M-052

携帯端末を利用した無線 LAN 自動設定方法の提案

Proposal on WLAN Zero Configuration Using Mobile Device

土岐 卓† 荒井 大輔† 吉原 貴仁†
Suguru Doki Daisuke Arai Kiyohito Yoshihara

1. はじめに

近年，PC をはじめゲーム機やフォトフレーム等，様々な機器に無線 LAN が搭載されている[1]．無線 LAN を利用するには，第三者によるなりすましや，電波盗聴等のセキュリティ上の問題を解決するため，SSID(Service Set ID)や暗号方式，暗号鍵等の通信パラメータを無線 LAN 搭載機器(以下，無線 LAN 機器と呼ぶ)と無線 LAN アクセスポイント(以下，無線 LAN AP と呼ぶ)に設定する必要がある．これらの設定は複雑で面倒な課題がある．この課題を解決するため，本稿では，携帯端末を用いて無線 LAN 設定の自動化を図る新たな方法を提案する．

2. 想定環境

1 台の無線 LAN AP と複数台の携帯端末，複数台の無線 LAN 機器が存在するホームネットワークを想定する．無線 LAN AP はインターネット接続サービスを利用する際に通信事業者から提供される．少なくとも 1 台の携帯端末の SSID や暗号方式，暗号鍵等の無線 LAN 設定は，例えば，携帯端末購入時に通信事業者のサポートスタッフが実施する等，完了しているとする．無線 LAN 機器は，無線 LAN 設定の標準規格である WPS(Wi-Fi Protected Setup)[2]に準拠しているものとする．

3. 従来技術と解決すべき課題

3.1. 従来技術

無線 LAN を簡便に設定するために，無線 LAN AP に設定用のボタンを設け，無線 LAN 機器を設定モードにした上で無線 LAN AP のボタンを押下することで設定する技術が従来ある[3].

3.2. 解決すべき課題

2 章に前述の想定環境において，無線 LAN の設定を自動化するためには，次の課題を解決する必要がある．

(課題) 無線 LAN 機器を設定モードにする必要がないこと

無線 LAN 機器を無線 LAN の設定モードにする操作は無線 LAN 機器毎に異なる．このため，IT リテラシの低い利用者にとっては，依然として無線 LAN 設定が難しい，あるいは，無線 LAN の知識を持った利用者でも面倒で，これを解消する課題がある．無線 LAN 機器を設定モードにすることなく，設定ができる方法が望まれる．

4. 無線LANの自動設定方法の提案

2 章に示す環境を対象に，3.2 節に示す課題を解決する，新たな無線 LAN 設定の自動化方法を提案する．本提案方法では，無線 LAN AP との接続設定が済んだ携帯端末を無線 LAN 機器に近づけるだけで無線 LAN の設定を完了する．これを実現するためのハードウェア要件は次の通りとなる．

- **無線 LAN AP のハードウェア要件：**
  (ア) 複数の SSID をサポートする．
  (イ) MAC アドレスによるアクセスフィルタリングをサポートする．
- **携帯端末のハードウェア要件：**
  (ウ) プロミスキャスモードをサポートする．
- **無線 LAN 機器のハードウェア要件：**
  (エ) WPS をサポートする．

†株式会社 KDDI 研究所，KDDI R&D Laboratories Inc.

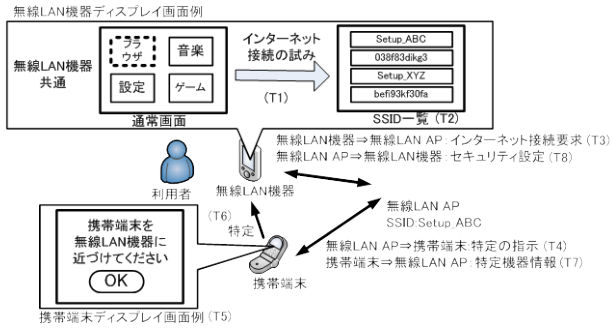

図 1. 本提案方法概要

4.1. 提案方法概要

無線 LAN AP がサポートする複数の SSID の内 1 つを，暗号化不要の通信チャネルを使って設定対象の無線 LAN 機器を特定するために使用する．この SSID は，例えば“Setup-***”(***には利用サービス名+固有文字)等，利用者が直観的に設定用だと理解できる文字列とし，暗号化不要の通信チャネルとする(無線 LAN 機器が本 SSID を選択するのみで，無線 LAN AP との通信が可能となる)．また，無線 LAN AP は，MAC アドレスのフィルタリングにより，本提案方法で設定を完了した無線 LAN 機器以外の通信を遮断することで，第三者による不正利用を防止する．

本提案方法による無線 LAN 機器の設定は次の 3 つのステップからなる．概要を図 1 とともに示す．

(ステップ 1) 無線 LAN 機器からの接続要求

利用者は，無線 LAN 機器の設定，未設定を意識することなく，無線 LAN 機器の Web ブラウザを起動する等，ネットワーク接続を試みる(図 1(T1))．無線 LAN 機器は，未設定の場合，電波範囲内にある SSID をディスプレイ表示し，利用者に SSID の選択を要求する(図 1(T2))．利用者は，直観的に設定用と理解できる SSID(例えば，“Setup-***”)を選択する．無線 LAN AP は，これを無線 LAN 機器からの接続要求とし，本提案方法を開始する(図 1(T3))．

(ステップ 2)設定対象の無線 LAN 機器の特定

無線 LAN AP は，接続要求を受信すると，設定済みの携帯端末に対し，指示を出す(図 1(T4))．指示を受けた携帯端末は，ディスプレイ上に携帯端末を無線 LAN 機器に物理的に近づけるように求めるメッセージを表示する(図 1(T5))．利用者が無線 LAN 機器の設定を望む場合には，メッセージに従い無線 LAN 機器に近づける．携帯端末は，無線 LAN 機器の受信電波強度が，あらかじめ設定された閾値以上となる場合，無線 LAN 機器と接近したと判断し，設定対象として特定する(図 1(T6))．さらに，特定した設定対象の無線 LAN 機器の MAC アドレスを無線 LAN AP に通知する(図 1(T7))．

(ステップ 3)無線 LAN 機器のセキュリティ設定

無線 LAN AP は，携帯端末より通知された MAC アドレスを持つ無線 LAN 機器のセキュリティ情報を，WPS で規

定されたメッセージシーケンスを拡張利用することで，設定する(図 1(T8)).

4.2. 提案方法詳細

無線 LAN AP は，電源投入と同時に周囲に飛び交うビーコンから，SSID“Setup-***”の存在有無を確認する．もし“Setup-***”が存在した場合，重複を避けるため無線 LAN AP は，“***”を変えて SSID“Setup-***”を生成し，自身に設定する．無線 LAN AP はその SSID をビーコンに含めて周囲に継続的に送信する．その SSID は暗号化不要の通信チャネルとする(図 2(S1)). 携帯端末は，サポートスタッフの手動操作等により，無線 LAN AP がサポートする複数の SSID の内，暗号化が必要な SSID や，暗号方式，暗号鍵等の通信パラメータの設定が予め済んでいる(図 2(S2)). 携帯端末は，設定済みの無線 LAN AP からの継続的なビーコンを受信すると，無線 LAN AP からの指示メッセージを受信可能とするために，無線 LAN AP と HTTP のセッションを確立し続ける(図 2(S3)). また携帯端末は，周囲に複数の“Setup-***”が存在した場合，設定済みの無線 LAN AP の SSID の情報を，ディスプレイ表示で利用者に定期的にポップアップ通知する(図 2(S4)).

(ステップ 1)：無線 LAN 機器の接続要求

利用者は，無線 LAN 機器の設定，未設定を意識することなく，無線 LAN 機器に内蔵の Web ブラウザ等を用いてインターネットに接続を試みると，無線 LAN 機器から設定を要求される．無線 LAN 機器は，無線 LAN が未設定の場合，電波範囲内にある SSID の一覧をディスプレイ上に表示する(図 2(S5)). 利用者は，SSID の一覧の中から，“Setup-***”と表示された文字列を直感的に設定用と理解し，選択する．このとき，“Setup-***”が複数存在する場合，利用者は携帯端末のディスプレイ上のポップアップ通知を確認することで該当 SSID を選択する(図 2(S6)). SSID が選択されると無線 LAN 機器は，その SSID の無線 LAN AP と標準手順を利用して一時的に接続を確立する(図 2(S7))[4]. このとき無線 LAN 機器は，次のステップ 2 が終了するまで，ホームネットワークからインターネットへの接続が拒否される(図 2(S8)).

(ステップ 2)：無線 LAN 機器の特定

無線 LAN AP は，設定済みの携帯端末宛てに，未設定の MAC アドレスの一覧を送信する(図 2(S9)). 携帯端末はそれを受信して，ディスプレイ上に，携帯端末を無線 LAN 機器に物理的に近づけるように求めるメッセージを表示する(図 2(S10)). 設定済みの携帯端末が複数あった場合，それぞれの携帯端末のディスプレイ上に，メッセージが表示される．利用者が設定を望む場合，携帯端末を無線 LAN 機器に近づける(図 2(S11)). このとき携帯端末は，無線 LAN 機器が送信するメッセージを捕捉するため，プロミスキャスモードで動作する(図 2(S12)). 無線 LAN AP は，例えば，標準手順の接続解除メッセージを一覧に含まれる MAC アドレス宛てに送信する(図 2(S13)). その MAC アドレスに対応する無線 LAN 機器が接続解除メッセージを受けると，無線 LAN AP に対して継続的に再接続要求メッセージを送信する(図 2(S14)). プロミスキャスモードで動作する携帯端末が，一覧に含まれる MAC アドレスからの再接続要求メッセージを捕捉し，かつその電波強度が予め定められた閾値以上であった場合，その MAC アドレスを無線 LAN AP に送信する(図 2(S15)). 無線 LAN AP は，

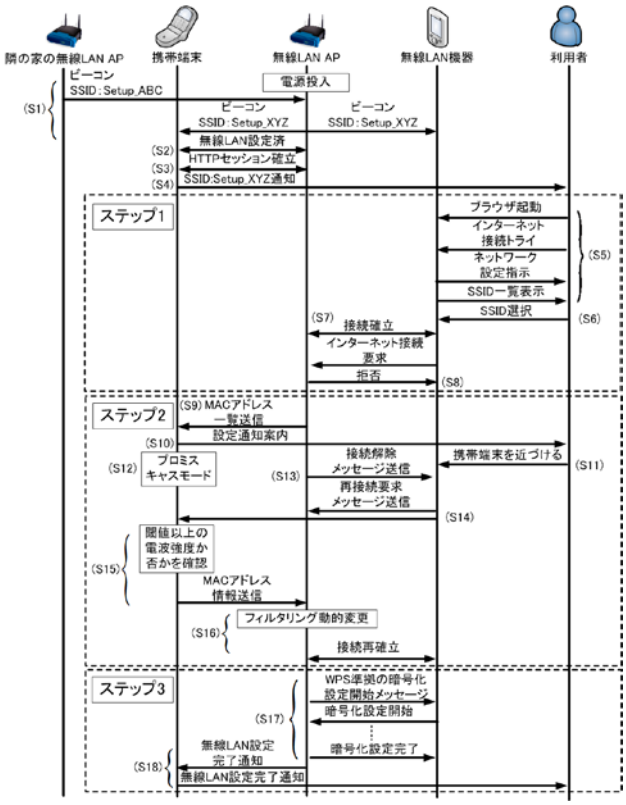

図 2. 本提案方法シーケンス

その MAC アドレスに対するフィルタリングを変更し，インターネット接続を許可する．かつその MAC アドレスを設定対象として無線 LAN 機器を特定し，ステップ 3 へ進む(図 2(S16)).

(ステップ 3)：セキュアな無線 LAN 通信の設定

無線 LAN AP は，ステップ 2 で特定した無線 LAN 機器に対して，WPS に準拠した暗号化設定開始のメッセージを送信する．それを受信して無線 LAN 機器は，暗号化の設定を開始する．以降 WPS のシーケンスに従って無線 LAN 機器と無線 LAN AP にセキュアな設定が実施される(図 2(S17)). 無線 LAN の設定が完了後，無線 LAN AP は，完了した旨を携帯端末の鳴動やディスプレイ表示を介して利用者に通知する(図 2(S18)).

以上により，本提案方法は，利用者が無線 LAN 機器を設定モードにすることなく，携帯端末を無線 LAN 機器に近づけるだけで無線 LAN の設定を実現する．

5. 終わりに

本稿では，無線 LAN の設定が済んだ携帯端末と無線 LAN AP の連携により，無線 LAN 機器の無線 LAN 設定を自動化する方法を新たに提案した．本提案により，無線 LAN を搭載した機器の利便性向上が期待できる．提案方法の実装が今後の課題である．

[1]シード･プランニング, “次世代無線 LAN 市場の最新動向と将来展望,” http://www.seedplanning.co.jp/press/2009/2009070901.html.
[2] Wi-Fi Alliance, “Wi-Fi Protected Setup Specification,” Wi-Fi Alliance Document, January 2007.
[3]株式会社バッファロー, “AirStation One-Touch Secure System,” http://buffalo.jp/aoss/.
[4]Mattbew S. Gast, OREILLY, “802.11 Wireless Networks The Definitive Guide,” April, 2005.