

無線LANの利用方法 (学生向け)

白梅学園大学・白梅学園短期大学



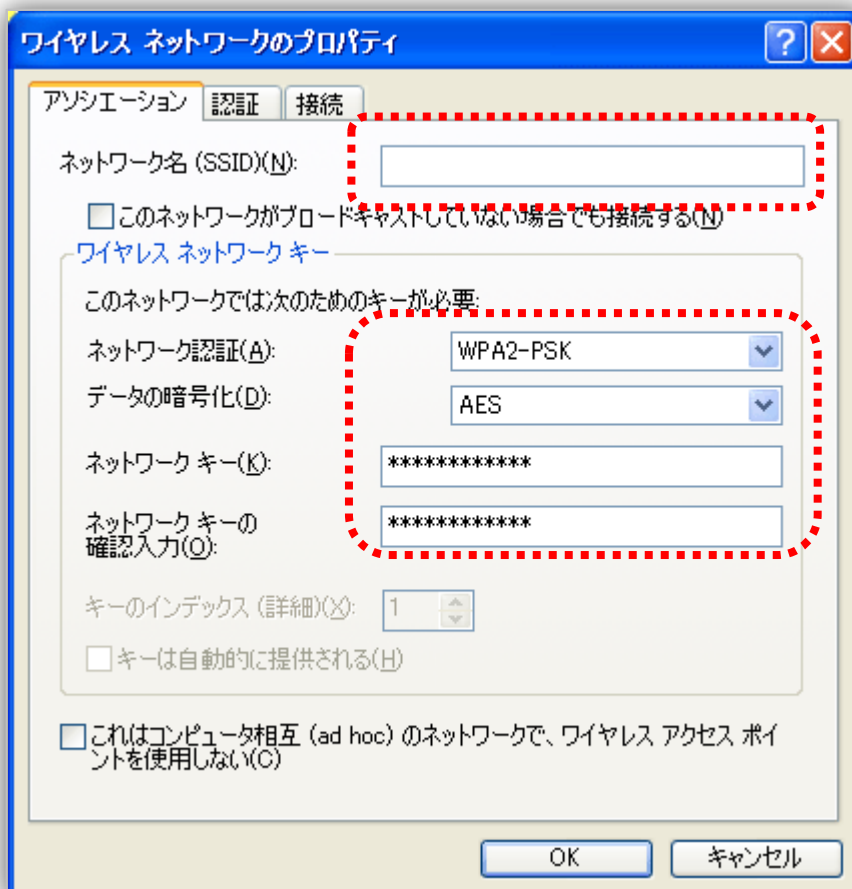
無線LANへの接続 Step.1

* 以下の情報を設定し、無線LANに接続してください。

※具体的な設定方法はお使いのパソコンやネットワーク機器の説明書をご確認ください。

ネットワーク名 (SSID)	
パスワード	
ネットワーク認証	WPA2-PSK (パーソナル)
データの暗号化	AES
通信規格	IEEE 802.11b/g

例) Windows XPの場合



無線LANへの接続 Step.2

- * Shiraume. に接続できたらWEBブラウザを起動して、どこでも良いので任意のWEBサイトにアクセスしてください。以下の認証ページが表示されます。


無線LANネットワーク 認証ページ

<http://>

- * 認証ページが表示されたらコンピュータ室で使用している「ユーザー名」「パスワード」を入力し、ログオンしてください。

ユーザー名

パスワード

 白梅学園大学 白梅学園短期大学
Shiraume Gakuen University & College

【無線LANネットワーク 認証】

ネットワークへのアクセスには、ログインが必要です。

ログイン方法

- ・ログインは左フレームから操作して下さい。
- ・「ユーザー名」「パスワード」はコンピュータ室で使用するものを入力してください。
- ・ログインしていない状態ではこのページ以外を表示することができません。

Copyright (c)2011 Shiraume Gakuen University, All Rights Reserved.

無線LANへの接続 Step.3

- * ログインに成功すると、認証完了ページが表示されます。

The screenshot shows a web interface for wireless LAN authentication. On the left, there is a sidebar with the text 'ログインしています' (Logging in) and a 'ログアウト' (Logout) button. The main content area is titled '【無線LANネットワーク 認証】' (Wireless LAN Network Authentication). A red dashed box highlights the message: 'ログインが完了しました。ネットワークを利用できます。' (Login completed. Network is available for use). Below this, a section titled '無線LAN利用上の注意' (Notes on Wireless LAN Usage) contains a warning about security risks and a list of potential threats: unauthorized interception, impersonation, and data tampering. It also provides a reference link: '【安心して無線LANを利用するために(総務省)】' (For safe wireless LAN use (Ministry of Internal Affairs)).

- * 以上で無線LANへの接続は完了です。インターネットを利用することができます。
 - ※一部のサービスは利用できない場合があります。
 - ※無線LANの同時利用者が多い場合、一時的にログインできない場合があります。

無線LAN利用の終了

- * 無線LANの利用を終了する場合には、そのままパソコン等を終了してください。約3分で自動的にログアウトされます。

※複数の通信機器を使用する場合

1つのユーザ名／パスワードで、同時に無線LANを使用できるのは「1台のみ」です。複数の通信機器を使用したい場合は、無線LANを使用している通信機器で以下のURLにアクセスし、ログアウトボタンを押してください。その後、改めて別の機器にてログインしてください。

<http://>

【無線LANネットワーク 認証】

ログインしています

ログアウト

ログインが完了しました。ネットワークを利用できます。

無線LAN利用上の注意

無線LANは電波の届く範囲内で、ケーブルを使用せずネットワークをご利用いただくことが可能ですが、セキュリティに関する設定を行っていない場合、悪意ある第三者によって以下のような問題が発生する可能性があります。

- 電波を故意に傍受し、IDやパスワード、個人情報、メールの内容などの通信内容を盗み見られる
- 傍受した通信内容を書き換えて発信する(改ざん)
- 特定の人物になりすまして通信し、正しくない情報を発信する(なりすまし)
- 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)

以下のサイトなどを参考に、十分注意してご利用ください。

[【安心して無線LANを利用するために\(総務省\)】](#)