



燕市観光・防災Wi-Fiステーションの セキュリティについて

平成28年3月1日

燕市役所 総務部 総務課
情報統計チーム 山口優太



ランランおいらん



以下のセキュリティ対策を実施済

想定される 脅威	セキュリティ対策
① 無線LAN区間 における通信内容 の搾取及び改ざん	・WPA/WPA2 (CCMP) 設定 (PSK認証 パスフレーズ) ・Wi-Fiで接続している端末同士の通信を遮断 (ステーションアイソレーション機能)
② 内部ネットワー クへの侵入	・SSIDとVLANのマッピングを行い、既存ネットワークと観光・防災ネットワークを分離 ・アクセスポイント、無線コントローラの管理者ID・パスワードを適切に設定 ・ログの収集・保存・分析
③ 利用者なりすま し、不正利用	・利用者情報の記録 (メールアドレス、MACアドレス等) ・アクセス制限 (利用可能時間 (30分/回)、利用回数の設定 (20回/日)、制限回数を超えた場合は改めてメールアドレス再登録から開始。登録済みメールアドレス再登録可。) ・任意のユーザセッションをセンターから切断 ・ログの収集・保存・分析
④ 不正なアクセス ポイントによる通 信内容の搾取	・定期的に周囲のアクセスポイントを探索する機能により、不用意にアクセスポイントを設置されることを検知し、防止に役立てる



(1) ログの採取項目

AP、コントローラより出力されるログより下記のデータを取得

- ・ 認証ユーザ情報（メールアドレス、ユーザ/パスワード等）
- ・ 端末MACアドレス
- ・ 接続AP
- ・ トラフィック量
- ・ HTTPウェブログ 等

(2) 無線セキュリティ

WPA/WPA2（CCMP）を採用。

本方式はWPA2に未対応（WPA対応機器）とも通信ができるWPA互換モード

WPAは暗号化方式にRC4を使うTKIPとAESを使うCCMPがあり、よりセキュリティの強度なCCMPを採用



(3) ステーションアイソレーション

AP単体では、同一SSID間、他SSID間のアイソレーション機能を保有
コントローラと組み合わせ、複数APを跨るアイソレーションを実現

(4) SSID

観光・防災情報ステーション用に、例として『tsubame_kiralan』を共通で設定

SSIDは、2.4GHz、5GHzそれぞれに16個まで設定することが可能

(5) PSK

市民には広報誌で周知済み。旅行者等には公共施設等にパンフレットを掲示して周知予定。



(6) 利用時間・回数の具体的数値は？

- ・ メール認証をした場合、接続時間（30分/回）、接続回数（20回/日）で利用可能

(7) 災害時

メールアドレス認証を行わず認証フリーに切替える

災害時における避難所利用者のセキュリティ確保を考慮し、PSKの扱いについては今後検討を進める。