総務省
Ministry of Internal Affairs and Communications
MIC

無線LANにおける情報セキュリティについて

平成24年5月29日

情報流通行政局　情報セキュリティ対策室

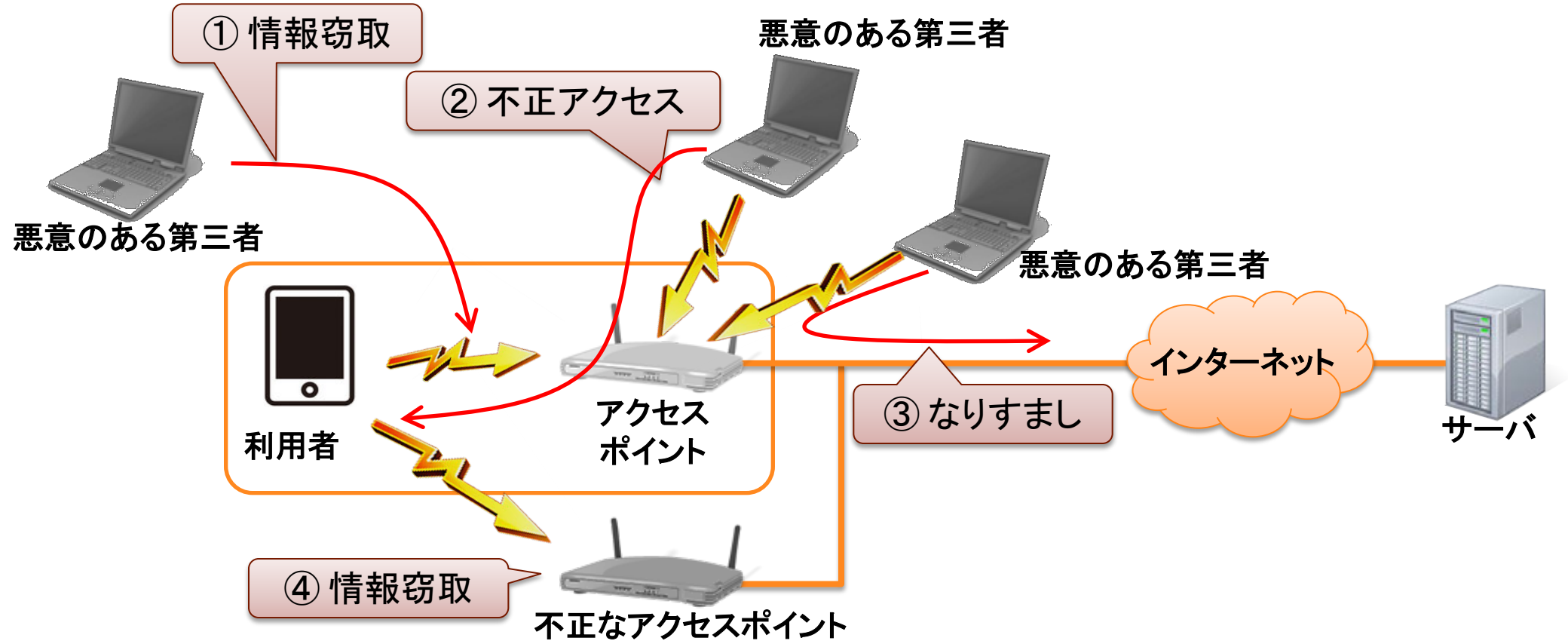
無線ＬＡＮに関する情報セキュリティ上の主な脅威

① 無線LAN区間における情報窃取

② 他の端末からの不正アクセス

③ 利用者端末へのなりすまし

④ 不正なアクセスポイントにおける情報窃取



無線ＬＡＮの脅威に関する情報セキュリティ対策の例

脅威	対策の例
① 無線LAN区間における情報窃取	◇ 無線LAN区間（利用者－アクセスポイント間）を暗号化し、情報窃取を防止。
② 他の端末からの不正アクセス	◇ アクセスポイントに接続している他の端末からのアクセス等を禁止。
③ 利用者の端末へのなりすまし等	◇ 利用者認証の実施。
④ 不正アクセスポイントにおける情報窃取	◇ 認証でなりすましアクセスポイントとの接続を防止。 ◇ 通信区間（利用者端末－サーバ間）を暗号化し、情報窃取を防止。

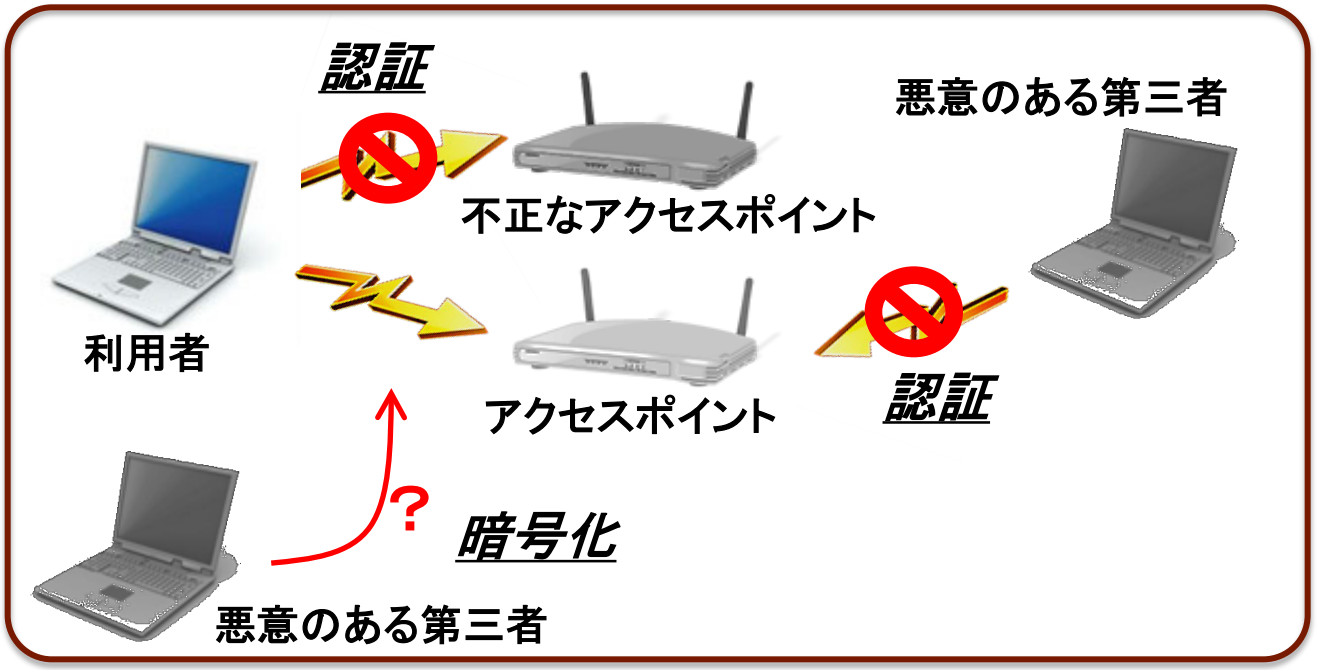
無線ＬＡＮに関する主な情報セキュリティ対策

暗号化

情報を暗号化し、通信内容を秘匿化

認証

利用者及びアクセスポイントが接続先の正当性を確認



無線LANに関する情報セキュリティ対策の方式	暗号化の強度	認証の強度
WEP（Wired Equivalent Privacy）	×	×
WPA（Wi-Fi Protected Access）	△	○
WPA2（Wi-Fi Protected Access 2）	○	○

無線ＬＡＮに関する情報セキュリティ対策の方式について

WEP

- ○ 無線LANにおける最初の情報セキュリティ対策方式。
- ○ 鍵管理の仕組みにぜい弱性が指摘されており、コンピュータセキュリティシンポジウム2008（CSS2008）に おいて神戸大学と広島大学の研究グループにより、10秒程度で解読する方法が実証。
- ○ 一部の携帯ゲーム機は、本方式のみの対応。

WPA

- ○ WEPのぜい弱性に対処することを目的に策定された情報セキュリティ方式。
- ○ WEPとの互換性を有し、WEP対応の多くの端末で利用可能。（ただし、一部の携帯ゲーム機は対応不可。）
- ○ 特殊な条件下においては、通信内容を解読されるぜい弱性が指摘されている。

WPA2

- ○ 現時点ではぜい弱性が発見されていない、無線ＬＡＮにおける最も強固な情報セキュリティ対策方式。
- ○ Wi-Fi Alliance ※の認証を得るためには、本方式に対応することが必須条件。

※ 無線LAN機器に関する業界団体

無線ＬＡＮの情報セキュリティに関するガイドライン(現状)

Wi-Fiがノートパソコンに標準搭載されるようになったことなどから、急速に無線LANの普及が進む一方、無線LANの使用に際して適切に情報セキュリティ対策を施さずに使用する危険性に対するユーザの認識は低く、情報セキュリティ対策が十分に行われていないという現状。

平成１６年４月に、国民一般向けの無線LANセキュリティの手引書として、「安心して無線LANを利用するために」を作成・公表。その後の技術動向を踏まえ、平成１９年１２月に改訂。

主な内容

無線LANを適切に利用するための対策例

暗号化

ID、パスワードなどの個人情報、メールの内容の通信が傍受されることを防ぐため、通信内容を暗号化

認証

重要な情報を不正な無線LAN アクセスポイントのネットワークに、窃取されてしまうこと、ウィルスの配布やDoS攻撃の踏み台にされることを防ぐために、接続の際に認証。

無線LANを安心・安全に利用するためのガイドライン

「家庭」、「オフィス」、「公衆無線LANサービス」及び「店舗開放型無線LANサービス」を取り上げ、それぞれの環境による無線LANの情報セキュリティレベル毎に、確認・設定すべき項目を提示。

※ 情報セキュリティに関して比較的リテラシーの高い、PC利用者等を対象

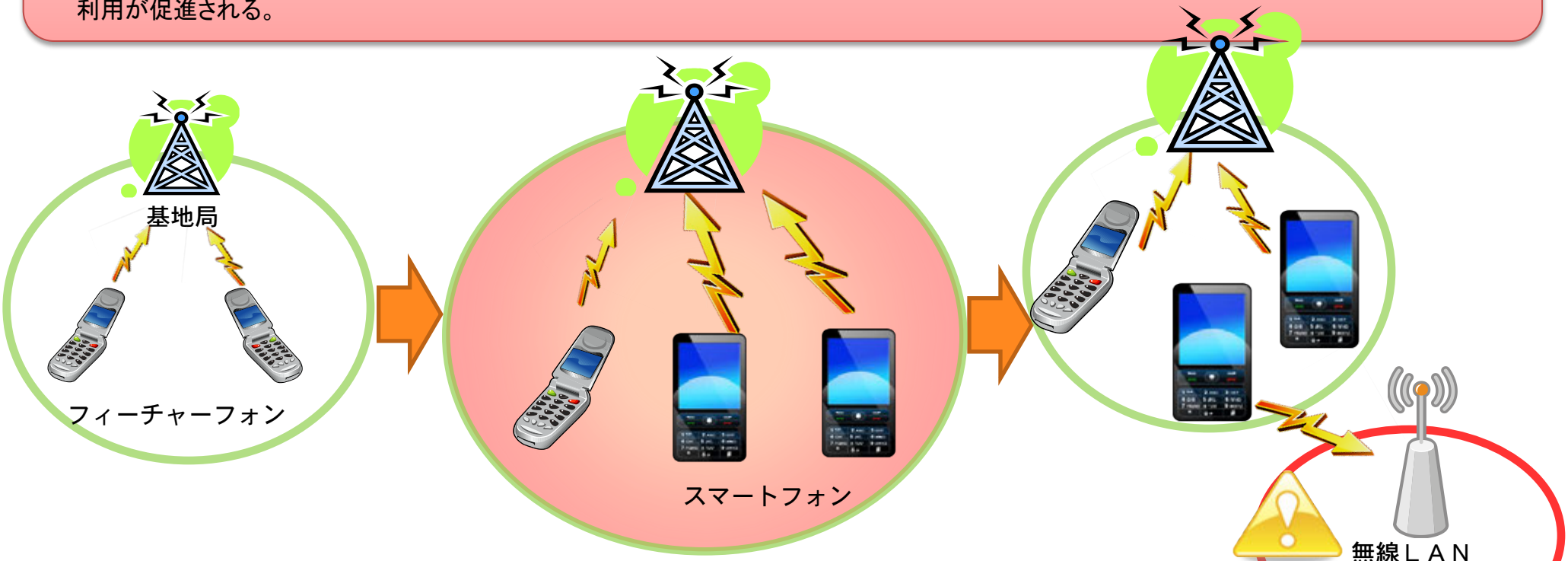
スマートフォンからのオフロードに関する経緯・脅威

○ 近年のスマートフォン普及によりモバイル通信網のトラフィックが急増。
⇒無線LANへオフロード（退避）の取組が行われている。

○ 適切な情報セキュリティ対策がなされていない無線LANを利用する場合、PCと同様スマートフォンも、無線LANの持つ情報セキュリティ上の脅威一般にさらされることになることに留意する必要。

○ スマートフォンの利用者のリテラシーレベルがPC利用者に比べ低い可能性がある。

○ スマートフォンから安全に無線LANを利用できる環境が整備されることにより、スマートフォンからのオフロードが進めば、電波の能率的な利用が促進される。



従来の通信

スマートフォンの普及による
トラフィック増大

無線ＬＡＮへのオフロード

無線ＬＡＮの情報セキュリティに関するガイドラインの改定

スマートフォン・クラウドセキュリティ研究会における検討

○　平成23年10月から開催している「スマートフォン・クラウドセキュリティ研究会」においても、無線LANの情報セキュリティに関し、以下の脅威と対策の必要性を指摘。

	一般的な無線LAN利用時に存在する脅威	スマートフォンから無線LANを利用する場合の特有の脅威
脅威	✓ なりすましアクセスポイント ✓ 通信パケットの傍受 ✓ 利用者になりすました不正アクセス	✓ スマートフォンの機能的制約 ✓ 利用者が意識せずに無線ＬＡＮを利用するという事象が発生しやすい ✓ 利用者のリテラシーレベルがPC利用者に比べ低い可能性
対策案	✓ 安全性の高い認証や暗号化技術の採用 ✓ 接続先を識別し、回線の信頼度に応じて保護レベルを変更できる仕組みの導入	✓ 利用者が無意識のうちに保護されていない無線LANを利用することを避けるため、利用する際に承認を求める等の利用者に気づきを与える仕組みの導入 ✓ 暗号や認証の仕組みが導入されていない無線LANの場合、通信内容が外部に読み取られる可能性があることを利用者に啓発

ガイドラインの改定

○　スマートフォン等の急速な普及による無線LANの利用者数の増大、利用者層の拡大、利用形態の変化等を踏まえ、今後、情報セキュリティ上の脅威や暗号の危殆化等について最新動向を調査した上で、スマートフォンからの利用に重点を置いて、「安心して無線LANを利用するために」を改訂する。

※ 情報セキュリティに関してリテラシーの低いユーザが増加していることを想定して作成