「無線ＬＡＮを利用した接続等を行う場合に実施すべき情報セキュリティ対策」

１．暗号化等の方式

暗号化等の方式については、ＷＰＡ２以上とすること。脆弱性の発見されているＷＥＰ方式やＷＰＡ方式は使用しない。

２．端末等の認証

原則として、ユーザを認証してから、ネットワークへの接続を許可するＩＥＥＥ８０２．１ｘ 認証による認証とする。ただし、小規模な場合、簡易な認証方式であるPSK認証による認証とすることができる。ＰＳＫ認証による認証を行う場合、端末及びアクセスポイントに設定するパスフレーズ（セキュリティキー）を定期的に更新する。

３．ＭＡＣ アドレスフィルタリングの実施

ＰＳＫ認証による認証を行う場合、登録された端末以外、無線ＬＡＮアクセスポイントへの接続できないようＭＡＣ アドレスフィルタリングを実施する。

４．ＳＳＩＤの設定

（１）ＳＳＩＤ のステルス化

正規ユーザ以外のユーザも容易にネットワークを発見して接続を試みることができないよう無線 LAN アクセスポイントから定期的に送信しているビーコン信号を停止する。正規ユーザには、別の手段でＳＳＩＤを通知し、端末へ設定してもらう必要がある。

（２）ＳＳＩＤ のANY 接続拒否

不特定多数の端末の無線ＬＡＮアクセスポイントへの接続を防ぐため、ＳＳＩＤ が「ANY」や空欄の設定になっている無線ＬＡＮ クライアントを拒否するよう無線ＬＡＮアクセスポイントの設定を行う。

５．電波の出力範囲

通信の傍受、無線ＬＡＮを経由した内部ネットワークへの侵入等の危険性を低減するため、アクセスポイントの電波の伝搬範囲を必要最低限の範囲とする。

６．無線ＬＡＮアクセスポイントの管理者パスワードの適切な設定

管理者は、無線ＬＡＮ アクセスポイントにログインした後、ユーザ管理や接続許可クライアントなどの様々な設定を行う。そのため、悪意のある第三者からの不正アクセスに備え、管理者のパスワードを推測されにくいパスワード（アルファベットの大文字/小文字、および数字の組み合わせで、最低８文字、１０文字以上を推奨）に設定し、かつ、３ヶ月に１回パスワード変更を行う。

７．無線ＬＡＮ アクセスポイントのログ収集

管理者は、不正なアクセスの早期検知や、事故後の追跡のためにも無線ＬＡＮ アクセスポイントのアクセスログを取得し、一定期間保存する。ただし、小規模な場合で、情報セキュリティ責任者が認めた場合には、省略することができる。

８．無線ＬＡＮを管理・運用するための知識の習得

管理者は、無線ＬＡＮを安全に管理・運用するための知識を習得しておかなければならない。

９．その他

上記の事項の他、申請が許可された際に追加で実施するよう指示された情報セキュリティ対策についても実施しなければならない。