資料23－３

無線LAN及びテレワークにおける セキュリティ対策の強化について

総務省
サイバーセキュリティ統括官室

令和２年４月16日

無線LANのセキュリティガイドラインの見直しについて

- 総務省では、無線LANの提供者・利用者向けにガイドラインを作成しており、周知啓発に活用。
- 新技術や最新のセキュリティ動向に対応するため、内容を見直し予定。

「Wi-Fi利用者向け 簡易マニュアル」（2015年３月版）の見直しポイント

- ✓ セキュリティ対策の訴求点を明確にするため、**セキュリティ対策のポイント**を**整理**
  - ① 接続する**アクセスポイントをよく確認**（偽アクセスポイント対策として接続URL等を確認）
  - ② **原則HTTPS通信**の利用を（Wi-Fi暗号化等に関わらず通信内容を保護）
  - ③ 自宅に設置する**Wi-Fi機器の設定**に注意（管理用パスワードの変更等）
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

「Wi-Fi提供者向け セキュリティ対策の手引き」（2016年８月版）の見直しポイント

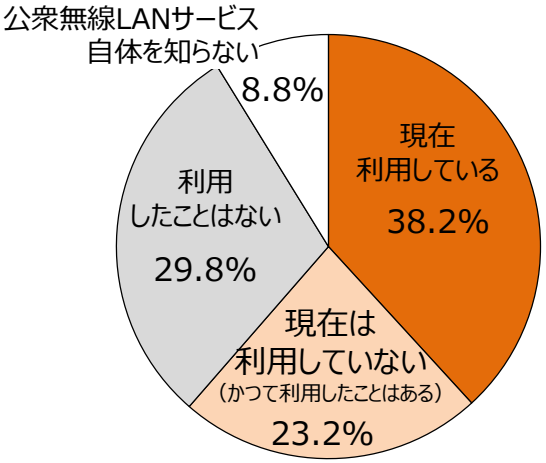
- ✓ ガイドラインの対象者の明確化（**自店利用者のみへの提供する者も対象**）
- ✓ 近年懸念されている**偽アクセスポイント対策**（認証画面のURLの周知等）を追記
- ✓ 暗号化のための**パスフレーズを公開**している場合解読の**リスクが高まる**ことを明示
- ✓ 状況に応じたセキュリティ対策の選択と**利用者への周知**が必要であることを明確化
- ✓ セキュリティ関連の**新技術**（WPA3、Enhanced Open等）を**紹介**

➡ **改定後はWi-Fi提供者（医療機関、宿泊施設、教育機関等を含む）等に改めて周知予定。**

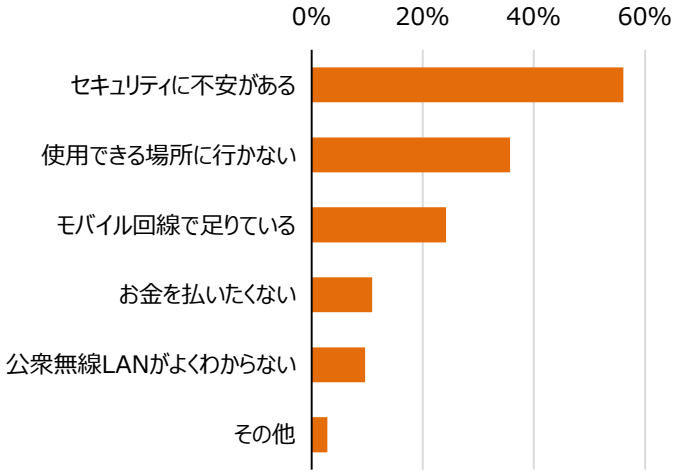
（参考）公衆無線LAN利用者意識調査

➢ 利用者の公衆無線LANに対するセキュリティ意識等を把握するための調査をWebアンケートにより実施。
（対象地域：全国　期間：2020年2月13日～17日　調査数：31,112（無線LAN利用者1,392をスクリーニング調査））

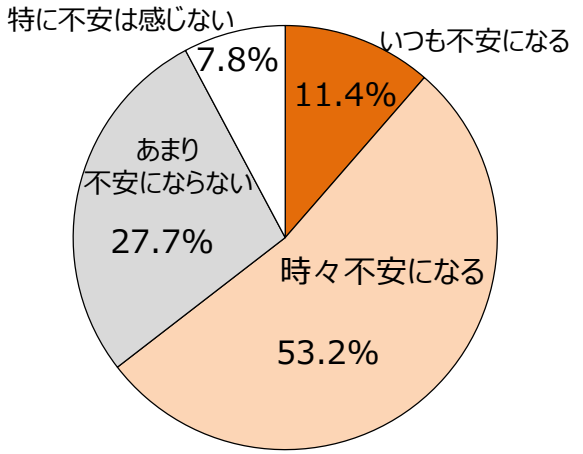
公衆無線LANを利用しているか
（n=31,112）



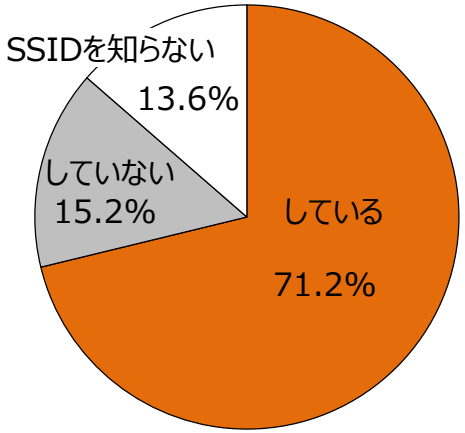
公衆無線LANを利用しなかった理由
（n=16,473：現在未利用者）



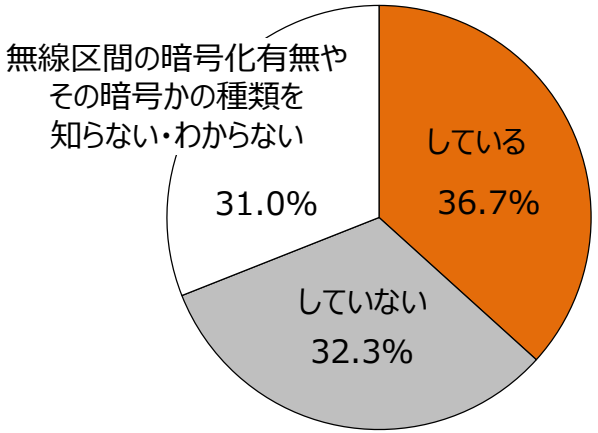
公衆無線LANで不安を感じるか
（n=1,392：公衆無線LAN利用者）



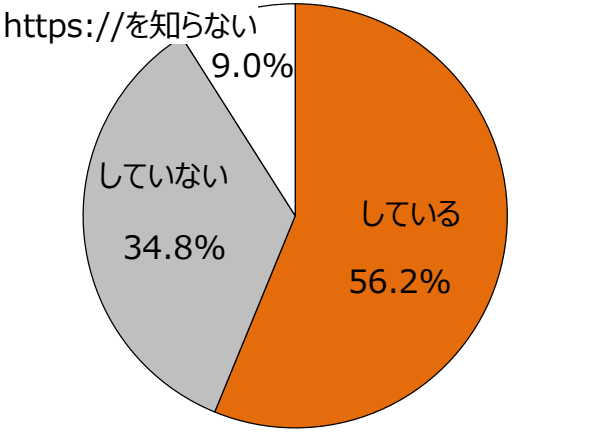
公衆無線LAN利用時のSSID確認
（n=1,392：公衆無線LAN利用者）



公衆無線LAN利用時の暗号化確認
（n=1,392：公衆無線LAN利用者）



公衆無線LAN利用時のhttps確認
（n=1,392：公衆無線LAN利用者）



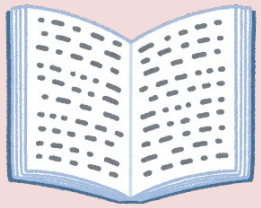
テレワークにおけるセキュリティ対策の強化

- 総務省では「**テレワークセキュリティガイドライン**」を**策定**し、**セキュリティ対策の考え方**を示している。
- 新型コロナウイルスの影響により、これまで未導入だった中小企業等においてもテレワークの導入が広まる中で、より**具体的で分かりやすく、実践的な内容のチェックリスト**が求められており、**策定に向けた検討を開始予定**。
- またチェックリスト策定と併せ、**セキュリティ対策**に関する**専門的な相談に対応できる窓口**を設ける予定。

テレワークセキュリティガイドライン
（平成30年４月総務省策定）

チェックリスト形式による具体化例（イメージ）

抽象度の高い一般的な記載
（例）
「ファイアウォールを設置し
不必要なアクセスを遮断する」

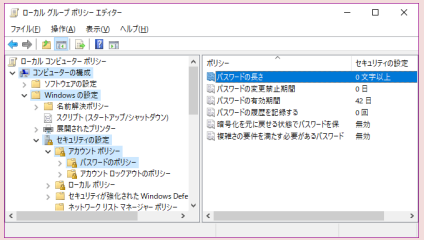


チェックリスト形式による具体化（例）
- ☐ ファイアウォール機能を有効にする
- ☐ NAT機能を有効にする
- ☐ DNSフィルタリング機能を有効にする
- ☐ UPnP機能を無効にする　　等

設定例（パラメーター）の具体化例（イメージ）

考え方・方針について記載
（例）
「パスワードは一定以上の長さ
で推測されにくものを用いる」

具体的な設定例の解説（例）
Windowsに備わる
LGPE機能を使用して
一定のパスワード長を
強制することが可能



これからテレワークを導入する企業のセキュリティ対策の参考となるだけでなく、
テレワーク導入済企業におけるセキュリティ対策の自己チェックへの活用も可能

（参考）テレワーク関連情報の周知について

総務省トップページ
https://www.soumu.go.jp/

新型コロナウイルス感染症対策としてのテレワークの積極的な活用について
https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/02ryutsu02_04000341.html

はじめに

新型コロナウイルスの感染の拡大を防止するためには、多くの人が集まる場所での感染の危険性を減らすことが重要です。通勤ラッシュや人混みを回避し、在宅での勤務も可能となるテレワークは、その有効な対策の一つです。

2月25日には新型コロナウイルス感染症対策本部において、新型コロナウイルス感染症対策の基本方針が決定されました。当該基本方針に基づき、患者・感染者との接触機会を減らす観点から、可能な限り、テレワークの積極的な活用をお願いします。

（参考）内閣官房 新型コロナウイルス感染症対策推進室ホームページ

テレワーク関連支援情報

総務省をはじめ関係省庁等においてテレワーク導入に向けた支援を実施しています。

○総務省令和2年度 テレワークマネージャー相談事業【総務省】
https://www.nttdata-strategy.com/r01telework/
Web会議・電話にて、テレワークに適したシステム（在宅勤務などを行うためのICT機器、システム）や情報セキュリティ、勤怠労務管理、その他テレワーク全般に関する情報提供・相談を行っています。

○テレワーク緊急導入支援プログラムのご紹介【一般社団法人日本テレワーク協会】
https://japan-telework.or.jp/anticorona_telework_support/
テレワークを緊急導入される企業等向けに、日本テレワーク協会の会員企業・団体によるテレワーク緊急導入支援プログラムを紹介します。

○テレワークお役立ち情報
https://www.soumu.go.jp/main_content/000675457.pdf
関係省庁等における新型コロナウイルス感染症対策におけるテレワーク導入に関するお役立ち情報をまとめたリーフレットです。

テレワークにおけるセキュリティ確保

新型コロナウイルスの混乱に乗じたサイバー攻撃も確認されています。テレワークの実施に当たっては、適切なセキュリティ対策をお願いします。

「テレワークセキュリティガイドライン」の紹介

○テレワークセキュリティガイドライン（第4版）【総務省】
https://www.soumu.go.jp/main_content/000545372.pdf
テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示しています。

○テレワーク実施者の方へ【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/security-site/telework/
テレワークを実施される方に対して、セキュリティ上注意すべき基本的なポイントを簡潔にまとめています。

NISCからの周知情報

○インターネットの安全・安心ハンドブック【内閣サイバーセキュリティセンター】
https://www.nisc.go.jp/security-site/handbook/
インターネットの利用に当たっての一般的な留意点を、ハンドブックとして示しています。

○Wi-Fi（無線LAN）の安全な利用について【総務省】
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/wi-fi.html
Wi-Fiの利用に当たっての一般的な留意点を、利用者・提供者双方の観点からガイドラインとして示しています。

Wi-Fiガイドラインの紹介

関係機関からの注意喚起情報

○各種注意喚起等情報
関係機関が発出するテレワーク関連の主な脆弱性情報等について掲載しています
・Zoomの脆弱性対策について【IPA】
https://www.ipa.go.jp/security/cladr/vul/alert20200403.html
・新型コロナウイルスを題材とした攻撃メールの例【IPA】
https://www.ipa.go.jp/security/announce/20191202.html#L12

そのほか

○テレワークの推進【総務省】
https://www.soumu.go.jp/main_sosiki/joho_tsusin/telework/
総務省におけるテレワーク推進施策全般についてのポータルです。

問合せ先

<テレワーク全般について>
総務省 情報流通行政局 情報流通振興課 情報流通高度化推進室
担当：飯村、日野、澤田
Email: telework_atmark_ml.soumu.go.jp
※スパムメール対策のため、「@」を「_atmark_」と表示しております。送信の際には「@」に変更してください。
TEL：03-5253-5751

<セキュリティ対策について>
総務省 サイバーセキュリティ統括官室
担当：梅城、黒田、山下
TEL：03-5253-5749