

電磁シールドを用いた無線 LAN ルータの設定検証システムの提案

浮田博揮[†] 谷口義明[‡] 井口信和[‡]
 近畿大学大学院総合理工学研究科[†] 近畿大学理工学部情報学科[‡]

1. 序論

中小企業や一般家庭、教育機関等における無線 LAN ルータやモバイルルータの普及が進んでいる。無線 LAN は電波を用いて通信を行うことからセキュリティの確保が非常に重要であり、無線 LAN ルータの適切な設定が不可欠である。しかしながら、必ずしも無線 LAN に詳しい管理者が無線 LAN ルータを設定するとは限らない。例えば、中小企業や一般家庭においては、無線 LAN やセキュリティに詳しくない管理者が無線 LAN ルータを設定する場合がある。また、大学においては、出入りが比較的自由であるため、攻撃を受ける機会が多い。これらのことから、脆弱性のある無線 LAN を運用している場合、第三者に攻撃される可能性がある。その結果、研究データや個人情報の流出や研究室無線 LAN を踏み台とした違法行為等の被害にあう可能性がある。

そこで本研究では、電磁シールドを用いた無線 LAN ルータの設定検証システム（以下、本システム）を提案する。本システムは、無線 LAN ルータに対して設定が正しく行われているか自動的に確認し、無線 LAN ルータの設定の不備を検出する。対象となる無線 LAN ルータ以外の無線 LAN ルータに誤って設定を確認することを防ぐため、本システムでは、検証用の機器と無線 LAN ルータを電磁シールド¹⁾で被覆された箱の中に同梱する。本システムを用いることで、外部に影響を与えることなく安全に無線 LAN ルータのセキュリティの検証を行える。

2. 関連サービス

関連サービスとしてスペクトラム・テクノロジー株式会社が提供している無線 LAN 侵入試験サービスの「WiFi Pen Test サービス」がある²⁾。これは、専門家が測定ツールを使用することで、無線アクセスポイントや無線 LAN 端末等の無線 LAN 全体のシステムの安全性を確認できるサービスである。また、株式会社ファイブドライブでは、無線アクセスポイントの暗号化キーと承認されていない無線アクセスポイントを調査し、見つかった問題点と改善点を提供する無線 LAN 診断サービスを行っている³⁾。

これらに対して、本システムは無線 LAN に詳しく

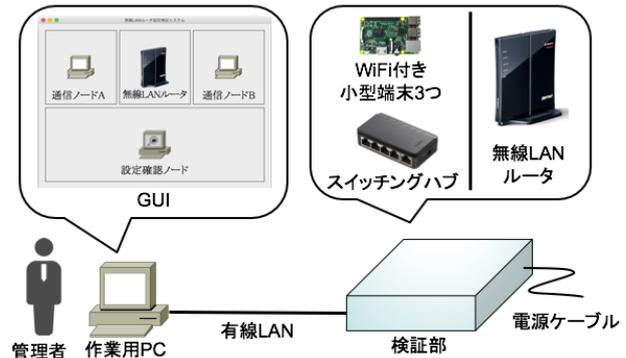


図1：システム構成



図2：GUI

くない管理者が利用することを想定しており、無線 LAN ルータとその管理画面に対して自動的に設定の確認を行う。また、電磁シールドを活用することで対象となる無線 LAN ルータ以外に誤って攻撃することを防ぐ。

3. 提案システム

ここでは、提案するシステムの概要と機能について述べる。

3.1 システム構成

本システムの構成を図1に示す。本システムは、検証部と作業用 PC から構成される。検証部と作業用 PC は有線 LAN ケーブルにより接続される。検証部は電磁シールドで被覆されており、中には、3 台の小型端末とスイッチングハブが設置される。小型端末としては、無線 LAN モジュールを内蔵した Raspberry Pi 3 を想定する。小型端末のうち 1 台は、無線 LAN ルータの設定を確認する設定確認ノードであり、残りの 2 台は無線 LAN ルータを介して通信を行う通信ノードである。設定確認ノードの OS としては、ペネトレーションテストでよく用いられ

る Kali Linux を用いる。すべての小型端末は作業用 PC とスイッチングハブを介して有線で接続されており、作業用 PC から図 2 の GUI を用いて操作可能である。

本システムを用いて無線 LAN ルータの検証を行う場合、まず、管理者は検証部の中に検証対象となる無線 LAN ルータを入れる。次に、作業用 PC の GUI を用いて、無線 LAN ルータの画像を選択し SSID とパスワード等の基本情報を入力する。その後、本システムの無線 LAN ルータ情報取得機能、無線 LAN ルータ検証機能を用いることにより、無線 LAN ルータの検証を行う。また、検証結果および検証結果に基づく対策の提案を専用の GUI により確認する。なお、管理者は、ネットワーク通信可視化機能を用いて、検証の様子を視覚的に確認することができる。以降、それぞれの機能の詳細について説明する。

3.2 無線 LAN ルータ情報取得機能

本機能は、チャンネルや周波数、認証方式、暗号化方式等の無線 LAN ルータの基本設定情報を取得する機能である。本機能で取得した基本設定情報は、作業用 PC の GUI に表示される。また、基本設定情報の一部は、無線 LAN ルータの設定を確認する際に使用する。

3.3 無線 LAN ルータ検証機能

本機能は、対象の無線 LAN ルータの設定を検証する機能である。まず、無線 LAN ルータの認証を行わなくても実施可能な検証を試みる。無線 LAN 情報取得機能により無線 LAN ルータの情報を取得する。暗号方式として WEP や WPA/WPA2 が用いられている場合には、WEP キーや WPA/WPA2 キーの解析を行う。WEP が用いられている場合、無線 LAN ルータを介して行われる通信ノード間のパケットをキャプチャすることで WEP キーの解析を行う。また、WPA/WPA2 が用いられている場合、一般的な単語やよく使用されるパスワード等のリストを利用して WPA/WPA2 キーの解析を行う。

そして、無線 LAN ルータにおいて WPS が有効な場合、WPS の PIN コードの解析を行う。WPS は、無線 LAN ルータとの接続を容易に行えるように標準化された規格であるが、PIN 認証に脆弱性⁴⁾⁵⁾がある。本システムでは総当たりに PIN コードを確認することで解析を行う。

次に、無線 LAN ルータに対する認証を行った後に実施可能な検証を試みる。具体的には、無線 LAN ルータの管理画面のユーザ名とパスワードにデフォルトのものや容易に類推されるものが使用されていないかを確認する。

これら一連の検証は、設定確認ノードが自動的に確認を行う。また、セキュリティの検証を終えると、

無線 LAN ルータの設定の検証結果に関するフィードバックを管理者に提示する。無線 LAN ルータに設定の不備がある場合、その対策を GUI 上に表示するとともに、推奨される設定を表示する。

3.3 ネットワーク通信可視化機能

本機能は、通信ノード間の通信や攻撃ノードの攻撃の様子をリアルタイムに可視化する機能である。可視化することで、どのような検証が行われているかを管理者が把握することができる。また、無線 LAN ルータに対する攻撃の脅威が存在することを認知できる。通信ノードと攻撃ノードは、常時パケットを収集し、作業用 PC に送信する。作業用 PC は、受け取ったパケットから IP アドレス等の情報を利用し、GUI 上にアニメーションで表示する。これにより、検証の様子を可視化できる。

4. 実験

本システムの性能評価実験内容と実証実験内容を述べる。性能評価実験では、電磁シールドで被覆した箱の内外から無線 LAN ルータの電波を検出できるか確認する。箱内からは、対象となる無線 LAN ルータの電波のみが検出できること、箱外からは対象の無線 LAN ルータの電波が検出できないことを確認する。

実証実験では、本学の研究室に実際に配置している無線 LAN ルータを対象とし、本システムを利用した検証を行う。また、無線 LAN ルータの設定を様々に変えて攻撃を行い、攻撃にかかる時間を計測する。この結果から、検証に必要な時間に関する評価、考察を行う。

5. 結論

本研究では、電磁シールドを用いた無線 LAN ルータの設定検証システムを提案した。本システムでは、電磁シールドを活用することで外部に影響を与えることなく安全に無線 LAN ルータのセキュリティの検証を行える。今後は、機能の実装と性能評価実験および実証実験を実施し、本システムの有用性を確認する。

参考文献

- 1) 村田美久, “シールドの方法”, 電気設備学会誌, Vol.26, No.10, pp760-763 (2006).
- 2) スペクトラム・テクノロジー株式会社: WiFi Pen Test (無線 LAN 侵入試験) サービス, http://spectrum-tech.co.jp/service/wifi_pen_test.html.
- 3) 株式会社ファイブドライブ: 無線 LAN 診断, <https://www.fivedrive.jp/diagnosis/lan.html>.
- 4) Indra Dwi Raianto, “Anticipating WPS PIN Vulnerability To Secure Wireless Network”, ComTech, Vol.4, No.2, pp.1116-1121 (2013).
- 5) Japan Vulnerability Notes: JNVNU#72375 5 Wi-Fi Protected Setup, <http://jvn.jp/vu/JVNU72375/>.