平成 24 年 3 月 30 日

情報部情報基盤課

情報セキュリティ対策室

無線 LAN の利用に関する Q&A 集

(KUINS に接続する無線 LAN アクセスポイント設置のガイドラインの解説文書)

-第 1 版-

目　次

1. はじめに

本文書は平成 24 年 2 月 8 日に制定した「KUINS に接続する無線 LAN アクセスポイント設置のガイドライン」（以下「ガイドライン」という）に関して各部局からいただいた質問等について解説を行うことで、今後より安全な無線 LAN アクセスポイント（以下「AP」という）の設置運用を行っていただくことに寄与することを目的としています。

2. 電波の干渉と AP の設置

2.1. 電波の干渉はどのような理由で起こるのでしょうか

同じ周波数(チャンネル)を複数の機器が共用している場合､相互の距離が近いと妨害が発生し、いわゆる「電波が干渉して通信できない」状態となります。これを防ぐには、

・ 周波数（チャンネル）を変える
・ 距離を離す
・ 機器の電波の出力を落とす（その代わり利用範囲は狭くなる）

の 3 つのうちどれかの対策を行う必要があります。

無線 LAN では周波数帯として 2.4GHz 帯と 5GHz 帯の 2 つが使われています。2.4GHz 帯は IEEE 802.11b/g/n の各規格で定められ、最も一般的に使われています。しかし、2.4GHz 帯は、無線 LAN だけでなく、他のさまざまな機器でも使われています。具体的には

・ 電子レンジ
・ ワイヤレスマイク
・ コードレスホン
・ Bluetooth （パソコンや携帯電話と周辺機器の間で使用）

などが挙げられます。
これらの機器が存在する場所では、通信に障害が起こる可能性があります。

一例として、AP と無線 LAN 利用機器の間に電子レンジが存在する場合、電子レンジを使用していると、2.4GHz 帯での通信ができなくなるという問題があります。この場合は、電子レンジの位置を変えるなどして影響を出にくくする対策が必要です。
一方、5GHz 帯は IEEE 802.11a/n の各規格で定められ、2.4GHz 帯よりも多くのチャンネルを使うことができます。しかし、2.4GHz 帯よりは波長が短く、障害物があると電波が届きにくいという特性を持っています。また、日本では法律により原則として屋内利用に限られているなどの制限があります。
現在販売されている無線 LAN 機器では、通常 2.4GHz 帯には対応していますが、5GHz 帯に対応しているもの（IEEE 802.11a 準拠のもの）はあまり多くないのが実情です。そのため、互換性を考えると、2.4GHz の利用を主に考える必要があります。

2.2. APが相互に妨害しないようにするためにはどのようにすれば良いのでしょうか

チャンネルの使用状況を、専用のツールや機器を使って確認し、干渉しているAPがある場合は周波数の変更や出力を落とすなどの方法で回避することが必要です。

APがどのようにチャンネルを使っているかに関する簡易的な測定法としては、ノートパソコンの内蔵無線LANアダプタを使って測定するツール(inSSIDer[2]など)が入手できます。より正確な測定を行いたい場合は、専用の測定器(Fluke社の製品[3]など)や、外部接続できる無線LANアダプタとノートパソコンの組み合わせを使って使用状況を調べます。このようなツールや測定器を使うことで、どんなAPがアクセス可能かについて、MACアドレスやSSIDなどを調べることができます。

チャンネルの配置については、以下に述べる技術的な制約事項に留意する必要があります

無線LANでは、2.4GHz帯では5MHz間隔のチャンネルを13個、5GHz帯では20MHz間隔のチャンネルを19個使用することができます。しかし、実際には1つの通信路に必要な周波数の幅は複数チャンネルにわたるため、各々のチャンネルを通信路として使えるわけではありません。

2.4GHz帯を使うIEEE 802.11b/g規格では、1つの通信路に20MHz、つまり4チャンネル分を確保する必要があります。実際の運用では余裕を見て5チャンネル分を1つの通信路に確保するため、使える通信路の数は3つとなり、チャンネルの番号は1ch、 6ch、 11chとなります。

また、IEEE 802.11n規格で2.4GHz帯を使う場合では、最大40MHz、つまり8チャンネル分の周波数を確保する必要があります。この場合は使える通信路の数は2つしかありません。

実際には、複数の通信路間でチャンネルが干渉した場合、速度が遅くなったり、通信状況が不安定になることがあります。このような場合は、各APの管理者で調整を行い、重なり合うチャンネルの数ができるだけ少なくなるように設定する必要があります。

なお、KUINSが提供する学内無線LANのAP設置の際は、チャンネルの利用状況の実測を行い、干渉が少なくなるように調整しています。

3. AP導入の際の検討事項

3.1. WEPにしか対応していない古いAPや端末はどうすれば良いのでしょうか

WEPにしか対応していない機器については、使用を停止するか、WPAまたはWPA2でAESによる暗号化に対応した機器への交換をお願い致します。

ガイドライン第5条第2項では、「WEPは暗号化方式に使用してはならない」としています。WEPの暗号解読については、2008年に「10秒で解読可能」とする研究結果[5]が発表されており、簡単に解読できるツール等も出回っていることが確認されています。

ただし、WEP以外の暗号化に対応していない機器（古い計測機器など）で、交換できないなどのやむを得ない事情で使わなければならない場合は、ガイドライン第6条の例外措置の適用につい

て、部局情報セキュリティ責任者がご判断くださるようお願いしています。

3.2. AP の買い替えや導入の時にはどのような点に注意すれば良いのでしょうか

ガイドライン第 3 条第 1 項では、「AP に接続する特定部局情報システムならびに利用者端末を限定する措置を取らなければならない」と定めています。このためには、AP にどのような MAC アドレスの機器が接続されたかなどのログ情報の取得を行う必要があります。また、ログ情報を syslog などのプロトコルで他のサーバ機器等に転送できる機能を持つ AP もあり、このような AP では外部のサーバにログを転送することで、より長期間にわたりログの自動収集を行うことができます。

4. 認証の方法

4.1. 各 AP の利用者を認証する手段としてはどんなものがありますか

AP における利用者の認証手段については、以下に述べるものが使用できます。

(1) AP ごとにパスフレーズを定め、そのパスフレーズによる端末 - AP 間の通信内容の暗号化を行う方法。ほとんどの AP で利用できます。ガイドライン第 5 条第 1 項～第 3 項では、この方法による暗号化を必ず使用し(第 1 項)、WPA または WPA2 で AES による暗号化を使うこと（第 2 項）を定めています。また、パスフレーズには 10 文字以上の十分に予測困難な文字列を使い、年 1 回以上変更しなければなりません（第 3 項)。この方法では、パスフレーズを複数の利用者が知ることになるため、パスフレーズの管理には注意を払う必要があります。

(2) IEEE 802.1X 規格による認証を行う方法。この規格は LAN スイッチに端末を接続する際に、利用者 ID とパスワードの組、あるいはクライアント証明書を認証サーバとやり取りして接続の可否を決めます。無線 LAN の場合は、AP が LAN スイッチに相当するため、同様の方法を適用することができます。本学では eduroam[6]のサービスにてこの方法を使用しています。

(3) VPN を使う方法。この方法では、AP を通して利用できるプロトコルとして、各利用者が PPTP や SSH など利用者認証を必ず行うもののみに制限することで、AP 自身での認証を行わなくとも、PPTP や SSH のサーバで利用者を制限することができます。本学では、MIAKO ネットを通じた KUINS への接続で、この方法を利用しています。

5. 無線 LAN を通じて起こり得る不正利用の可能性

5.1. 無線 LAN の AP の不正利用を予防するにはどのような対策を取れば良いでしょうか

無線 LAN は、有線 LAN とは違い、以下の特徴があります。

(1) 電波を使っていることにより、電波の届く範囲では、通信を行っている当事者とは関係のない第 3 者が、通信内容を知る（傍受する）ことができます。つまり、通信内容の暗号化を行っていない場合は、第 3 者に傍受される可能性が常にあります。

(2) 無線 LAN の利用には、機械的接続を必要としません。このため、攻撃者が自らの存在を

知られることなく AP に不正に接続することが容易となります。

(3) 無線 LAN の AP は安価に入手でき、設置も容易です。このため、他の AP と同一の SSID を騙るなどの手段により、攻撃者が利用者の機器を不正に誘導して接続させ、該当 AP を介した通信内容を盗聴することもできます。

これらの特徴に見られる不正利用の可能性に対して、ガイドラインでは以下の対策を取ることを義務付けています。

(1) 通信の内容は必ず暗号化し、WPA または WPA2 で AES による暗号化を使う（ガイドライン第 5 条第 1 項および第 2 項）。これによって、通信内容の傍受の可能性を抑えます。

(2) AP の設置にあたっては、設置する部局の部局情報セキュリティ技術責任者の了承を得なければならない（ガイドライン第 4 条第 1 項）。これによって、誰が管理しているかわからない AP の存在をなくし、無線 LAN を通じた KUINS への接続が把握できるようにします。

(3) 部局情報セキュリティ技術責任者は、管理する AP の SSID について、命名規則を定める措置の必要性の有無を検討し、必要と認めた場合は措置を講ずるものとする（ガイドライン第 5 条第 5 項）。これによって、部局に属している AP の SSID をわかりやすくすると共に、部局に属していない SSID については区別を容易にできるようにしています。

また、ガイドラインによる対策が十分な効果を上げるためには、以下の注意が必要です。

(1) AP の通信内容の暗号化に必要なパスフレーズは、利用者以外に知られないよう注意すること。パスフレーズが漏洩するなどの危険が発生した場合は、速やかにパスフレーズを変更すること。

(2) 部局情報セキュリティ責任者は、各 AP の設置場所や SSID を把握し、不正侵入などの事案（インシデント）が発生した場合の場所の限定を可能とすること。ガイドライン第 4 条第 2 項には、部局情報セキュリティ技術責任者が AP の設置開始および終了時の申請手続を整備しなければならない、と定めています。この手続の際、設置場所や SSID を記録することで、インシデント発生時の調査がより容易となります。

(3) 各 AP にどの機器がいつ接続されたかを判別するために、MAC アドレスと接続時刻の証跡（ログ）を記録すること。

6. ガイドラインの運用

6.1. ガイドラインの「例外措置」を適用するためには、どのような手順を取れば良いのでしょうか

各 AP に関して、ガイドライン第 6 条にある例外措置を適用するためには、次の手順が必要です。

(1) 各 AP を管理する部局情報システム技術担当者は、当該 AP を設置している部局の、部局情報セキュリティ責任者に申請を行った上で、許可を得なければなりません（ガイドライン第 6 条第 1 項）。部局情報セキュリティ責任者は部局長が担当します。（京都大学の情報セキュリティ対策に関する規程 第 5 条）つまり、部局長の許可が必要ということになります。

(2) 部局情報セキュリティ責任者は、例外措置に関する審査の手続を定めなければなりませ

ん（ガイドライン第6条第2項)。具体的な審査の手続については、各部局で定めることができます。一例として、部局情報セキュリティ責任者が長であるところの部局情報セキュリティ委員会に委任する、などの方法を取ることができます。

(3) 部局情報セキュリティ責任者は、例外措置にあたる許可を行った場合、その適用審査記録を整備し、最高情報セキュリティ責任者に報告しなければなりません（ガイドライン第6条第3項)。部局情報セキュリティ責任者は、例外措置を認めた場合、その審査記録を残し後日閲覧できるようにした上で、最高情報セキュリティ責任者に報告する必要があります。つまり、例外措置の適用については、最高情報セキュリティ責任者の知るところとなります。

6.2. 「臨時利用者」がAPを利用する際の手続として定めるべきことは何ですか

部局情報セキュリティ技術責任者は、APを利用できる者の中に特定部局情報システム臨時利用者を含む場合、許可手続を定めなければならないことになっています（ガイドライン第2条第3項)。この許可を得ていない者はAPを利用することはできません。

この際、部局情報セキュリティ技術責任者は、APの利用を許可した特定部局情報システム臨時利用者に対し、京都大学全学情報システム利用規則[8]を遵守させるよう必要な措置を講じなければなりません（ガイドライン第2条第4項)。

具体的な許可手続きの例として、KUINS運用委員会では、ビジター用アカウントを発行する際、以下の手順を定めています[7]。各部局においても、同様の手順を定めることが必要です。

(1) アカウント発行者は、ビジター（全学情報システムの臨時利用者に相当）に発行した各アカウントに対して、対応するビジターの氏名、所属、住所、メールアドレス、電話番号を書面で記録し、利用終了日から最低3ヶ月間保管する。

(2) アカウント発行者は、各ビジターに対して、京都大学全学情報システム利用規則を遵守するよう伝える。

7. 参考文献/URL集

[1] アライドテレシス 無線LAN 基礎知識
http://www.allied-telesis.co.jp/products/list/wireless/knowl.html

[2] inSSIDer （無線LANのチャンネル使用状況を調べるフリーソフトウェア、Windows用）
http://www.metageek.net/products/inssider/

[3] Fluke Air-Check Wi-Fi Tester
http://jp.flukenetworks.com/enterprise-network/network-testing/AirCheck-Wi-Fi-Tester

[4] KUINS 提供無線 LAN の使い方
http://www.kuins.kyoto-u.ac.jp/ja/index.php から 「学内無線 LAN 設定」を選択

[5] 「WEP は 10 秒で解読可能」、神戸大と広島大のグループが発表
http://internet.watch.impress.co.jp/cda/news/2008/10/14/21162.html

[6] eduroam.jp 技術資料（研究会発表資料、技術情報など）
http://www.eduroam.jp/docs.html

[7] KUINS PPTPG 接続サービス
http://www.kuins.kyoto-u.ac.jp/ja/index.php?PPTPG

[8] 京都大学全学情報システム利用規則
http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/documents/pdf_p/zengaku_joho_system_riyoukisoku.pdf