

# ご使用上の注意点

## 初期化を行う際の注意

初期化を行う際は管理端末を DHCP の設定にせず、端末には初期化を行う PK-WL014-B の 1 台のみを接続し、他のアクセスポイントは接続しないで行ってください。

初期化実行後、アクセスポイントの再設定をおこなう場合、PK-WL014-B を有線で接続している管理端末の TCP/IP 設定にある IP アドレスを 169.254.128.\*\*\* に設定してください。(\*\*\*の部分は 132 以外で設定してください、“132”は 初期化後の PK-WL014-B が使用しています。)

## 初期化後の注意

本機は、初期化に時間がかかる場合があるため電源投入後、リセット後、設定登録後に最大約5分程度無線電波を停止する場合があります。

## RADIUS 設定を行う際の注意

「RADIUS Acct」の「Enable Backup RADIUS Authentication Server」の設定および「Link Integrity」の設定を行う場合は先に「Link Integrity」の設定を行って下さい。又、「Enable Backup RADIUS Authentication Server」の設定後は絶対に「Link Integrity」のタブをクリックしないで下さい、万が一クリックしてしまった場合は、初期化(工場出荷時状態 ユーザーズマニュアル P 92)に戻して下さい。

## 無線LAN AP-S100-B 使用時の無線LAN カードに関する注意

6 月に発売開始しました PK-WL014-B 「無線LAN AP-S100-B 」について、仕様上、下記のような現象が起こる可能性があります。以下の点にご注意願います。

PK-WL014-B 「無線LAN AP-S100-B 」のチャンネルの初期値は、オートチャンネルモードとなっており、同環境で14ch が使用されていない場合、自動的に14ch が選択されます。

よって、PK-WL06W 「無線LAN(11Mbps)カードEW 」をクライアントとして使用した場合、無線リンクを確立出来ない場合があります。

このため、使用するクライアントカードは14ch 対応の PK-WL006J 「無線LAN(11Mbps)カードEJ 」をご使用頂くことを推奨します。

11ch対応のPK-WL006W 「無線LAN(11Mbps)カードEW 」またはPK-WL009 「無線LAN USB ポックスE 」を使用する場合は、PK-WL014-B 本体と設定PC を有線LAN で接続し、チャンネルを1 ~ 11ch の間に設定してください。

## 設定内容の復元時に関する注意

「Commands」 - 「Download」タブで「Config」ファイルをダウンロードする場合「File Operation」の設定を“Download&Reboot”に必ず設定して下さい。

## Encryption 設定に関する注意

Encryption の設定変更を行う場合は無線クライアント側からは行わないで下さい。

万が一設定してしまった場合、「OK」を押した時点で Encryption Key が変更されるため、無線クライアント側からのアクセスができなくなります。この場合は有線側のアクセスポイント管理端末から正しく設定を行って下さい。

## TCP/IP Port 設定に関する注意

"Configure" - "Filterling" - "TCP/IP Port" にて "Enable TCP/UDP Port Filtering " のチェックを変更すると、ページエラーが発生しますが問題はありません。

エラーが発生した場合は、IE のツール インターネットオプション 詳細設定 “スクリプトデバックを使用しない”にチェックをし、F5 で画面の更新を行って下さい。

無線LAN AP-S100-B (PK - WL014 - B) のファームウェアは、随時改善して参ります。

最新版ファームウェアは下記URLにて提供予定ですので、常に最新版をダウンロードの上、ご使用いただくことをお勧めいたします。

弊社無線LAN商品 ホームページ URL:

「 <http://www.necinfrontia.co.jp/products/wlan/jp/download.html> 」

## 無線 LAN 製品ご使用時におけるセキュリティに関するご注意 (お客様の権利(プライバシー保護)に関する重要な事項です!)

無線 LAN では、LAN ケーブルを使用する代わりに、電波を利用してパソコン等と無線アクセスポイント間で情報のやり取りを行うため、電波の届く範囲であれば自由に LAN 接続が可能であるという利点があります。

その反面、電波はある範囲内であれば障害物(壁等)を越えてすべての場所に届くため、セキュリティに関する設定を行っていない場合、以下のような問題が発生する可能性があります。

- 通信内容を盗み見られる  
悪意ある第三者が、電波を故意に傍受し、  
ID やパスワード又はクレジットカード番号等の個人情報  
メールの内容  
等の通信内容を盗み見られる可能性があります。
- 不正に侵入される  
悪意ある第三者が、無断で個人や会社内のネットワークへアクセスし、  
個人情報や機密情報を取り出す(情報漏洩)  
特定の人物になりすまして通信し、不正な情報を流す(なりすまし)  
傍受した通信内容を書き換えて発信する(改ざん)  
コンピュータウイルスなどを流しデータやシステムを破壊する(破壊)  
などの行為をされてしまう可能性があります。

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。

無線 LAN 機器は、購入直後の状態においては、セキュリティに関する設定が施されていない場合があります。

従って、お客様がセキュリティ問題発生の可能性を少なくするためには、無線 LAN カードや無線 LAN アクセスポイントをご使用になる前に、必ず無線 LAN 機器のセキュリティに関する全ての設定をマニュアルにしたがって行ってください。

なお、無線 LAN の仕様上、特殊な方法によりセキュリティ設定が破られることもあり得ますので、ご理解の上、ご使用下さい。

セキュリティの設定などについて、お客様ご自分で対処できない場合には下記までお問い合わせ下さい。

NEC インフロンティア

マーケティング本部 ネットワーク販売推進部

無線 LAN 商品お問い合わせ窓口

TEL : 03-5282-5823

Mail : [wlan-info@nec-i.jp.nec.com](mailto:wlan-info@nec-i.jp.nec.com)

\*可能な限り Mail にてお問合せください。

当社では、お客様がセキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。