アクセスポイント設定ガイド

はじめに

この「アクセスポイント設定ガイド」では、弊社製無線LANアクセスポイントLWN-A54APSの詳細な設定をWEBブラウザ上から行う方法についてご説明いたします。設定を行う前に以下の点を確認してください。

・「Logitec無線LANクライアントユーティリティ」がインストールされていること。

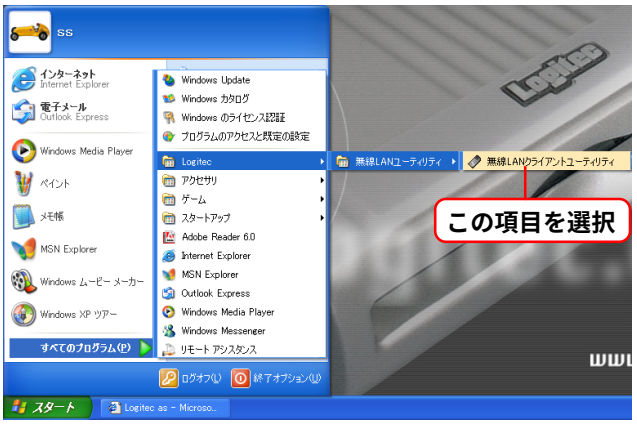
・設定用パソコンには、製品に付属のクライアントカードがセットされ、有線LAN経由でネットワークに参加していること。**設定は必ず有線LAN経由で行ってください。**通信チャネルや通信方式を変更する場合等に、無線通信で設定を行っていると、設定中に通信ができなくなることがあります。

・設定用パソコンが、弊社製アクセスポイントLWN-A54APSと同一セグメントのネットワーク上にあること。

目次

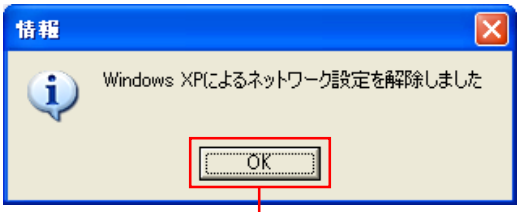
1. 設定画面へのログイン

①設定用パソコンから「スタート」－「プログラム」（Windows XP の場合は「すべてのプログラム」）-「Logitec」-「LWN-A54CBS」-「ロジテック無線 LAN クライアントユーティリティ」と選択してください。



画面は Windows XP のものです

※ Windows XP の場合、右のようなメッセージが表示される場合があります。そのまま「OK」をクリックしてください。
表示されない場合は、手動でワイヤレスネットワーク設定が変更してある必要があります。詳しくは「無線 LAN アクセスポイント・ユーザーズマニュアル」をご参照ください。

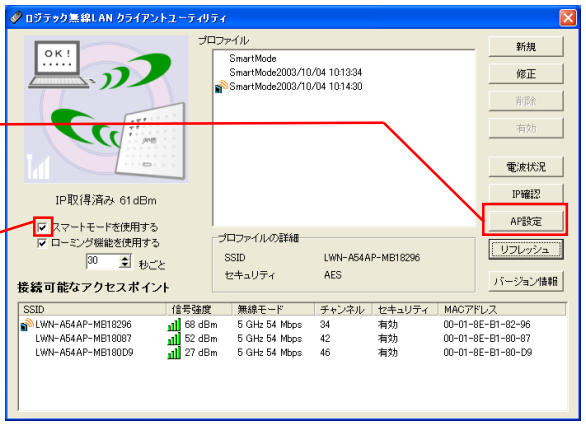


「OK」をクリック

②ロジテック無線LANクライアントユーティリティが起動します。「AP設定」ボタンをクリックしてください。
※「AP 設定」ボタンは管理者用 LAN カードのみ選択できます。

「AP 設定」をクリック

スマート認証モードを使用する場合は、この項目にチェックが入っていることを確認してください。



Point ポイント

はじめて本アクセスポイントとアクセスを行う場合は、同梱の LAN カードが自動的に「管理者用 LAN カード」となりますが、設定画面から、アクセスポイントの「設定初期化」を行った場合は、「管理者用 LAN カード」は、本アクセスポイントと一番初めにスマート認証されたカードとなります。
また、設定画面の「ユーザー管理」メニューより設定を行えば、「管理者用 LAN カード」を増やすことができます。

③「AP サーチ＆設定」画面が表示され、通信可能なアクセスポイント名と IP アドレス、MAC アドレスが表示されます。通信を行うアクセスポイント名をダブルクリックしてください。

アクセスポイント名を
ダブルクリック

Point ポイント

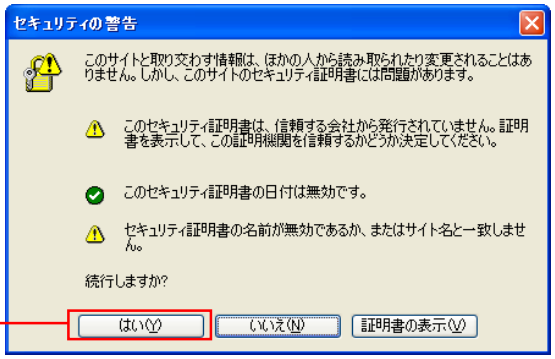
複数の弊社製アクセスポイントを導入される場合、１台ずつ順番に設定を行い、各アクセスポイントの名前を変更して MAC アドレスとアクセスポイントの組み合わせをメモしておくことをお勧めします。
弊社製アクセスポイントの無線側の MAC アドレスは機器本体の裏フタをあけなければ確認できません。

④WEB ブラウザをが自動的に起動し以下の画面が表示されます。「ログイン」ボタンをクリックしてください。

このボタンをクリック

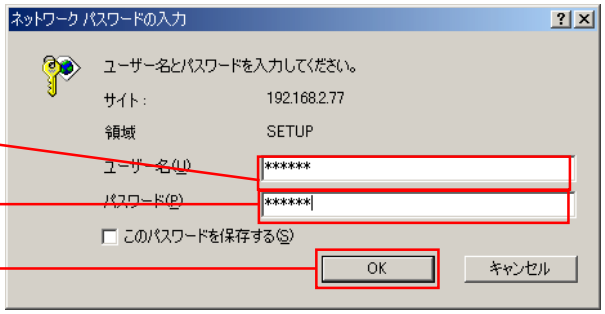
⑤「セキュリティの警告」画面が表示されます。「はい」をクリックしてください。
表示されない場合はそのまま次の手順へ押すすみください。

「はい」をクリック



⑥ネットワークパスワードの入力画面が表示されるので、ユーザー名とパスワードを入力して「OK」ボタンをクリックしてください。ユーザ名、パスワードは「無線 LAN アクセスポイント・ユーザズマニュアル」をご参照ください。

1. ユーザ名を入力
2. パスワードを入力
3. 「OK」をクリック



※ユーザー名・パスワードは大文字・小文字を区別します。また、設定メニューよりパスワードを変更する場合、半角英数字と記号を使用して最大 32 文字まで設定することができます。

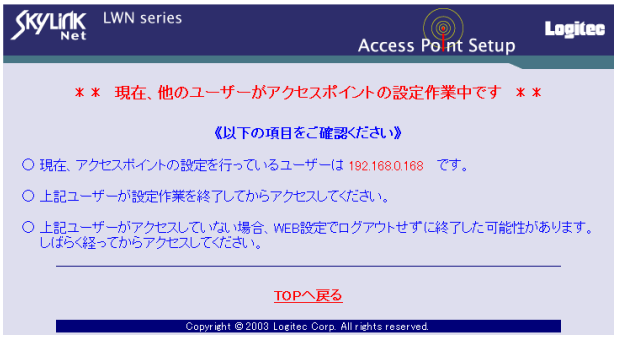
⑧設定画面に切り替わります。これでアクセスポイントの各設定が可能となります。

ご注意

ユーザー名、パスワードは、無線 LAN アクセスポイント・ユーザーズマニュアルをご参照ください。設定画面ログイン後は、安全のため必ず、パスワードを変更してください。パスワードは「パスワード設定」メニューより変更することができます。

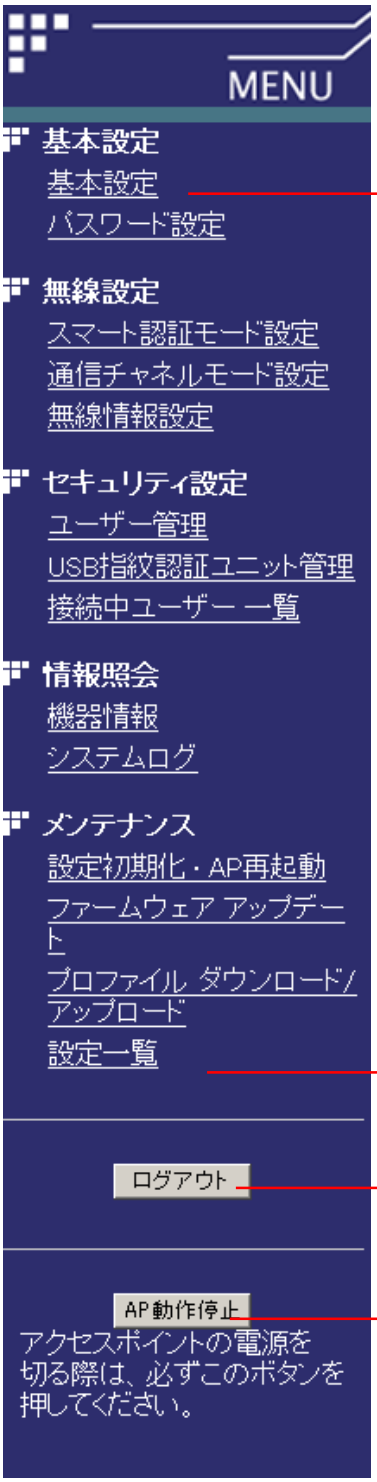
参考

すでに、別のユーザーが設定画面にアクセスしている場合は、右のメッセージが表示されます。この場合は、そのユーザーが設定を終えてからログインしてください。本アクセスポイントの設定画面へは一度に 1 クライアントしかアクセスできません。



2. メニューの見かた

アクセスポイントの設定画面にログインすると、左側に以下のような設定メニューの一覧が表示されます。各項目から設定・参照できる内容につきましては次ページをご参照ください。



設定メニュー

ログアウトボタン

設定を終了するときは、必ずこのボタンをクリックしてください。このボタンを押してログアウトしないと、5分間は他のクライアントからは設定画面にアクセスできなくなります。これは本アクセスポイントの設定画面へ複数のクライアントからのアクセスを防止するための仕様です。

AP動作停止

アクセスポイントの動作を停止する場合、本体の電源スイッチを切る前に必ずこのボタンを押してください。動作中に電源スイッチを切ると故障の原因ともなります。

■メニューの内容

各設定メニューからは以下のような設定が可能となります。

基本設定
アクセスポイントの名前、IP アドレスの取得方法、時刻を設定します。

パスワード設定
設定画面ログイン時のパスワードを変更します。

スマート認証モード設定
クライアントとの通信をスマート認証または手動設定から選択します。

通信チャネルモード設定
通信するネットワーク形態をシングルチャネルまたは複合通信から選択し、通信方式を 802.11a **または** 802.11b **に設定します。**

無線情報設定
クライアントとの通信に使用する SSID**、暗号化設定、送信チャンネル等の諸設定を行います。**

ユーザー管理
クライアント間通信の禁止/許可や、他社製無線LAN**カードが通信を行う場合の設定、**MAC**アドレスによるユーザーの管理を行います。**

USB 指紋認証ユニット管理
バイオモードで通信を行う場合に、認証に使用するUSB**指紋認証ユニットおよび通信を管理する方の指紋を登録します。**

接続中ユーザー一覧
現在アクセスポイントと通信を行っているユーザーが一覧表示されます。

機器情報
AP **名、**MAC **アドレス、システムバージョン、送受信パケットなどの情報を参照できます。**

システムログ
AP **アクセスログ、**AP **エラーログを参照できます。**

設定初期化・AP 再起動
設定の初期化とアクセスポイントの再起動を実行できます。

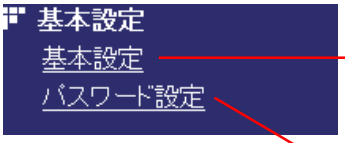
ファームウェアアップデート
アクセスポイントのファームウェアが更新された場合に、アップデートを行うことができます。

プロファイルダウンロード / アップロード
アクセスポイントの設定をパソコン側にダウンロードすることと、ダウンロードしたファイルをアクセスポイント側にアップロードすることができます。ローミング設定時や、障害からの復旧の際に使用します。

設定一覧
現在の設定を一覧表示します。

3．設定方法

基本設定



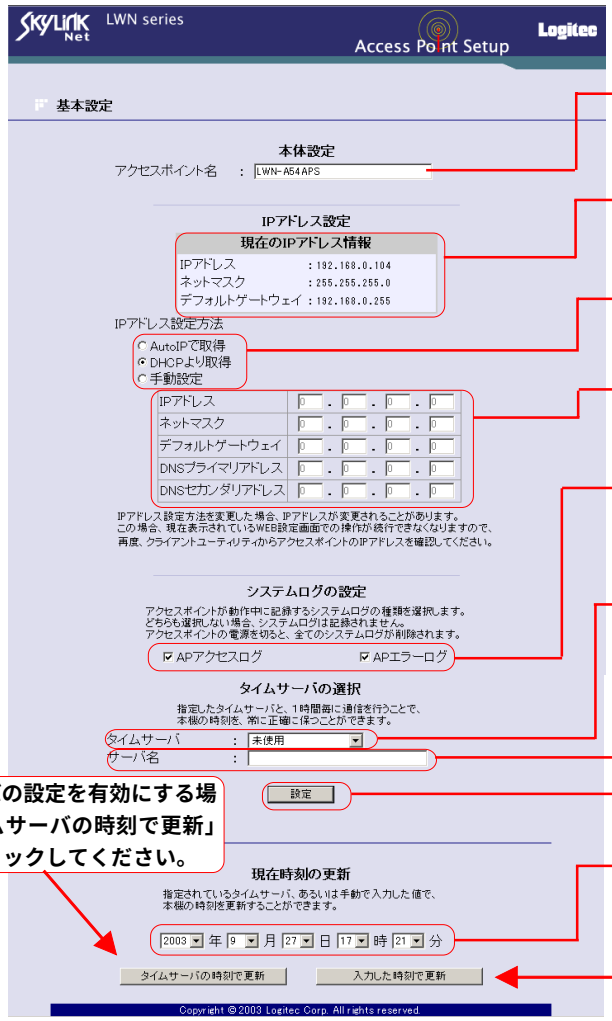
「基本設定」メニューは「基本設定」と「パスワード設定」の２つのサブメニューに分かれています。

・「基本設定」では、アクセスポイントの名前、IP アドレスの取得方法、時刻の設定といったアクセスポイントの設定・管理に必要な基本的な項目が設定可能です。

・「パスワード設定」では、アクセスポイントにログイン時のパスワードを変更することができます。

基本設定

設定メニューから「基本設定」のサブメニューを選ぶと以下の画面が表示されます。各項目の詳細については次ページをご参照ください。



アクセスポイントの名前を変更する場合はここに新しい名前を入力します。

現在アクセスポイントに割り振られている IP アドレス等が表示されます。

この中から IP アドレスの設定方法を選択します。

手動設定を選択した場合、ここに必要な値を入力します。

アクセスポイントへのアクセスログ、エラーログを記録する場合はチェックを入れます。

現在時刻を合わせるタイムサーバを選択する場合、ここで指定します

タイムサーバのアドレスを直接指定する場合、ここで指定します

設定が終わったら、このボタンをクリックすると、設定内容が反映されます。

ここには、現在設定されている時刻が表示されています。（ここで手動で時刻を入力することもできます）

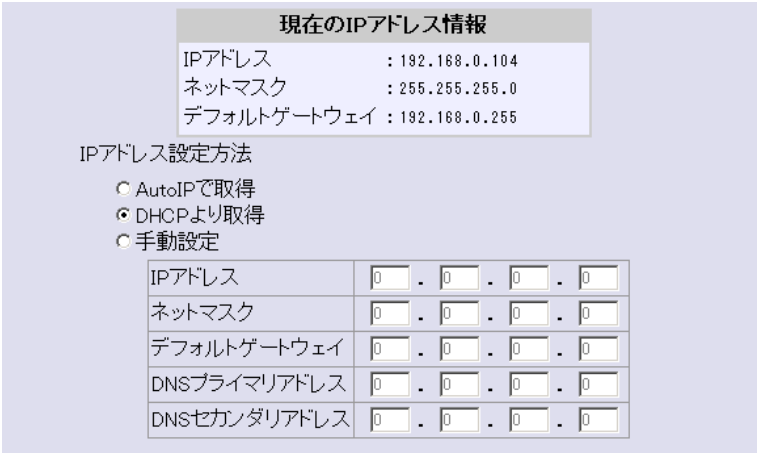
時刻の更新を行いたい場合、タイムサーバを参照するか、時刻を入力するか選ぶことができます。

タイムサーバの設定を有効にする場合は「タイムサーバの時刻で更新」ボタンをクリックしてください。

アクセスポイント名

アクセスポイント名はクライアントユーティリティよりAPサーチを使用してアクセスポイントを検索する際に表示される名前です。本製品と同じアクセスポイントはすべて「LWN-A54APS」と出荷時に設定されていますので、同じアクセスポイントが複数ある場合は、ここで出荷時設定から名前を変えておくことをお勧めします。

※アクセスポイント名はSSIDとは異なります。SSIDを変更したい場合は、「無線設定」の「無線情報設定」より行ってください。



IP アドレス設定方法

アクセスポイントの設定はWEBブラウザを使用するため、IPアドレスの設定が必要となります。本製品のIPアドレスは以下の３つの方法より設定可能です。

Auto IP で取得

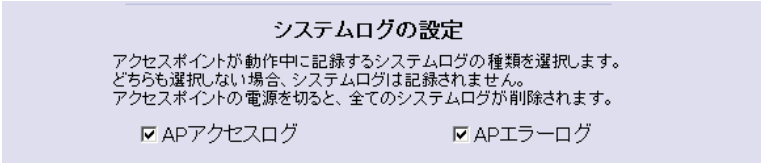
・この設定が選択されていると、DHCPサーバがない環境でも、自動的にIPアドレスを自己生成します。DHCP サーバがない場合は 169.254.*x.x*/255.255.0.0（*x.x* は任意の値）の IP アドレス / ネットマスク（サブネットマスク）がつきます。DHCP サーバがある場合は、サーバを自動的に検出し DHCP クライアントとして動作します。

DHCP より取得

・本アクセスポイントが参加しているネットワーク内に DHCP サーバがある場合、この設定を選択しているとDHCPサーバよりIPアドレスを取得します。出荷時にはこの設定が選択されています。

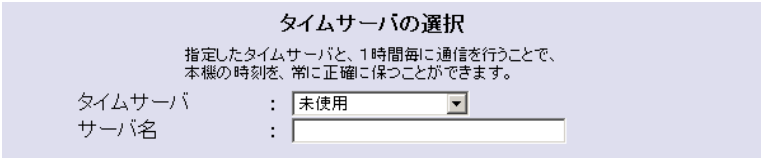
手動設定

・本アクセスポイントのIPアドレスを固定したい場合はこの設定を選択し、IPアドレス、ネットマスク（サブネットマスク）デフォルトゲートウェイ等の値を入力しネットワーク内で本製品の識別に必要な値を固定します。異なったネットワークからIPアドレスを直接指定する場合もあるため、デフォルトゲートウェイの設定は必ず行ってください。
ここで入力する値についてはネットワーク環境により異なりますので、システム管理者にお問い合わせください。



システムログの設定

アクセスポイント動作中のアクセスログ、エラーログを記録することができます。記録する場合は、各項目のチェックボックスにチェックを入れてください。チェックを入れない場合、ログは記録されません。また、基本的にアクセスポイントの電源を切ると全てのシステムログは削除されます。(アクセスポイント側面のリセットスイッチを押し、ソフトウェアリセットの再起動をした場合はログは残ります。) ログを保存しておきたい場合は、「情報照会」の「システムログ」メニューで行います。スループットをあげたい場合は、チェックを外してください。



タイムサーバの選択

タイムサーバとは、インターネット上にある、現在時刻を提供しているサーバのことです。ここでタイムサーバを指定すると、1時間ごとに指定したタイムサーバと時刻同期を取ります。タイムサーバは「マイクロソフト」「通信総合研究所1」「通信総合研究所2」「通信総合研究所3」から指定ができます。自動切断モードを実行する場合や、ログを記録する際に、なるべく正確な時刻を使用するために、、タイムサーバを指定することをお勧めします。

※その他のタイムサーバをご指定になる場合は、「タイムサーバ」の欄で「サーバ名指定」を選択し、「サーバ名入力」欄に指定するタイムサーバのアドレスを入力してください。

ここまでに行った設定を反映する場合は「設定」ボタンをクリックしてください。

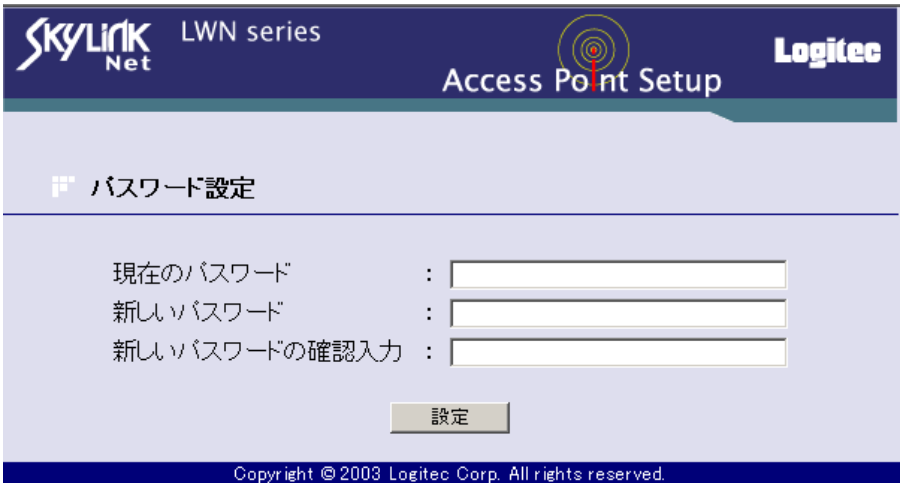
現在設定されている時刻が表示されます。画面の更新を行うと、最新の設定で現在時刻を表示します。

現在時刻の更新

タイムサーバを参照して時刻を更新する場合は「タイムサーバの時刻で更新」ボタンを、直接時刻を指定した場合は「入力した時刻で更新」ボタンをクリックしてください。
指定した方法で時刻の更新を行います。

パスワード設定

設定メニューから「パスワード設定」のサブメニューを選ぶと以下の画面が表示されます。



パスワードを変更する場合、はじめに現在のパスワードを入力し、次に新しいパスワードを入力してください。最後に新しいパスワードを確認入力し、設定ボタンをクリックすればパスワードの変更は完了です。次回ログイン時からは新しいパスワードを使用することができます。

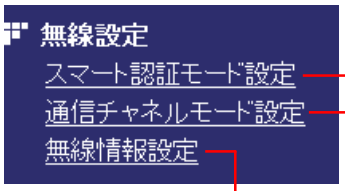
※パスワードは半角英数字、記号を使用して最大31文字まで設定可能です。大文字小文字を区別します。

ご注意

変更したパスワードは絶対に忘れないようにしてください。忘れてしまった場合、設定画面にアクセスできなくなります。その場合、弊社といたしましても、工場出荷時の設定に戻す以外のサポートはいたしかねますのでご注意ください。
工場出荷時に戻した場合、設定した内容は全て失われます。
ただし、パスワード変更前のアクセスポイントの設定情報をパソコンに保存していた場合はその状態までは回復させることができます。詳しくは「プロファイルダウンロード / アップロード」をご参照ください。

無線設定

「無線設定」メニューは「スマート認証モード設定」と「通信チャネルモード設定」「無線情報設定」の３つのサブメニューに分かれています。クライアントを通信に参加させる前に、この３つの設定を完了させておいてください。参加後に設定を行うと、クライアント側で再設定が必要になります。



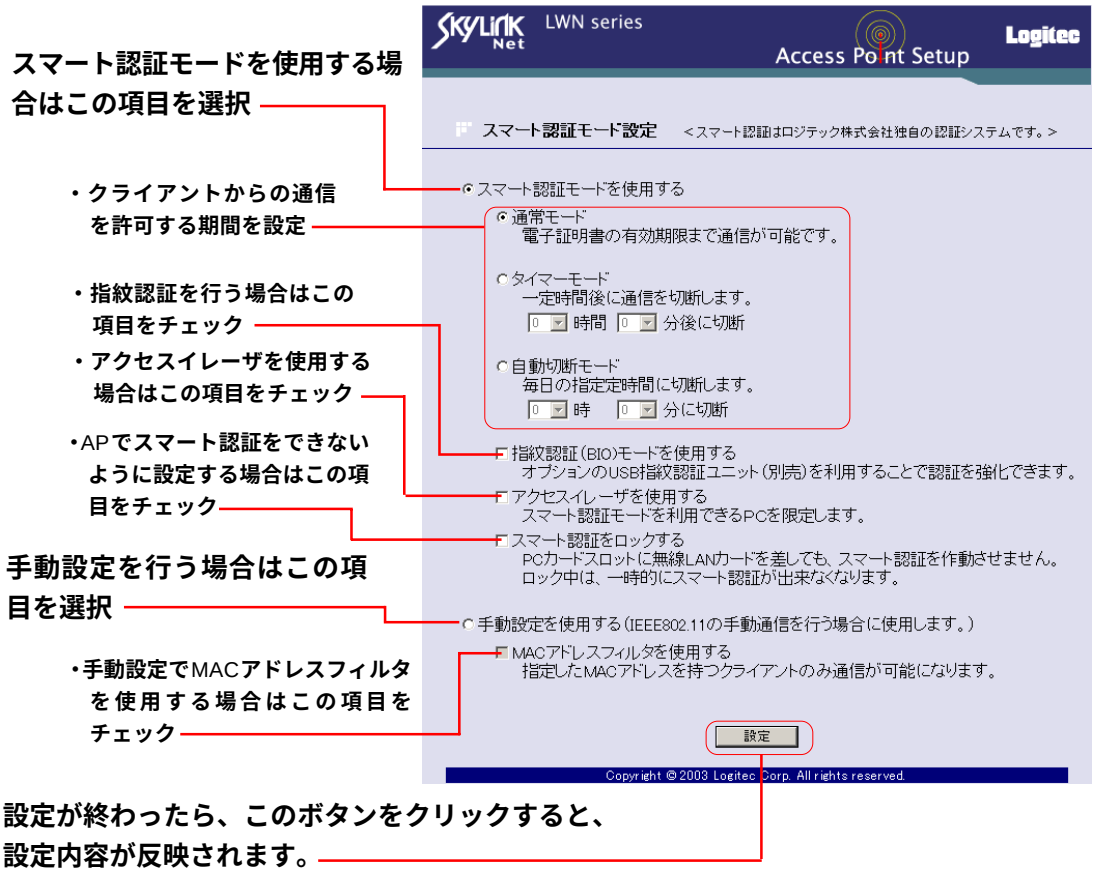
・「スマート認証モード設定」では、スマート認証を行う場合のオプション（「有効期限の設定（通常、タイマー、自動切断から選択）」「指紋認証（BIO）モードの設定」「アクセスイレーザの設定」を指定できます。また、手動設定を選択することも可能です。

・「通信チャネルモード」では本アクセスポイントで１つのネットワークを構築するか、２つのネットワークを構築するかを選択することができます。

・「無線情報設定」では通信に必要な具体的な設定（SSID、暗号方式、送信チャネル等）を行います。設定内容は「スマート認証モード設定」「通信チャネルモード設定」の設定内容に応じて変わります。

スマート認証モード設定

設定メニューから「スマート認証モード設定」のサブメニューを選ぶと以下の画面が表示されます。各項目の詳細については次ページをご参照ください。



スマート認証モードを使用する場合はこの項目を選択

・クライアントからの通信を許可する期間を設定

・指紋認証を行う場合はこの項目をチェック

・アクセスイレーザを使用する場合はこの項目をチェック

・APでスマート認証をできないように設定する場合はこの項目をチェック

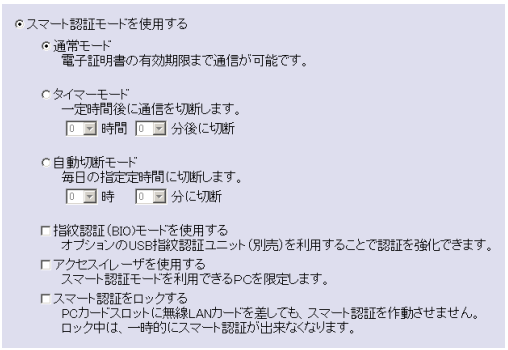
手動設定を行う場合はこの項目を選択

・手動設定でMACアドレスフィルタを使用する場合はこの項目をチェック

設定が終わったら、このボタンをクリックすると、設定内容が反映されます。

スマート認証モードを使用する

スマート認証とはクライアントカードをアクセスポイントにセットして行う認証のことです。
スマート認証モードでは、アクセスポイントに弊社製無線LANカード（LWN-A54CBS）をセットして、取り外すだけで、そのカードをセットしたクライアントとアクセスポイントの通信が可能となりますので、クライアント側で面倒な設定は必要ありません。



※具体的には、アクセスポイントに無線LANカードをセットしたときに、アクセスポイントから無線LANカードへ、SSID、暗号モードの情報、APの公開鍵、カード用秘密鍵を発行し、カード側からアクセスポイントにMACアドレスを送ります。情報の受け渡しを行った無線LANカードをクライアントパソコンにセットすると、交換した情報を元に認証と通信を行います。通信開始時にはLDLS（Logitec Datalink Layer Security）認証によるユーザ確認を行い、通信時はユーザーごとに異なる暗号キーを使用します。

※LDLS認証とは、通信開始時にデータリンク層において公開鍵暗号方式でアクセスポイントとクライアント間の相互認証を行い、その後セッションキー（暗号キー）を生成し、そのキーをAP-クライアント間で共有して通信を行う弊社独自の認証方式です。

スマート認証モードは、以下のオプションが選択可能です。設定後は画面下部の「設定」ボタンをクリックしてください。設定内容が反映されます。

通常モード

クライアントはスマート認証時に発行された電子証明書の有効期限まで通信が可能になります。出荷時設定では、クライアントに発行する電子証明書は無期限になっておりますので、有効期限を設定したい場合は、「セキュリティ設定」の「ユーザー管理」内の登録ユーザー一覧より、個別に設定してください。

タイマーモード（相対時間指定）

現在の時刻から一定時間が経過したら通信を切断するように設定ができます。この設定を行う場合は「タイマーモード」のラジオボタンをONにして、ドロップダウンリストより時間を選択してください。
※通信切断後にアクセスポイントと通信を再開する場合は、再度無線LANカードをアクセスポイントにセットしてスマート認証を行ってください。

自動切断モード（絶対時間指定）

毎日一定の時刻が来ると通信を切断するように設定できます。この設定を行う場合は「自動切断モード」のラジオボタンをONにして、ドロップダウンリストより時間を選択してください。
※通信切断後にアクセスポイントと通信を再開する場合は、再度無線LANカードをアクセスポイントにセットしてスマート認証を行ってください。

指紋認証（BIO）モードを使用する

このチェックボックスにチェックを入れると、ネットワーク管理者の指紋を認証に使用し、管理者が許可したユーザーのみネットワークに参加ができるようなります。スマートモードのセキュリティに加え、指紋認証による制限を加えるので、より高度なセキュリティが確保されます。このモードを使用するには別売の弊社製USB指紋認証ユニット（LWN-BF16U）が必要です。

アクセスイレーザを使用する

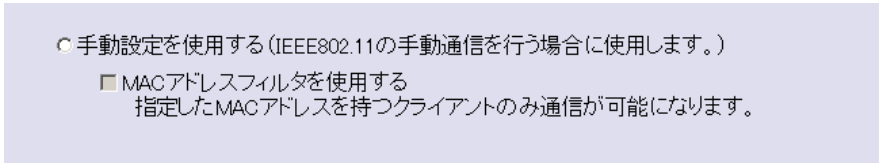
この機能をONにすると、スマート認証時に無線LANカードへ登録されたパラメータ（セッションキー、SSID）が、クライアントパソコンへ接続すると同時に無線LANカードから削除されます（パラメータはクライアントパソコン内部にセキュアな形で保持されます）。これにより、該当する無線LANカードを使用可能なパソコンが限定され、最初に装着されたパソコンでのみ使用可能となります。

スマート認証をロックする

このチェックボックスにチェックを入れると、アクセスポイントに無線LANカードをセットしてもスマート認証が行われないようになります。すでに認証を行ったクライアントの通信は継続されます。
管理者がアクセスポイントの近くにいない場合などに、不正認証を防ぎセキュリティを確保することができます。

ポイント

「通常モード」「タイマーモード」「自動切断モード」は１台のアクセスポイントで、アクセスするクライアントにより、別々の設定をおこない、同時に併用することが可能です。
たとえば、「タイマーモード」の設定で一定時間後に通信を切断するという設定にした後に、クライアント 1 に対してスマート認証を行い、その後に設定を「自動切断モード」で毎日 17 時に通信を切断する設定にして、クライアント 2 に対してスマート認証を行えば、クランアント 1 とクライアント 2 はそれぞれ別々の時間設定でアクセスポイントにアクセスすることになります。



手動設定を使用する

この設定を選択すると、SSID、暗号化方式、暗号化キーなどの設定を全て手動で行うことになります。選択後は無線情報設定画面で必要な設定を行ってください。他社製無線 LAN カードを使用して 802.11a または 802.11b 通信を行う場合に使用します。

MAC アドレスフィルタを使用する

手動設定にて通信を行う場合にクライアントの通信の禁止/許可をMACアドレスにて行う場合はこのチェックボックスにチェックを入れてください。
MACアドレスフィルタ設定を行わない場合、SSID、暗号キーが一致すれば無制限にクライアントのアクセスを受け付けてしまいます。セキュリティ確保のため、手動設定の場合もMACアドレスフィルタの設定を行うことをお勧めします。MAC アドレスフィルタ設定については「セキュリティ設定」の「ユーザー管理」をご参照ください。

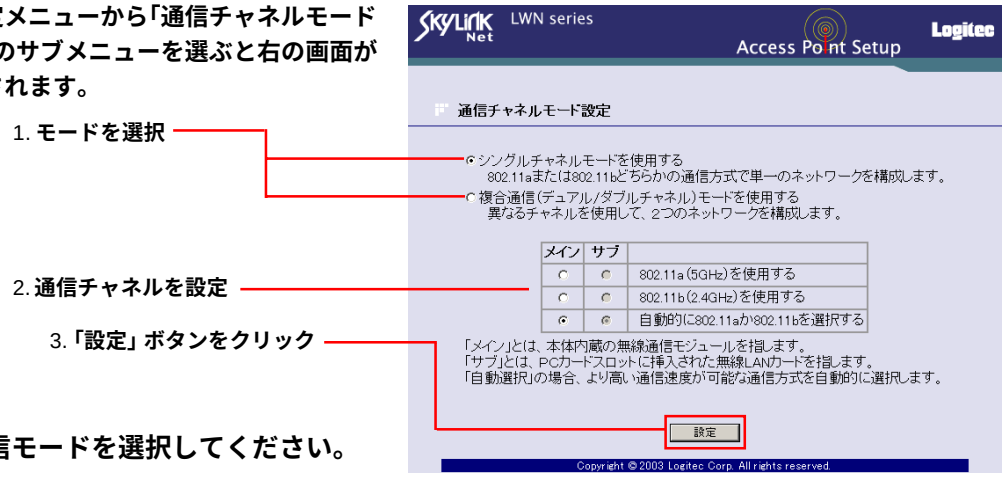
ご注意

スマート認証を行った無線 LAN カードと手動設定（802.11 通信）の無線 LAN カードの混在は、セキュリティ上の理由から不可となります。そのため、手動設定に設定した場合、それまでスマート認証で通信を行っていたユーザも再度手動にて設定を行わなければ、通信ができなくなります。

「設定」ボタンをクリックしてください。ここまでに行った設定が反映されます。

通信チャネルモード設定

設定メニューから「通信チャネルモード設定」のサブメニューを選ぶと右の画面が表示されます。



1. 通信モードを選択してください。

シングルチャネルモードを使用する

このモードを選択すると本アクセスポイントを使用して、802.11a または 802.11b どちらか 1 つのネットワークを運用する場合はこのモードを選択します。

複合通信（デュアル / ダブルチャネル）モードを使用する

このモードを選択すると、本アクセスポイントに付属の無線 LAN カード（または無線 LAN アダプタ）をセットすることにより、1 台で 2 つのネットワークを構築することができます。2 つのネットワークは、それぞれ別の規格を使用する（デュアルモード）ことも、同規格の通信モードで別のチャンネルを使用する（ダブルモード）ことも可能です。

2. 通信チャネルを設定してください。

通信チャネルは「802.11a」「802.11b」「自動選択」から選択します。802.11a または 802.11b のどちらかの通信で固定する場合は「802.11a（5GHz）を使用する」「802.11b（2.4GHz）を使用する」のいずれかを選択します。どちらで通信を行っても構わない場合は「自動的に 802.11a か 802.11b を選択する」を選択してください。

参考

「メイン」とは、本体内蔵の無線通信モジュールを使用した通信を指します。
「サブ」とは、PC カードスロットにセットされた無線 LAN カードがアンテナとなる通信を指します。
複合通信を選択した場合のみ設定してください。
「自動選択」の場合、802.11a と 802.11b が交互に切り替わり、クライアントが最初に接続を試みた規格を選択し、使用します。

※ 802.11b は室内、屋外でも利用できますが、802.11a は電波法上室内のみの使用に限定されておりますのでご注意ください。

3. 設定が終わったら「設定」ボタンをクリックしてください。

設定内容が反映されます。

参考

複合通信を行う場合は、通信中アクセスポイントに弊社製無線 LAN カード（LWN-A54CBS）をセットしておく必要があります。詳しくは「無線 LAN アクセスポイント　ユーザーズマニュアル」をご参照ください。

無線情報設定

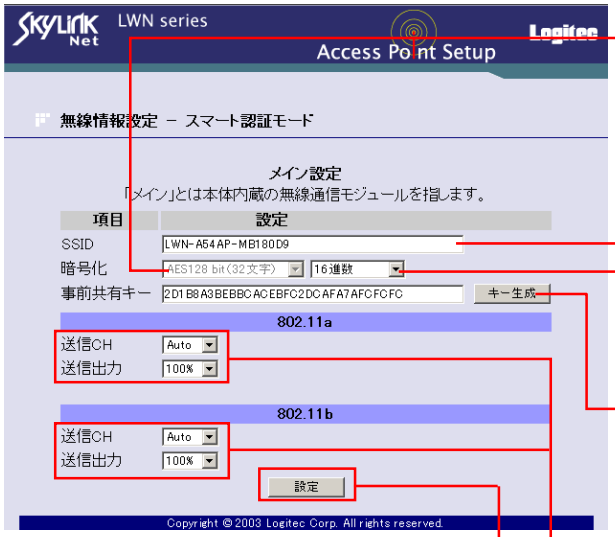
ご注意

「無線情報設定」を行った後に、「スマート認証モード設定」「通信チャネルモード設定」の変更を行うと、再度「無線情報設定」をやり直さなければいけません。「無線情報設定」は「スマート認証モード設定」「通信チャネルモード設定」を終えてから行ってください！

「無線情報設定」のサブメニューでは、本製品のSSID、暗号化方式、暗号化キー（または事前共有キー）、送信チャネル、送信出力の設定を行うことができます。また、設定可能項目は「スマート認証モード設定」「通信チャネルモード設定」の設定内容に異なります。該当する部分をご参照ください。

■「スマート認証モード設定」で「スマート認証モードを使用する」に設定している場合

この場合、以下のような画面が表示されます。必要に応じてSSID、入力形式、事前共有キー（注）、送信チャネル、送信出力の設定を行ってください。各項目の内容については17ページをご参照ください。



※シングルチャネルモードを選択した場合に表示される画面

参考：
スマート認証時は暗号化方式はAESに固定され、WEPを選択することはできません

SSIDを変更する場合はここに入力

暗号鍵（キー）の入力形方式を選択します

事前共有キー（注）の値を変更する場合はこのボタンをクリックするか、左側のテキストボックスに直接値を入力します。

通信に使用する規格の送信チャネルと出力を設定します。（自動選択にしている場合は、802.11aと802.11b両方設定してください）

全ての設定が終了したら「設定」ボタンをクリックしてください。

注：事前共有キー（PSK：Pre-Shared Key）とは、LDLS認証を行う際に使用する暗号通信用の鍵（キー）です。

○「通信チャネルモード設定」で「複合通信」を選択している場合

複合通信を選択している場合、メイン設定の下にサブ設定という画面が追加されます。サブ設定で表示される設定項目もメイン設定と同じとなります。ただし、デュアルモードを選択している場合は、SSID、暗号化、事前共有キーの設定はメイン設定で設定された値と同じになりますのでグレイアウトして設定できません。デュアルモードのサブ設定では、送信チャネル、送信出力のみ設定を行ってください。

■「スマート認証モード設定」で「手動設定を使用する」に設定している場合

この場合、以下のような画面が表示されます。必要に応じてSSID、暗号化方式、入力形式、暗号化キー、送信チャネル、送信出力の設定を行ってください。各項目の内容については次ページをご参照ください。

802.11a通信を行う場合に設定

802.11b通信を行う場合に設定

SSIDを変更する場合はここに入力

暗号化方式、キー入力方式を選択

暗号化キーの値を変更する場合はこのボタンをクリックするか、左側のテキストボックスに直接値を入力します。

通信に使用する規格の送信チャネルと出力を設定します。

全ての設定が終了したら「設定」ボタンをクリックしてください。

※シングルチャネルモードを選択した場合に表示される画面

Point ポイント

「通信チャネルモード設定」で、通信に使用する規格を「自動的に802.11aか802.11bを選択する」にしている場合は802.11aと802.11b共に送信チャネルと送信出力の設定を行っておいてください。

○「通信チャネルモード設定」で「複合通信」を選択している場合

複合通信を選択している場合、メイン設定の下にサブ設定という画面が追加されます。サブ設定で表示される設定項目もメイン設定と同じとなります。

※サブ設定でもサブ設定の通信に使用する規格を「自動的に802.11aか802.11bを選択する」に設定している場合は802.11aと802.11b共に送信チャネルと送信出力の設定を行っておいてください。

設定項目について

メイン設定 / サブ設定

シングルチャネルモード、および複合通信時にメインとなるネットワークの設定を行う部分がメイン設定となります。メインとなるネットワークはアクセスポイント自身の内部モジュールを使用して通信を行います。
これに対して、複合通信時にサブとなるネットワークの設定を行う部分がサブ設定となります。サブとなるネットワークはアクセスポイントに装着した弊社製無線 LAN カード（LWN-A54CBS）をアンテナとして通信を行います。

SSID（Service Set Identification）

ここではアクセスポイントのSSIDを変更することができます。SSIDとは通信機器同士を認識するためのIDです。手動設定を行う場合は、このIDをクライアント側でも設定してください。SSIDは半角英数字と記号を使用して最大 32 文字まで使用できます。大文字小文字は区別します。（SSIDは1つのアクセスポイントが構築している無線ネットワークに環境内の全ての機器が同じ番号に設定されていなければいけません。ただし、手動設定にて複合通信を行う場合は、メインとサブに異なる SSID を使用できます。）

暗号化

ここでは、通信に使用する暗号化の種類を選択することができます。スマート認証モードに設定している場合は AES128bit に固定されます。手動設定の場合は AES128bit、WEP64bit、WEP128bit、WEP152bit、off（暗号化なし）の５つから設定を選択できます。ただし、802.11b 通信では WEP152bit には対応していません。

入力方式

通信時の認証に使用する暗号化キーを16進数で行うかASCII文字で行うかを選ぶことができます。ASCII 文字で入力を行うと、入力された文字を元にクライアント側、アクセスポイント側共に特定のアルゴリズムを使用して 16 進数を生成します。

事前共有キー（スマート認証時）

スマートモード選択時に、LDLS 認証のための通信を暗号化するための鍵です。
※キー生成ボタンを押せば、アクセスポイント側で自動的に任意の値を生成することもできます。

暗号化キー（手動設定時）

手動設定時に選択された暗号方式に従って、任意の値を入力します。
※キー生成ボタンを押せば、アクセスポイント側で自動的に任意の値を生成することもできます。

送信 CH（チャネル）

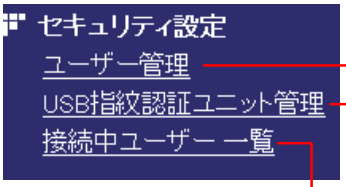
802.11a では 34、38、42、46 の 4 チャンネルから通信を行うチャネルを選択できます。
802.11b では 1～14 チャネルから通信を行うチャネルを選択できます。複数の 802.11b 通信ネットワーク環境が混在している場合は、他のネットワークが使用しているチャネルの状況を判断して設定を行ってください（4 チャンネル以上離すことを推奨）
802.11a、802.11b 共に通常は Auto を選択しておけば自動的にチャネル調整を行います。

送信出力

無線電波の送信出力を 100%、50%、25%、12.5%、Min から選択します。電波の盗聴などを避けなければいけない環境でご使用の場合は、なるべく出力を弱めに設定して、限られたエリアでしか通信ができないように調節しておくことをお勧めします。

セキュリティ設定

「セキュリティ設定」メニューからは「ユーザー管理」「USB 指紋認証ユニット管理」「接続中ユーザー一覧」を選択することが可能です。



・「ユーザ管理」ではクライアント側のカードのMACアドレスを元に通信の許可/拒否や権限の変更と、クライアント間通信の許可/拒否の設定、他社製無線LANクライアントを使用する場合の必要な情報の出力を行います。

・「USB指紋認証ユニット管理」では、指紋認証（BIO）モードで認証に使用する弊社製 USB 指紋認証ユニットおよび指紋の管理を行います。

・「接続中ユーザー一覧」では、現在接続されているユーザーの一覧が表示されます。

ユーザー管理

設定メニューから「ユーザー管理」のサブメニューを選ぶと以下の画面が表示されます。各項目の詳細については次ページをご参照ください。

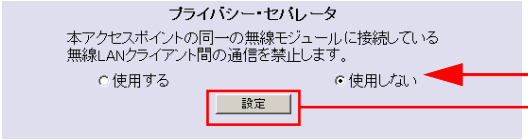
クライアント間通信を制限する場合はここで行います。

他社製無線 LAN クライアントと通信を行う場合に使用します。

事前にMACアドレスがわかっていて、あらかじめフィルタリングしておく必要がある場合は、ここでMACアドレスを追加しておきます。（スマート認証時では、弊社製対応無線 LAN カードは、アクセスポイントにカードをセットするだけで自動的にMACアドレスが登録されるので、ここで追加する必要はありません）

現在登録されているMACアドレスの一覧が表示されます。

登録ユーザー一覧の中で設定を変更した場合は「更新」ボタンを押してください。



1.「使用する」または「使用しない」を選択
2.「設定」ボタンをクリック

プライバシーセパレータ

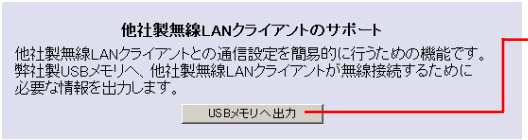
この設定を「使用する」に設定した場合本アクセスポイントにアクセスしているクライアントはお互いのパソコンを参照できなくなるようになります。(ファイル共有等は行えません) この設定は複合通信時は使用できません。

「使用しない」にした場合、本アクセスポイントにアクセスしているクライアント同士が通信可能になります。

選択後、「設定」ボタンをクリックすると、設定が有効になります。

Point **ポイント**

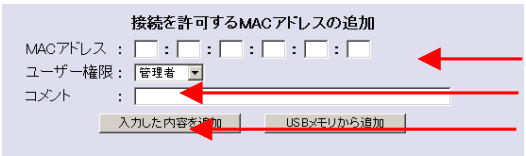
ホットスポットや、ホテルなど不特定多数のクライアントがアクセスするような環境では、「使用する」に設定することをお勧めします。
複合通信時は、プライバシーセパレータは使用できないのでご注意ください。



弊社製USB指紋認証ユニットまたはUSBメモリをアクセスポイントのUSBポートにセットして、このボタンをクリック

他社製無線LANクライアントのサポート

手動設定で通信を行う時に無線LANクライアントと本アクセスポイントとの802.11認証で通信設定を簡易的に行う場合に使用します。別売の弊社製USB指紋認証ユニット(LWN-BF16U)をアクセスポイントのUSBシリーズAポートにセットして「USBメモリに出力」ボタンをクリックしてください。USBメモリに通信に必要な情報(WEPキー、SSID等)が出力されます。出力された情報は弊社製USB指紋認証ユニット付属のソフトウェア「Logitec Connection Help」を使用して無線無線LANクライアントに受け渡されます。「Logitec Connection Help」の使用方法はUSB指紋認証ユニットのユーザーズマニュアルをご参照ください。



1.MACアドレスを入力
2. ユーザ権限を設定
3.「追加」ボタンをクリック

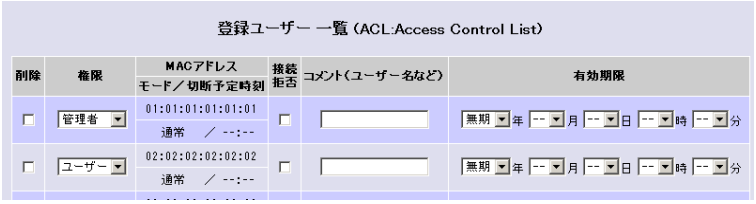
接続を許可するMACアドレスの追加

注：この設定は手動設定時のみ意味のある操作です。

事前にクライアントのMACアドレスがわかっていて、接続を許可しておく場合は、ここでMACアドレスを追加しておきます。追加方法は直接MACアドレスを入力する方法と、USBメモリにMACアドレスを登録しておきそこから追加する方法があります。直接入力する場合は、ユーザー権限を「管理者」または「ユーザ」から選択できます。「管理者」権限を持つユーザは、クライアントユーティリティを起動したときに「AP設定」ボタンが有効になります(弊社製無線LANカードおよびユーティリティを使用している場合のみ)。

設定を行ったら「追加」ボタンをクリックしてください。下の欄の「登録ユーザー一覧」に登録されます。

ただし、ここで接続を許可しても、SSID、暗号キーの設定は必ず行わなければなりません。



登録ユーザー一覧（ACL　Access Control List）

ここには、現在登録されているMACアドレスの一覧が表示されます。ここからは以下の設定が可能です。

・「削除」欄のチェックボックスにチェックを入れて「更新」ボタンを押すと、そのMACアドレスは一覧から削除され、通信ができなくなります。

・「権限」の欄ではそのMACアドレスを持つクライアントを「管理者」とするか、「ユーザー」とするかを決めることができます。権限を選択して、更新ボタンを押すとそのMACアドレスには新しい権限が与えられます。ただし、ここで変更しただけでは、すぐに設定が有効になりません。いったんクライアント側の無線LANカードをパソコンから取り外し、再度スマート認証を行ってください。アクセスポイントと無線LANカード間で新しい権限に必要な値を交換します。この後、無線LANカードをパソコンにセットしてはじめて設定が有効となります。

・「MACアドレス、モード/切断予定時刻」欄には登録されているMACアドレス、クライアントからの通信を許可する期間（通常・タイマー・自動切断）、切断予定時刻が表示されます。

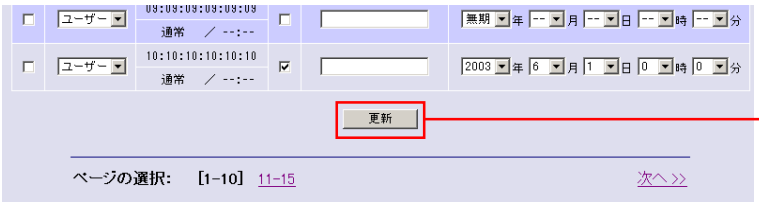
・「接続拒否」欄のチェックボックスにチェックを入れて「更新」ボタンをクリックすると、そのMACアドレスをもつ無線LANカードを使用しているクライアントは、本アクセスポイントとチェックを外すまで通信ができなくなります。

・「コメント」欄には、利用者名やカードの種類などをコメントとして登録しておくことをおすすめします。

・「有効期限」欄では、そのMACアドレスを持つ無線LANカードの電子証明書（スマート認証時に発行されるもの）の有効期限を設定することができます。（デフォルトでは無制限に設定されています）この画面で値を変えるとすぐにその期限に再設定されます。設定が変更されても再度スマート認証を行うは必要ありません。手動設定の場合はこの値を設定しても有効になりません。

Point　ポイント

本アクセスポイントでは、MACアドレスフィルタリングを補助的に使用しています。これを利用しなくても、LDLS認証を利用してセキュアな認証を実現しています。ただし、紛失したカードのMACアドレスの「有効期限」を過去の日付に設定しておくことは有効な手段です。



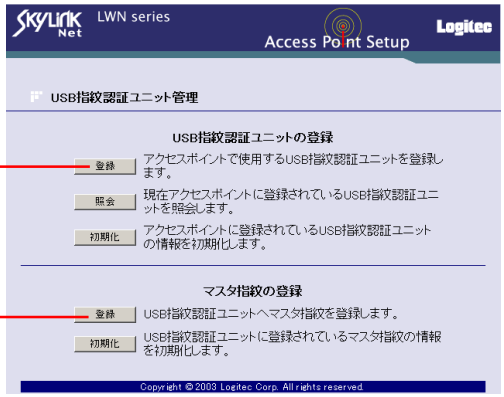
設定を変更した場合は、更新ボタンをクリックしてください。変更内容が反映されます。

USB 指紋認証ユニット管理

設定メニューから「USB 指紋認証ユニット管理」のサブメニューを選ぶと以下の画面が表示されます。ここでは、指紋認証（BIO）モードでネットワークの管理を行う際に使用する弊社製USB指紋認証ユニット（LWN-BF16U:別売）の登録 / 初期化、管理者（マスタ）の指紋データの登録 / 初期化を行います。ここでの設定を行う前に、必ずクライアントパソコン側にUSB指紋認証ユニットのユーティリティをインストールしておいてください。ユーティリティのインストール方法につきましては、USB指紋認証ユニットのユーザーズマニュアルをご参照ください。

はじめに USB 指紋認証ユニットの登録を行います。

次にマスタ指紋の登録を行います。



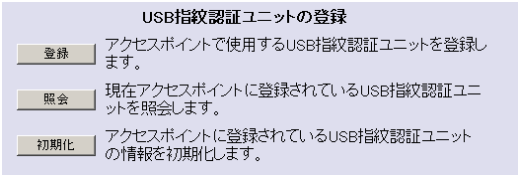
Point ポイント

マスタとして登録されたユーザーは、指紋認証によるスマート認証許可権限を持つ子ユーザーを以下の 2 つの方法で作ることができます。

・同じ USB 指紋認証ユニット内に子ユーザーを作成する（集中管理）

・別の USB 指紋認証ユニットを子ユーザーとして登録する（分散管理）

詳しくは USB 指紋認証ユニットのユーザーズマニュアルをご参照ください。

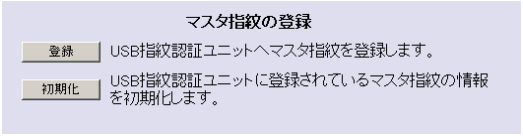


USB 指紋認証ユニットの登録

・新しくUSB指紋認証ユニットを登録する場合は、登録するUSB指紋認証ユニットを本アクセスポイントのUSBシリーズAポートに接続し、「登録」ボタンをクリックします。（本設定画面から登録するのはマスタとなる「親指紋認証ユニット」1台のみです。子ユーザーとなる「子指紋認証ユニット」の作成・登録は、パソコン上で行います。詳しくはUSB指紋認証ユニットのユーザーズマニュアルをご参照ください。）

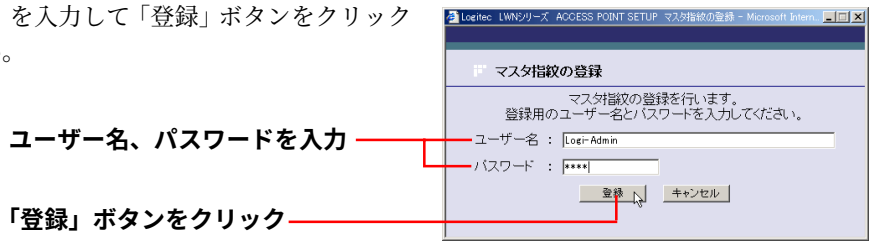
・USB 指紋認証ユニットが本アクセスポイントに接続されているとき「照会」ボタンをクリックすると、接続されている指紋認証ユニットが「親指紋認証ユニット」か「子指紋認証ユニット」かが確認できます。また、この確認はUSB 指紋認証ユニットのユーティリティからも確認できます（詳しくは USB 指紋認証ユニットのユーザーズマニュアルをご参照ください）。

・「初期化」ボタンをクリックすると、アクセスポイントに登録されているUSB指紋認証ユニットの情報を初期化します。



マスタ指紋の登録

・USB 指紋認証ユニットの登録が済んだらマスタ指紋の登録を行います。アクセスポイントに USB 指紋認証ユニットが接続されている状態で、「登録」ボタンをクリックしてください。右の画面が表示されますので、任意の「ユーザー名」「パスワード」を入力して「登録」ボタンをクリックしてください。

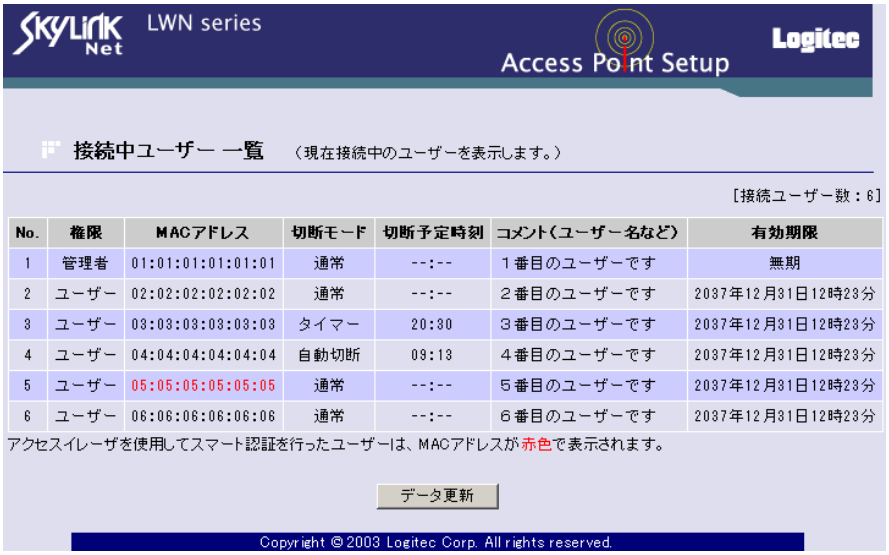


USB 指紋認証ユニットに登録する指を乗せるようメッセージが表示されます。この後は、画面の指示に従ってマスタ指紋の登録を行ってください。

・「初期化」ボタンをクリックすると、登録されているマスタ指紋のデータを初期化することができます。初期化を行うと、もとのデータは失われます。

接続中ユーザー一覧

設定メニューから「接続中ユーザー一覧」のサブメニューを選ぶと以下の画面が表示されます。ここでは、現在アクセスポイントと通信を行っているユーザーの一覧が表示されます。「データ更新」ボタンを押すと、最新の状態に更新されます。



Point ポイント

- **表示されている内容は「ユーザー管理」の「登録ユーザー一覧」で変更可能です。**
- **MACアドレスが赤色で表示されているものは、アクセスイレーザを使用して認証を行っているユーザーです。**

情報照会

「情報照会」メニューは「機器情報」と「システムログ」の２つのサブメニューに分かれています。

・「機器情報」では、アクセスポイントの名前、MACアドレス、ハードウェア/ソフトウェアのバージョン、送受信パケット情報が参照できます。

・「システムログ」からは、アクセスポイントのアクセスログおよびエラーログを参照できます。

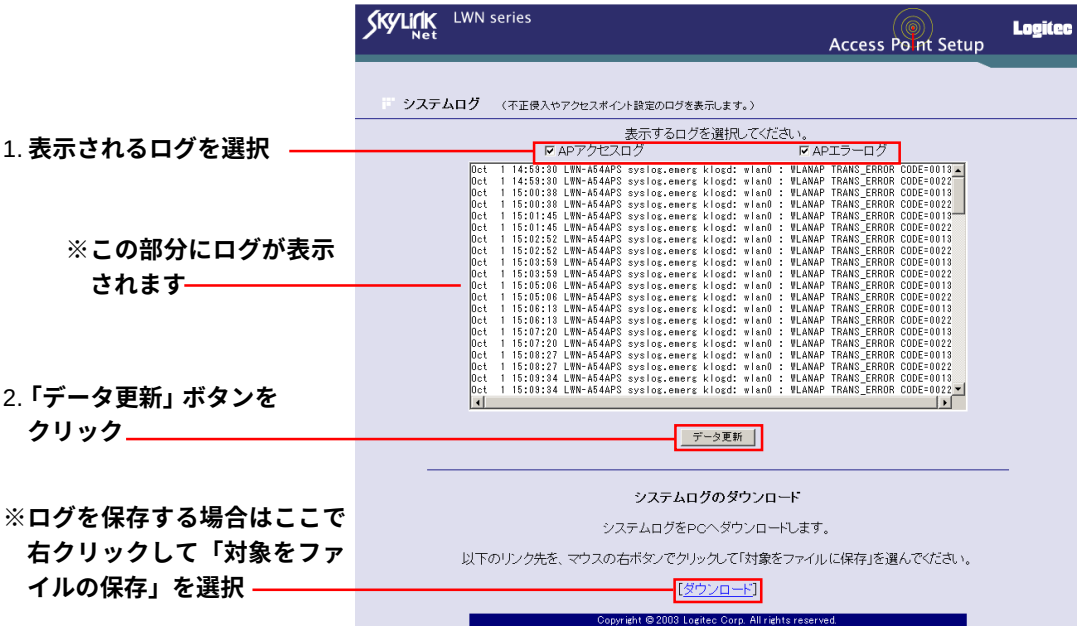
機器情報

設定メニューから「機器情報」のサブメニューを選ぶと以下の画面が表示されます。

データ更新ボタンを押すと、最新の情報に更新されます。

システムログ

設定メニューから「システムログ」のサブメニューを選ぶと以下の画面が表示されます。



システムログは「基本設定」メニューの「システムログの設定」でログを記録するように設定されていなければ表示されません。

・「AP アクセスログ」を選択して「データ更新」ボタンをクリックすると、不正アクセスなどの履歴が表示されます。ここでは以下のような場合にログが記録されます。
  ・スマート認証モード通信時または手動設定でMACアドレスフィルタリングを使用した通信時に、登録ユーザー一覧の欄に登録されていないユーザーからアクセスポイントへのアクセスが試みられた時。
  ・LDLS 認証時に、チャレンジテキストのデコードまたはエンコードを失敗した時。
  プライバシーセパレータを使用している時に、同一無線ネットワーク内でクライアント間通信を検出した場合。

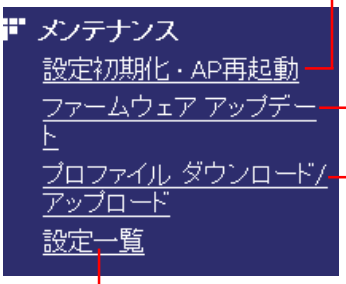
・「AP エラーログ」をして「データ更新」ボタンをクリックすると、システムエラーなどの履歴が表示されます。ここではアクセスポイントのドライバが動作中に通信障害と認識される状態を検知した場合にログが記録されます。

※表示されるログの内容につきましては、「付録：ログ一覧」をご参照ください。

・基本的にアクセスポイントの電源を切ると全てのシステムログは削除されます。(アクセスポイント側面のリセットスイッチを押し、ソフトウェアリセット後に再起動した場合はログは残ります。) ログを保存しておきたい場合は、画面下の［ダウンロード］にマウスポインタを当て、右クリックして表示されるメニューから「対象をファイルに保存」を選択します。

メンテナンス

「メンテナンス」メニューは「設定初期化・AP 再起動」と「ファームウェア アップデート」「プロファイルダウンロード / アップロード」「設定一覧」の４つのサブメニューに分かれています。



・「設定初期化・AP 再起動」では、アクセスポイントの初期化または、再起動を行うことができます。

・「ファームウェアアップデート」では、本アクセスポイントの最新のファームが公開された際にファイルをアップデートすることができます。(アクセスポイントのファームをアップデートするときに、クライアントユーティリティも同時にアップデートする必要がある場合もあります。あらかじめご了承ください。) 最新の情報につきましては弊社ホームページをご参照ください。

・「プロファイル ダウンロード / アップロード」では、アクセスポイントの設定情報を設定用のパソコンにダウンロードすることと、ダウンロードした情報を元のアクセスポイントや、同じ機種（LWN-A54APS）のアクセスポイントにアップロードすることができます。本製品設定後、直ちにこの機能を使用してプロファイルとアクセスコントロールリスト（ACL）をお手元のパソコンに保存しておくことをお勧めします。万一、故障などでアクセスポイントを交換した時に、保存したファイルをアップロードすれば、設定時の状態に戻すことができます。

・「設定一覧」では、現在アクセスポイントに設定されている内容が一覧で確認することができます。

設定初期化・AP 再起動

設定メニューから「設定初期化・AP 再起動」のサブメニューを選ぶと以下の画面が表示されます。

・「初期化実行」ボタンをクリックすると、それまでに行っていた設定内容を全て破棄してアクセスポイントの設定を任意の初期設定値に戻します。実行後、その他の設定を再度行うためには、いったん表示されている設定画面を終了し、再度ログインしなおす必要があります。実行する前に、「プロファイル ダウンロード / アップロード」で全情報をいったんダウンロードしておくことをお勧めします。

・「再起動実行」ボタンをクリックすると、アクセスポイントを再起動します。このボタンで再起動した場合もログは消去されます。

※アクセスポイントにUSB機器を接続した状態で再起動を実行しないでください。

ポイント

初期化を行うと、アクセスポイントは、スマート認証モードのシングルチャネルモードとなります。また、AP 側で管理しているユーザー情報は消去されるので、複数のカードに管理者権限があった場合は、再認証時に一番初めにスマート認証を行ったユーザー以外は管理者権限を失います。再度複数のクライアントに管理者権限をもたせる場合は、再設定が必要です。

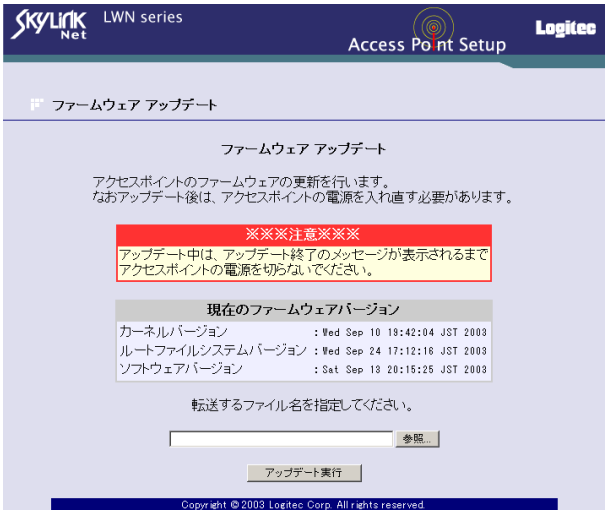
ファームウェア アップデート

ご注意

本アクセスポイントの最新ファームが公開された際は、このメニューからアームウェアのアップデートを行うことができます。アップデートを行う前に、アップデートファイルと共に提供される“Readme.txt”ファイルをよくお読みください。
最新の情報については弊社ホームページをご参照ください。

ロジテック株式会社ホームページアドレス： http://www.logitec.co.jp/

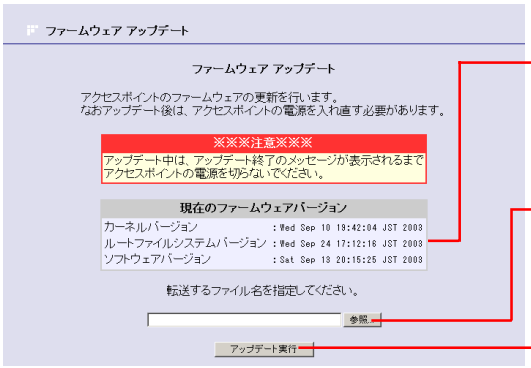
設定メニューから「ファームウェア アップデート」のサブメニューを選ぶと以下の画面が表示されます。アップデート手順については次ページをご参照ください。



重要！

- **参照するアップデートファイルは、ドライブレター、ディレクトリ名、ファイル名の合計が255バイトを超えない場所に保存して置いてください。ディレクトリ名には日本語が使用できますが、ファイル名は半角英数字をご使用ください。**
- **アップデート時は、2つ以上のファイルを同時に連続してアップデートしなければいけない場合があります。（例　ルートファイルシステム+MTDファイルシステム）その場合は、途中で再起動を行わず、全てのファイルをアップロードしてから再起動してください。また、再起動を行う際は、ユーザーはアクセスポイントと通信を行わないようにしてください。**
- **ファームウェアアップデート終了のメッセージが表示されるまで絶対にアクセスポイントの電源を切らないようにしてください。**
- **アクセスポイントのファームウェアをアップデートすると、クライアントユーティリティもアップデートする必要がある場合もあります。詳細はファームウェア公開時にご案内いたしますので、よく語確認ください**

■アップデート手順

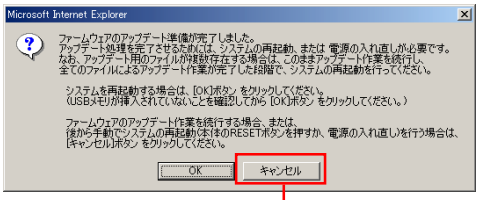


①「参照」ボタンをクリックしてアップデートするファイルを指定してください。

②「アップデート実行」ボタンをクリックしてください。

③右の画面が表示されます。「OK」ボタンをクリックしてください。アップデートが実行されます。

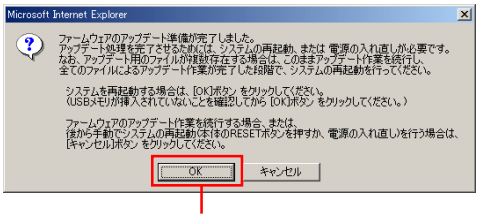
④アップデートが完了すると右の画面が表示されます。複数のファイルをアップデートする場合はキャンセルボタンをクリックしてください。
※アップデートファイルが１つしかない場合は、ここで OK ボタンをクリックします。



⑤アップデートするファイル数に応じて、手順①から③の操作を繰り返します。

⑥一番最後のファイルのアップデートが完了し、右の画面が表示されたら「OK」ボタンをクリックしてください。

以上でアップデートは完了です。



ご注意

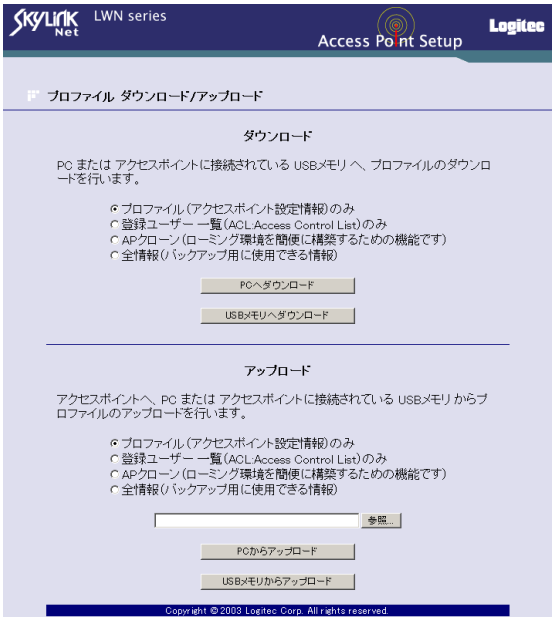
再起動を後で手動で行う場合は、必ず以下のいずれかの方法で行ってください。

・アクセスポイントを設定メニューの「AP 動作停止」を行い、その後に電源を切り、５秒以上たってから起動する。
・設定メニューを終了し、アクセスポイント側面のリセットスイッチを押す。

メンテナンスメニューにある「AP 再起動」は行わないようにしてください。

プロファイル ダウンロード / アップロード

設定メニューから「プロファイル ダウンロード / アップロード」のサブメニューを選ぶと以下の画面が表示されます。ここでは、アクセスポイントの設定情報をパソコンにダウンロードすることと、ダウンロードしておいたファイルをアクセスポイントにアップロードすることができます。



プロファイルダウンロード / アップロードは以下の２点の機能を実行するためにあります。

バックアップ用途として使用

○設定をパソコンにダウンロードしておき必要なときにその設定をアップロードすれば、いつでもダウンロード時の設定でアクセスポイントを復元することができます。この場合は「全情報」をダウンロードしておいてください。

ローミング機能使用のために使用

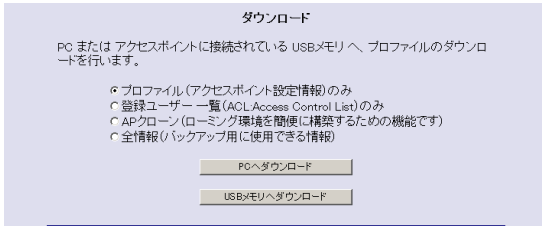
○ここで、特定のアクセスポイント（AP1とします）の設定をダウンロードして、その設定を他のアクセスポイント（AP2とします）にアップロードすることにより複数のアクセスポイント間で同じ通信情報が共有できるようになります。そのためクランアントはAP1の通信可能範囲からAP2の通信可能範囲へ移動した場合も同じ設定で通信を継続することができるようになります。（ローミング機能）

※ AP2 へ AP1 の情報をアップロードするためには、AP1 の設定メニューから「AP クローン」のダウンロードを行い、そのファイルを AP2 の設定メニューからアップロードしてください。

※ダウンロードおよびアップロード内容の詳細および､ローミング設定の手順は次ページ以降をご参照ください。

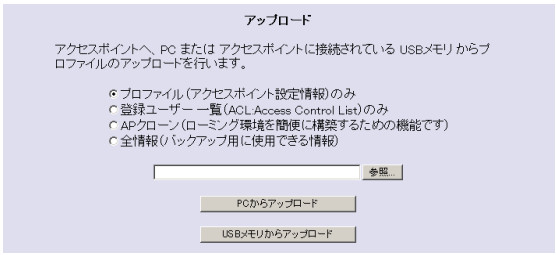
ご注意

「AP クローン」または「全情報」をダウンロードした場合、パスワードの情報も暗号化されてダウンロードされます。この設定でダウンロードしたファイルをアップロードするとダウンロードされた時点で使用していたパスワードが必要になりますので、特にパスワードを変更した場合など、十分にご注意ください。パスワードがわからなくなった場合は、弊社といたしましても、工場出荷時に戻す以外のサポートはいたしかねますのでご注意ください。



ダウンロード欄

ダウンロードする設定情報の種類を、「プロファイル」「登録ユーザー一覧」「APクローン」「全情報」の中からから選択し、プロファイルを保存する先に応じて「PCへダウンロード」「USBメモリへダウンロード」どちらかのボタンをクリックしてください。「USBメモリへダウンロード」を選択する場合、アクセスポイントに弊社製USB指紋認証ユニット（LWN-BF16U）をセットしておいてください。選択した情報が、指定した先にダウンロードされます。



アップロード欄

アップロードする設定情報の種類を、「プロファイル」「登録ユーザー一覧」「APクローン」「全情報」の中からから選択し、「参照」ボタンからアップロードするファイルを指定して、「PCからアップロード」ボタンをクリックするか、アクセスポイントに弊社製USB指紋認証ユニット（LWN-BF16U）をセットして、参照横のテキストボックスにファイル名を入力し、「USBメモリからアップロード」ボタンをクリックします。選択した情報がアクセスポイントへアップロードされます。

プロファイル（アクセスポイント設定情報のみ）

プロファイルを選択した場合はアクセスポイントの設定情報（アクセスポイントのIPアドレス、アクセスポイントが使用する暗号キーもしくは事前共有キーの情報）のみをダウンロードまたはアップロードします。ユーザーの管理情報などは含まれません。

登録ユーザー一覧

登録ユーザー一覧を選択した場合は、ユーザーの管理情報（ユーザーが使用している暗号キー、MACアドレス、ユーザー権限、電子証明書の有効期限など）のみをダウンロードまたはアップロードします。アクセスポイントの設定情報などは含まれません。

APクローン

APクローンを選択した場合はIPアドレスを除くアクセスポイントの設定情報全て（パスワード情報も含みます）がダウンロードまたはアップロードされます。ローミング機能を使用する場合は、この設定を選択してください。

全情報

全情報を選択するとアクセスポイントの設定情報を全て（パスワード情報も含みます）アップロードします。設定情報のバックアップにご使用ください。IPアドレス情報も含まれるため、ローミング用には使用できません。

※パスワード情報も含まれますので、アップロードを行うとダウンロードした時点のパスワードに戻ります。ご注意ください。

ローミング機能設定の手順

○アクセスポイントのローミング機能を使用したい場合は、以下の手順をご参照ください。

1.ローミングさせたいユーザを全て、スマート認証を使用してアクセスポイントに登録させます。登録情報は ACL（Access Control List）としてアクセスポイント内部に作成されます。登録可能ユーザ数は最大 256 ユーザとなります。

2. ダウンロード欄で「AP クローン」を選択して、保存先に応じて「PC へダウンロード」または「USB メモリへダウンロード」ボタンをクリックし、設定ファイルを保存してください。

3.ローミングを行いたいアクセスポイントの設定画面へアクセスして、「プロファイル ダウンロード / アップロード」画面を表示させ、アップロード欄で「AP クローン」を選択して、「参照」ボタンでアップロードするファイルを指定して、ファイルの場所に応じて「PCからアップロード」または「USB メモリからアップロード」ボタンをクリックして、ファイルをアップロードしてください。

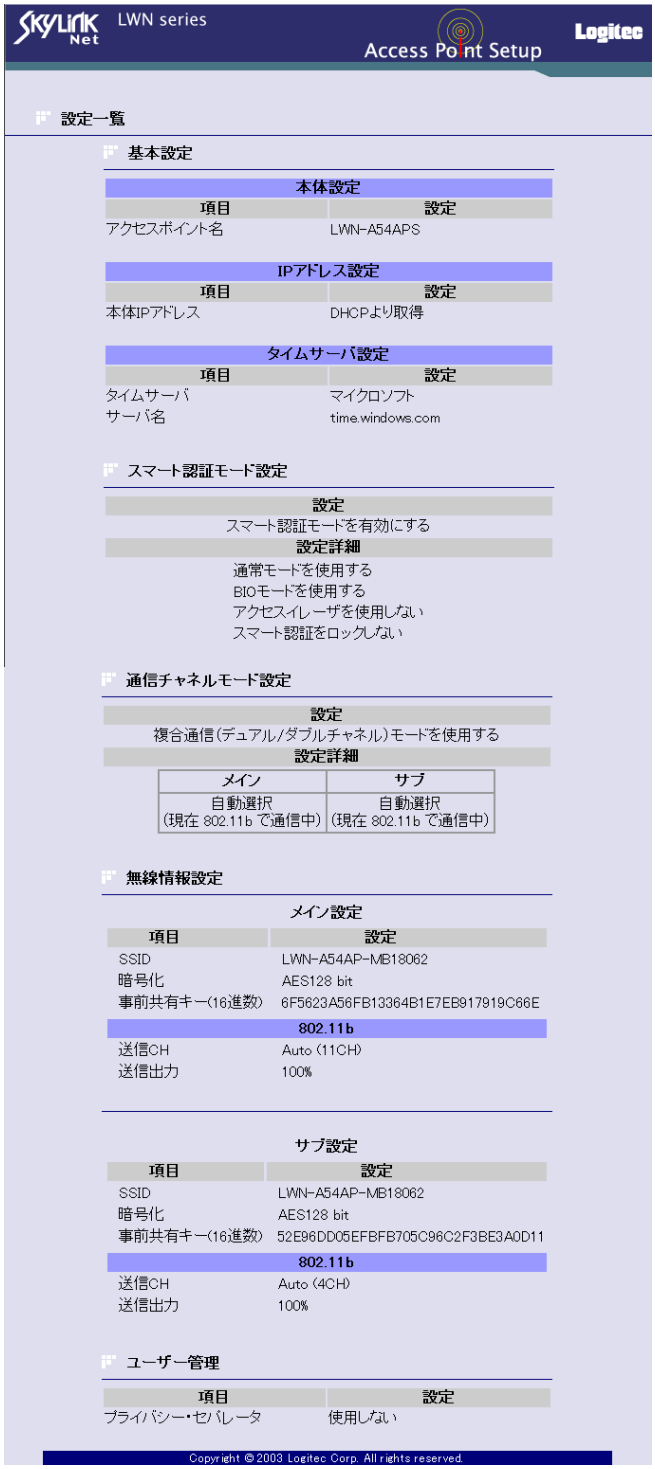
4. 必要なアクセスポイントの数だけこの手順を繰り返します。

Point ポイント

- **ローミングを行うアクセスポイントを管理するクライアントパソコンが異なる場合は、USB メモリにファイルをダウンロードしておき、ローミングを行うアクセスポイントに USB メモリをセットしてファイルをアップロードします。**
- **付属の無線 LAN カードにはプロファイルを自動的に選択して通信するアクセスポイントを切り替えるクライアントローミング機能を使用することもできます。この機能の設定方法については、CD-ROM に収められている「無線 LAN カードユーティリティガイド」（PDF）をご参照ください。**

設定一覧

設定メニューから「設定一覧」のサブメニューを選ぶと以下の画面が表示されます。ここでは現在のアクセスポイントの設定が一覧で確認できます。



付録：ログ一覧

■ AP アクセスログ

理由	ログに含まれる文字列
DLS==ON、あるいはMACフィルター==ON時、ACL未登録STAからのAuthフレーム（seq１・２）or Managementフレーム（ProbeRequest・Response、Beaconは除く）、Controlフレーム受信で出力される。	WLANAP REJECT MAC xx:xx:xx:xx:xx:xx
DLS==ON、あるいはMACフィルター==ON時、ACL登録STA（DENY bit ON）からのAuthフレーム（seq１・２）or Managementフレーム（ProbeRequest・Response、Beaconは除く）、Controlフレーム受信で出力される。	WLANAP REJECT MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq１）を受信し、CharengeTxtのRSAデコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq１）を受信し、CharengeTxtのRSAデコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
DLS==ON時、CharengeTxtから取得した証明書（Subject）のユーザータイプが不正である場合、出力される。	WLANAP AUTH-FAIL MAC xx:xx:xx:xx:xx:xx
DLS==ON時、CharengeTxtから取得した証明書（Subject）の発行番号が不正である場合、出力される。	WLANAP AUTH-FAIL MAC xx:xx:xx:xx:xx:xx
DLS==ON時、CharengeTxtから取得した証明書（Subject）の所属MACアドレスが不正である場合、出力される。	WLANAP AUTH-FAIL MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq２）作成のために、CharengeTxtのRSAエンコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq２）作成のために、CharengeTxtのRSAエンコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq３）を受信し、CharengeTxtのRSAデコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
DLS==ON時、Authフレーム（seq３）を受信し、CharengeTxtのRSAデコードに失敗した場合、出力される。	WLANAP AUTH-ERROR MAC xx:xx:xx:xx:xx:xx
プライバシーセパレータ==ON時、クライアント間通信パケットを受信した場合、出力される。	WLANAP PRIVACY MAC xx:xx:xx:xx:xx:xx
不正フォーマットフレームを受信した場合、出力される。	APSRCH FORMAT-ERROR MAC xx:xx:xx:xx:xx:xx

■ AP エラーログ

文字列末尾の %n は実際には表示されません。

理由	ログに含まれる文字列
パワーモード設定に失敗した場合に出力される。	WLANAP INIT_ERROR CODE=0052\n
Key Tableへの登録失敗時に出力される。	WLANAP INIT_ERROR CODE=0021\n
AES鍵の拡張失敗時に出力される。	WLANAP INIT_ERROR CODE=0022\n
AESパラメータの生成失敗時に出力される。	WLANAP INIT_ERROR CODE=0023\n
AES CCMの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0024\n
SIBテーブルの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0001\n
SIB登録メモリ（APのSIBエリア）の取得失敗時に出力される。	WLANAP INIT_ERROR CODE=0002\n
規定外レートの指定時に出力される。	WLANAP INIT_ERROR CODE=0003\n
SIBテーブルへのエントリ登録失敗時に出力される。	WLANAP INIT_ERROR CODE=0004\n
IEEE 802.11のための初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0005\n
Chanel設定失敗時に出力される。	WLANAP INIT_ERROR CODE=0006\n
Beaconの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0007\n
カーネルによるデバイス情報の登録失敗時に出力される。	WLANAP INIT_ERROR CODE=0014\n
動的メモリ取得の失敗時に出力される。	WLANAP INIT_ERROR CODE=0017\n
SKB（カーネル・モジュール間 I/Fメモリ）の取得失敗時に出力される。	WLANAP INIT_ERROR CODE=0015\n
Beaconの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0009\n
Beaconの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0018\n
カーネルによるIRQ割り当て失敗時に出力される。	WLANAP INIT_ERROR CODE=0010\n
カーネルによるIRQ割り当て失敗時に出力される。	WLANAP INIT_ERROR CODE=0019\n
Beaconの初期化失敗時に出力される。	WLANAP INIT_ERROR CODE=0008\n
動的メモリ取得の失敗時に出力される。	WLANAP INIT_ERROR CODE=0025\n
動的メモリ取得の失敗時に出力される。	WLANAP INIT_ERROR CODE=0026\n
MACレジスタバージョン不正時に出力される。	WLANAP INIT_ERROR CODE=0027\n
PHY or MACレジスタのRead失敗時に出力される。	WLANAP INIT_ERROR CODE=0028\n
PHY or MACレジスタのRead失敗時に出力される。	WLANAP INIT_ERROR CODE=0029\n
5G Radio Chipバージョン不正時に出力される。	WLANAP INIT_ERROR CODE=0030\n
動的メモリ取得の失敗時に出力される。	WLANAP INIT_ERROR CODE=0031\n
2.4G Radio Chipバージョン不正時に出力される。	WLANAP INIT_ERROR CODE=0032\n
EEPROMバージョン or ROMサイズ不正時に出力される。	WLANAP INIT_ERROR CODE=0033\n
EEPROMチェックサムエラー時に出力される。	WLANAP INIT_ERROR CODE=0034\n
EEPROM Readエラー時に出力される。	WLANAP INIT_ERROR CODE=0035\n
EEPROM Readエラー時に出力される。	WLANAP INIT_ERROR CODE=0040\n
EEPROM Readエラー時に出力される。	WLANAP INIT_ERROR CODE=0041\n
EEPROM Modeエラー時に出力される。	WLANAP INIT_ERROR CODE=0042\n
EEPROM Modeエラー時に出力される。	WLANAP INIT_ERROR CODE=0043\n
不正Mode指定時に出力される（パワーモード設定時）。	WLANAP INIT_ERROR CODE=0051\n
不正Channel指定時に出力される（Chip Reset時）。	WLANAP INIT_ERROR CODE=0044\n
ノイズフローが規定値以上である場合に出力される。	WLANAP INIT_ERROR CODE=0045\n
不正Channel値を設定しようとした場合に出力される。	WLANAP INIT_ERROR CODE=0046\n
不正Channel値を設定しようとした場合に出力される。	WLANAP INIT_ERROR CODE=0047\n
ノイズフロー検出がタイムアウトした場合に出力される。	WLANAP INIT_ERROR CODE=0048\n
ノイズフローが規定値以上である場合に出力される。	WLANAP INIT_ERROR CODE=0049\n
一定時間、ノイズフローが規定値以上であった場合に出力される。	WLANAP INIT_ERROR CODE=0050\n
Chip Reset失敗時に出力される。	WLANAP TRANS_ERROR CODE=0007\n
Chip Reset失敗時に出力される。	WLANAP TRANS_ERROR CODE=0001\n
送信フレーム生成処理の失敗時に出力される。	WLANAP TRANS_ERROR CODE=0002\n
フレーム送信処理の失敗時に出力される。	WLANAP TRANS_ERROR CODE=0003\n
不正フレームタイプのフレーム送信時に出力される。	WLANAP TRANS_ERROR CODE=0004\n
フレーム送信処理の失敗時に出力される。	WLANAP TRANS_ERROR CODE=0005\n
DMA転送用メモリの取得失敗時に出力される。	WLANAP TRANS_ERROR CODE=0006\n
NULLデータフレームの生成失敗時に出力される。	WLANAP TRANS_ERROR CODE=0008\n
前回送信のDescriptorが無い、あるいは送信完了していない場合に出力される。	WLANAP TRANS_ERROR CODE=0009\n
キャッシュINDEXが不正値である場合に出力される。	WLANAP TRANS_ERROR CODE=0010\n
送信Descriptorが無い、あるいはHWリセット中である場合に出力される。	WLANAP TRANS_ERROR CODE=0011\n
指定MACアドレスがSIB未登録である場合に出力される。	WLANAP TRANS_ERROR CODE=0012\n
指定MACアドレスがACL未登録である場合に出力される。	WLANAP TRANS_ERROR CODE=0013\n
指定MACアドレスがSIB未登録であるが、フレームがDisAssoc or DeAuthである場合に出力される。	WLANAP TRANS_ERROR CODE=0014\n

■ AP エラーログ（続き）

文字列末尾の %n は実際には表示されません。

理由	ログに含まれる文字列
デバイスがダウンしている時にカーネルから送信要求があった場合に出力される。	WLANAP TRANS_ERROR CODE=0015\n
IEEE 802.3からIEEE 802.11へのコンバータエラーがあった場合に出力される。	WLANAP TRANS_ERROR CODE=0016\n
IEEE 802.11からIEEE 802.3へのコンバータエラーがあった場合に出力される。	WLANAP TRANS_ERROR CODE=0017\n
IEEE 802.3からIEEE 802.11へのコンバータエラーがあった場合に出力される。	WLANAP TRANS_ERROR CODE=0018\n
IEEE 802.11からIEEE 802.3へのコンバータエラーがあった場合に出力される。	WLANAP TRANS_ERROR CODE=0019\n
カーネルへの受信データ通知が失敗した場合に出力される。	WLANAP TRANS_ERROR CODE=0020\n
IEEE 802.3からIEEE 802.11へのコンバータエラーがあった場合に出力される。	WLANAP TRANS_ERROR CODE=0021\n
受信フレームの送信元STAがSIB未登録であった場合に出力される。	WLANAP TRANS_ERROR CODE=0022\n
不正フレームタイプのフレーム受信時に出力される。	WLANAP TRANS_ERROR CODE=0023\n
不正フレーム受信時に出力される。	WLANAP TRANS_ERROR CODE=0024\n
不正鍵タイプ（WEP、AES以外）が指定された場合に出力される。	WLANAP TRANS_ERROR CODE=0025\n
Descriptorエリアの取得失敗時に出力される。	WLANAP TRANS_ERROR CODE=0026\n
理由不明な送信失敗が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0027\n
割込事由が不明な割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0028\n
デバイスのHWリセット中に割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0029\n
rxORN割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0030\n
FATAL割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0031\n
rxEOL割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0032\n
txURN割込が規定回数発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0033\n
割込事由が不明な割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0034\n
デバイスのHWリセット中に割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0035\n
FATAL割込が発生した場合に出力される。	WLANAP TRANS_ERROR CODE=0036\n
Descriptorエリアの取得失敗時に出力される。	WLANAP TRANS_ERROR CODE=0037\n
受信フレームのデコード後データサイズが規定値を超えている場合に出力される。	WLANAP TRANS_ERROR CODE=0038\n
不正Key Cache INDEXが指定された場合に出力される。	WLANAP TRANS_ERROR CODE=0043\n
不正Key Cache INDEXが指定された場合に出力される。	WLANAP TRANS_ERROR CODE=0044\n
指定INDEXの示すKey Cache管理情報が未登録であった場合に出力される。	WLANAP TRANS_ERROR CODE=0045\n
UCSEの設定が不正値であった場合に出力される。	WLANAP TRANS_ERROR CODE=0046\n
AES鍵の拡張失敗時に出力される。	WLANAP TRANS_ERROR CODE=0047\n
AESパラメータの生成失敗時に出力される。	WLANAP TRANS_ERROR CODE=0048\n
AES CCMの初期化失敗時に出力される。	WLANAP TRANS_ERROR CODE=0049\n
AES鍵サイズが不正である場合に出力される（40bit or 104bit）。	WLANAP TRANS_ERROR CODE=0050\n
LDLSモードで受信フレームの証明書Subjectsのユーザータイプが不正である場合に出力される。	WLANAP TRANS_ERROR CODE=0051\n
LDLSモードで受信フレームの証明書Subjectsの証明書発行番号が不正である場合に出力される。	WLANAP TRANS_ERROR CODE=0070\n
DHペア鍵生成の失敗時に出力される。	WLANAP TRANS_ERROR CODE=0052\n
出力条件	出力文字列
デバイスがダウンしている時にAssociationフレームを受信した場合に出力される。	WLANAP TRANS_ERROR CODE=0053\n
Associationフレームの送信先SSIDが不正であった場合に出力される。	WLANAP TRANS_ERROR CODE=0054\n
Association Responseフレームの送信失敗時に出力される。	WLANAP TRANS_ERROR CODE=0055\n
Managementフレームであるにも関わらず、Authフレームでない場合に出力される。	WLANAP TRANS_ERROR CODE=0056\n
不正Authフレームシーケンスである場合に出力される。	WLANAP TRANS_ERROR CODE=0057\n
不正フレームサブタイプのフレーム受信時に出力される。	WLANAP TRANS_ERROR CODE=0058\n

著作権等について

○本書の著作権は、ロジテック株式会社に帰属します。本書の一部または全部を弊社に無断で転載することは禁止されております。

○本書の内容につきましては万全を期しておりますが、万一ご不審の点がございましたら、弊社テクニカルサポートまでご連絡願います。

- **本製品は**OpenSSL Toolkit**を使用するために**OpenSSL Project**により開発されたソフトウェアを含みます。（**http://www.openssl.org/**）**
- **本製品は** Eric Young（eay@crypsoft.com）**によって書かれた暗号ソフトウェアを含んでいます。**
- **本製品は** Apcache Software Foundation（http://www.apache.org/）**により開発されたソフトウェアを含みます。**

OpenSSL License

/ * Copyright (c) 1998-2000 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Apache License