HINET2007 部局無線 LAN アクセスポイント設置ガイドライン
(ゾーン A およびゾーン B)

平成 23 年 7 月 14 日　情報メディア教育研究センター

ノートパソコンやインターネット接続可能な携帯端末の普及により，無線 LAN アクセスに対する需要が増大しています。その一方で，暗号化等のセキュリティ対策が施されていない無線アクセスポイント（無線 AP）を悪用したネットワークの不正使用や偽装無線アクセスポイントによるパスワードの盗用などが問題となっています。本ガイドラインは，広島大学キャンパスネットワーク HINET2007 に部局・研究室等が用意した無線 LAN アクセスポイント（部局無線 AP）を接続する際，安全かつ適切な利用を行っていただくための設置基準と運用管理に必要な事項を定めるものです。ただし，各部局等では独自の情報セキュリティポリシー実施手順が定められており，無線 AP の設置そのものが認められてない場合もありますので，ご注意願います。

1. 対象ゾーン

本ガイドラインは HINET2007 ゾーン A（グローバルゾーン）およびゾーン B（ファイアウォールゾーン）に接続する無線 AP に対して適用されるものです。

2. 無線 AP の機能に関する要件

導入する無線 AP の要件としては，最低限以下の機能を有するものとします。

- インフラストラクチャモードとして動作できること
- 無線ネットワークを区別する SSID を設定できること
- ルータモードとして動作できること
- 暗号化方式として WPA2-PSK(AES)に対応していること

3. 無線 AP の運用方法

導入する無線 AP の運用については以下の事項を遵守し，設置・運用管理を行うこととします。

3-1) 設置・管理体制

無線 AP の設置・管理責任者はゾーン AB ホスト管理者とします。設置・管理責任者は設置場所を明確にし，設置後の無線 AP の運用状況を把握するとともに，不要になった場合はすみやかに撤去するようにして下さい。

3-2) 接続ネットワーク

無線 AP を設置するネットワークは HINET2007 ゾーン A またはゾーン B とし，設置する無線 AP は部屋内の単一情報コンセント（コネクタ）に接続されるように構成してください。

3-3) 無線 AP の設定

無線 AP の設定には次の事項を遵守して設定して下さい

(a) ルータ機能をオンにします。

無線 LAN ルータ（複数の LAN ポートが付いた無線 AP）の場合，WAN 側ポートをゾーン A または

ゾーン B として割り当てられた IP アドレスに設定し，コネクタに接続します。LAN（ローカル）側のネットワーク設定は利用者自身の環境に合わせて設定して下さい。

上記以外（LAN ポートが 1 つのみの無線 AP）の場合，LAN ポートをゾーン A またはゾーン B として割り当てられた IP アドレスに設定し，コネクタに接続します。

いずれの場合も，管理者は HINET2007 登録システムにログインし，接続したポートの MAC アドレスを登録する必要があります。

(b) SSID は「ZoneA−部屋番号(−部屋名称)」(ゾーン A の場合),「ZoneB−部屋番号(−部屋名称)」(ゾーン B の場合）とし，部屋名称は任意で付けてもよいこととします。例えば部屋番号が A101 の場合，SSID は「ZoneA−A101」もしくは「ZoneA−A101−mylabolatory」のようになります。SSID は最大 32 文字の英数字（記号を含む）です。

(c) 必ず暗号化を設定して下さい。推奨暗号化方式は最もセキュリティ強度が高い WPA2-PSK(AES)ですが，これを利用するためには無線 AP と接続する全てのクライアントが WPA2-PSK(AES)に対応していることが条件となります。どうしても WPA2-PSK(AES)に対応できない場合は WPA-PSK(AES)を選択して下さい。なお，WEP や WPA-PSK(TKIP)を選択しないで下さい。

暗号化キー（事前共有キー）は以下のルールに従って生成し，1 年に 1 回以上の頻度で変更するようにして下さい。

- 容易に推測できる文字列（英語の辞書等に載っている単語）を使わない
- 大文字，小文字，数字の全てを含むランダムな文字列とする
- 文字数は最低でも 8 文字とし，判別が難しい文字の利用はなるべく避ける

（参考）下記サイト(学内限定)へアクセスすると上記ルールに従った暗号化キーを自動生成します。

https://www.media.hiroshima-u.ac.jp/st/wifi_keygen

(d) 無線 AP の管理用パスワードについても，上記の暗号化キーの生成ルールに準じたものを設定するようにして下さい。

(e) 無線 AP の DHCP クライアント機能はオフにし，管理用 IP アドレスは，LAN（ローカルネットワーク）側のネットワーク設定に応じた IP アドレスを付与するようにして下さい。

(f) 近隣の無線 AP との電波干渉が生じないように，使用するチャネルの競合に注意して設定して下さい。また，電波出力制限機能等を用いて無線出力を必要最小限度に抑えるようにして下さい。

3-4) SSID と暗号化キーの取り扱い

ゾーン A およびゾーン B における SSID と暗号化キーは，厳重に管理する必要があります。原則として，管理者以外に知らせてはいけません。ゾーン A およびゾーン B では，すべてのインシデントに対し管理者が全責任を負うことになりますので十分注意して下さい。