインの周知について（依頼）

日頃より医療分野の情報化に関し、格別のご配慮を賜り、厚く御礼申し上げます。
今般、総務省より別添1のとおり、無線 LAN のセキュリティに関するガイドラインについて、ICT の利活用が進みつつあることを鑑みて、病院等に対して幅広く周知するよう依頼がございましたので、周知いたします。

なお、当該ガイドラインの内容のうち、医療機関で重要となる対策のポイントを別添2のとおり整理しましたので、あわせてご活用ください。

貴部（局）におかれましては、本ガイドラインを管内の医療機関等に対してご周知いただきますようご協力方よろしくお願いいたします。

なお、本周知は別途、公益社団法人日本医師会、公益社団法人日本歯科医師会、一般社団法人日本病院会、公益社団法人全日本病院協会、一般社団法人日本医療法人協会、公益社団法人日本精神科病院協会宛にも送付しておりますので申し添えます。



別添 1

総務統第106号

令和2年5月29日

厚生労働省医政局長

吉田 学 殿

総務省サイバーセキュリティ統括官

竹内 芳明



無線LANのセキュリティに関するガイドラインの周知について（依頼）

日頃より当省の業務に御理解と御協力をいただき誠にありがとうございます。

当省では、無線LANの利用者及び提供者において、無線LANを安全に利用又は提供するために必要となるセキュリティ対策等に関する理解を深めていただくことを目的として、無線LANのセキュリティに関するガイドライン（「Wi-Fi利用者向け 簡易マニュアル」及び「Wi-Fi提供者向け セキュリティ対策の手引き」）を策定しているところです。

今般、新技術や最新のセキュリティ動向に対応するため、当該ガイドラインの見直しを行い、令和2年5月版として改定の上、次のURLにて公表しています。

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

つきましては、安全・安心に無線LANを利用できる環境の整備に向けて、利用者及び提供者の双方に対してのセキュリティ対策に関する周知啓発を図っていく必要があることから、ICTの利活用が進みつつあることに鑑みて、病院等に対して幅広く、当該改定後のガイドラインの内容を周知していただきますようお願いいたします。

「Wi-Fi提供者向けセキュリティ対策の手引き」で医療機関で特に重要と考えられる対策

来訪者向けWi-Fiと業務用無線LANは分離しましょう
また、機器管理用PWは推測されにくいものを設定しましょう

無線LANの暗号化パスワードを掲示等する場合は
解読リスクがあることを認識しましょう

設定の書き換え、
アクセスログの盗難

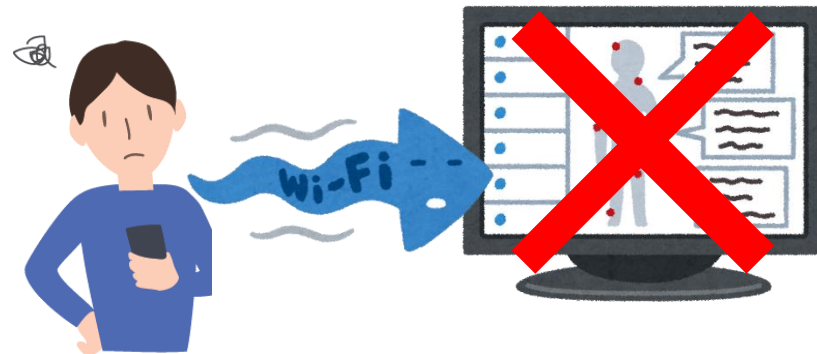


意図したエリア内に限ってサービスが提供されるように、電波の出力等について適切に調整しましょう（電波漏れ等のリスク）

混雑を避けるために周波数やチャンネルをよく検討しましょう
（業務用Wi-Fiや患者持込の回線との干渉リスク）



混雑により、データ入力中に切断して入力し直し



エリア外で勝手に利用され、悪意ある利用がされることも

セキュリティ対策を徹底し、大切な情報を守りましょう！

総務省「無線 LAN のセキュリティに関するガイドライン」における
医療機関で重要となる対策のポイント

今般、総務省が見直しを行った「無線 LAN のセキュリティに関するガイドライン」について、医療機関で特に重要と考えられる対策は、以下のとおり。

- ・ 来訪者向け Wi-Fi と業務用無線 LAN は分離すること
- ・ 機器管理用パスワードはして推測されにくいものを設定すること
- ・ 無線 LAN の暗号化パスワードを掲示等する場合は解読リスクを認識すること
- ・ 混雑を避けるために周波数やチャンネルをよく検討すること（業務用 Wi-Fi や患者持込の回線との干渉リスク）
- ・ 意図したエリア内に限ってサービスが提供されるように、電波の出力等について適切に調整すること（電波漏れ等のリスク）

「Wi-Fi 提供者向け セキュリティ対策の手引き」に記載されている主な対策（例）

頁数	題 名	対 策 内 容
P.3	2-1. 利用者への周知啓発	<ul style="list-style-type: none"> ・ 提供者側での十分なセキュリティ対策 ・ 利用者に対する周知啓発（「Wi-Fi 利用者向け簡易マニュアル」の周知等）
	2-2. 暗号化の実施とパスワードの伝達方法	<ul style="list-style-type: none"> ・ WPA2 による暗号化（パスワードを掲示等して誰もが知りうる状態にした際のリスクに注意） ・ 提供状況とリスクを総合的に判断し暗号化を実施しない場合は、利用者への適切な周知
P.5	2-3. 利用者の端末を保護するための端末同士の通信禁止	<ul style="list-style-type: none"> ・ 同じアクセスポイントに接続した端末同士の相互通信の禁止（状況に応じて検討）
	2-4. 偽アクセスポイント対策	<ul style="list-style-type: none"> ・ 利用者が正しいアクセスポイントであるかが分かるよう、認証画面の https 化や URL の周知
P.6	3-1. Wi-Fi 機器の適切な運用	<ul style="list-style-type: none"> ・ 管理者パスワードを第三者に推測されにくいものに変更 ・ 機器のファームウェアの更新（運用時の定期的な確認）
	3-2. 業務用ネットワークとの分離	<ul style="list-style-type: none"> ・ Wi-Fi 提供用ネットワークと業務用ネットワークの分離
P.7	3-3. 利用者情報の適切な確認	<ul style="list-style-type: none"> ※不特定かつ多数の利用者が利用する場合における、メールアドレスや SNS アカウント等を使っ

頁数	題名	対策内容
		た利用者識別が紹介されているが、患者や来訪者向けに Wi-Fi を提供するのであれば、取得する個人情報は最小限とすること、必要以上に取り過ぎないことに注意。
P.9	3-4. アクセスログの記録・保存	<ul style="list-style-type: none"> ・アクセスログはプライバシー性が高く、業務目的に照らして必要最小限で記録 ・利用者への同意なく外部へ提供できないが、礼状に従う場合は警察等に提供することが可能 ・Wi-Fi の運用を他の事業者に委託している場合は記録内容や保存期間等を把握し、問い合わせがあった際の対応方法を委託先と確認しておく
	3-5. その他の対策	<ul style="list-style-type: none"> ・接続 1 回当たりの利用時間制限 ・メール送信制限 等
P.10	4-1. Wi-Fi 利用者が安心して使うための適切な情報の提供	・利用者に対し、提供者・利用条件（料金・利用時間等）、セキュリティ対策の有無と内容（暗号化方式等）、Wi-Fi の危険性と安全な使い方（偽アクセスポイントの注意喚起等）を周知
	4-2. 青少年有害情報のフィルタリング	・フィルタリングを提供・販売するサイトの紹介等
	4-3. 法令に準拠した個人情報保護・通信の秘密保護	・アクセスログも含む利用者の情報を厳格に管理する法的な責任
P.11	5 より使いやすい Wi-Fi の提供に向けて	<ul style="list-style-type: none"> ・混雑を避けるために周波数やチャンネルをよく検討（業務用 Wi-Fi や患者持込の回線と干渉するリスク） ・施設内にのみ電波が届くように電波出力の調整

※ Wi-Fi（ワイファイ）とは、無線 LAN の普及促進を行う業界団体である Wi-Fi Alliance から認証を受けた機器のこと。現在は認証を受けた機器が増えたことから、無線 LAN 全般を指して Wi-Fi ということもあり、本手引きでもその意味で使用。また、本手引きでは、「Wi-Fi によるインターネット接続サービス」も「Wi-Fi」と表記。