Wi-Fi CERTIFIED Wi-Fi Protected Setup™:

一般住宅／小規模オフィスの Wi-Fi®ネットワーク ユーザー体験を大幅に向上

Wi-Fi Alliance®

初版発行：2010 年 12 月

更新：2020 年 12 月

本ドキュメントならびに本ドキュメントに記載されている Wi-Fi Alliance プログラムおよびリリース予定日に関する情報は、予告なく変更または取り消される場合があります。本ドキュメントは入手した情報に伴う誤りも含め（”WITH ALL FAULTS”）、作成時現在に利用可能な情報に基づいて（”AS AVAILABLE”）、作成時現在の状態のまま（ “AS IS”）で提供されています。本ホワイトペーパーならびに記載されている情報の利便性、品質、適宜性、真実性、正確性、完全性について、WI-FI ALLIANCE はいかなる主張、認証、条件提示、保証もしません。

概要

一般住宅や小規模オフィス ネットワークを利用しているユーザーには、最高レベルのセキュリティに加え、テクニカル サポートなどに頼ることなく、オンライン接続している設備や機器への追加や変更を簡単に行える環境が必要です。Wi-Fi CERTIFIED Wi-Fi Protected Setup™ によって、ユーザーは現時点で最高レベルのセキュリティに保護された環境で小規模 Wi-Fi®ネットワークを簡単・手軽に設定できます。設定プロセスはシンプルで、ボタンを押すだけでほぼすべてが自動的に行われます。

このように Wi-Fi Protected Setup™ は、SOHO (ホーム オフィス、スモール オフィス) 環境のネットワークのセットアップと構成設定を実現する、業界全体を通じたメカニズムを提供します。例えば従来の Wi-Fi 構成設定やセキュリティ設定に対する知識がほとんどない一般ユーザーでも、Wi-Fi Protected Setup によって新しい無線ネットワークを簡単に設定し、新しいデバイスをネットワークへ加えたりセキュリティを有効化したりすることができます。Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup 認定製品は、2007 年から市場に出回っています。

Wi-Fi Alliance®は、利用環境の質を高めると共に使用中のデバイスへ適用できる最高レベルのセキュリティ保護を実現する新機能によって、Wi-Fi Protected Setup プログラムを強化しました。

膨大な数の Wi-Fi 対応デバイスが市場に出回るようになった今日、Wi-Fi Protected Setup による手軽な使いやすさはすべてのユーザーが求める機能です。

Wi-Fi Protected Setup とは

Wi-Fi Protected Setup によって、購入した Wi-Fi デバイスのセキュリティ機能を Wi-Fi ネットワーク上で簡単に設定できると共に、新しい Wi-Fi Protected Setup デバイスを既存のネットワークへ非常に簡単に接続できるということをユーザーに保証することができます。

Wi-Fi Protected Setup は、家電や電話、またコンピュータ、アクセス ポイントなどを含む Wi-Fi CERTIFIED 802.11 製品のサポートを目的に規定された認定プログラムで、802.11a/b/g/n/ac を通じて通信するデバイスやマルチバンド デバイス、Wi-Fi Direct® 機能をサポートしているデイバスを含め、一般住宅および小規模オフィス向けの 802.11 デバイスを対象としています。2007 年 1 月に最初の Wi-Fi Protected Setup 製品が認定されましたが、それ以降、セキュリティ機能をさらに使いやすくするためのセットアップおよび設定の新機能が実装されています。

Wi-Fi Protected Setup は任意の認定プログラムで、特に SOHO 市場を念頭に考えられている Wi-Fi Protected Setup は、個別のネットワーク サーバーを展開してネットワーク アクセスの制御と暗号化の統制を行っているような大規模企業環境での利用をターゲットにしたものではありません。消費者は購入時、デバイスに Wi-Fi Protected Setup を示すマークがあることを確認してから購入できます。

Wi-Fi Protected Setup は、アクセス ポイント (AP) やルーターを使用したり、Wi-Fi Direct を通じて Wi-Fi CERTIFIED 製品間の直接接続が行われたりする一般的なホーム ネットワークに使われ、ネットワーク上のアクセス ポイントおよび Wi-Fi Protected Setup クライアント デバイスのネットワーク名（SSID）と Wi-Fi Protected Access® 2（WPA2™）、AP と Wi-Fi Protected Setup クライアント デバイスのセキュリティ キーを設定します。

© 2020 Wi-Fi Alliance. All rights reserved.

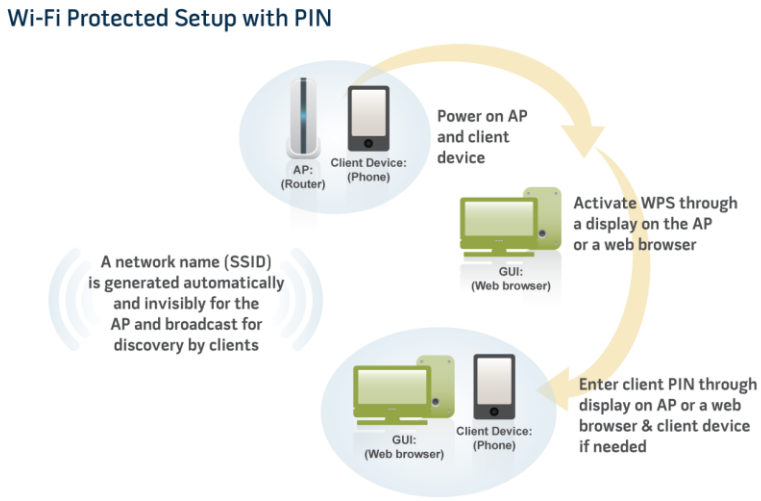
シンプルで標準化された Wi-Fi Protected Setup のアプローチによって、技術的背景やプロセスなどの知識を持っていない一般的な Wi-Fi ユーザーでさえも、セキュリティを有効化しながら Wi-Fi ネットワークを設定、拡張することが可能になります。例えば、SSID がネットワーク名を表していることや WPA2-Personal がセキュリティのメカニズムを表していることなどをユーザーが知る必要はありません。Wi-Fi Protected Setup によって、ネットワーク上のデバイスが利用できる最高レベルのセキュリティが自動的に適用されるので、ユーザーは数あるセキュリティ オプションの中から選択したりする手間がなくなります。

シンプルなセットアップ オプション

Wi-Fi Protected Setup 製品は、PIN（暗証番号）入力およびプッシュボタンの 2 つの簡単なセットアップ ソリューションをサポートしています。プッシュボタンはオプションですが、アクセス ポイントとクライアント デバイスは少なくとも PIN によるセットアップをサポートしていなければなりません。両方のセットアップ オプションによって、従来の手作業による面倒な設定作業が大幅に軽減されます。レガシー デバイスを使っているユーザーでも、各デバイスのメーカーが提供している手作業による方法を使い、Wi-Fi CERTIFIED for Wi-Fi Protected Setup デバイスを含む Wi-Fi ネットワークへレガシー デバイスを追加することができます。

PIN（暗証番号）による方法

PIN（暗証番号）は、ネットワークに接続する各デバイスに提供されます。デバイスには固定の PIN ラベルやステッカーが貼られるか、自動生成された動的な PIN 番号がデバイスのディスプレイに表示されます（例えばテレビの画面やモニター）。PIN によって、ユーザーがネットワークへ接続しようとしているデバイスが確実に接続され、偶発的または故意に他者が別のデバイスをネットワークへ接続することを防止できます。

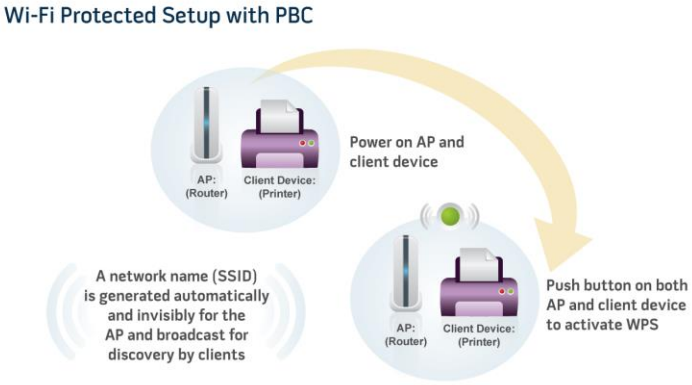


ユーザーは AP の GUI（グラフィカル ユーザー インターフェイス）を通じてレジストラへ PIN を入力するか、ネットワーク上の他のデバイスのインターフェイス画面を通じて管理ページへアクセスし、PIN を入力します（携帯機器のキーパッドや PC のキーボードなど）。

© 2020 Wi-Fi Alliance. All rights reserved.

プッシュボタン（PBC）による方法

ユーザーは AP やクライアント デバイスのボタンを押すか、Wi-Fi Direct 接続でグループ オーナーとなっているデバイスを通じて、ネットワークへの接続とデータの暗号化が有効になります。AP のボタンは、外部レジスタ（例えば上記の PIN の説明にあるようなネットワーク上の他のデバイス）で代用することも可能です。AP およびクライアントのボタンを押してから有効化されるまでにセットアップ時間があり、この間に意図しないデバイスがネットワークへ接続することも可能なので注意が必要です。



自動セットアップ vs. 手動セットアップ

従来の手作業によるネットワークのセットアップでは、ユーザーは自らいくつかの処理を行ってから自分の SSID やパスフレーズを作成しなければなりませんでした。Wi-Fi Protected Setup のメリットは、ユーザーがこのような処理をする必要がなくなることです。Wi-Fi Protected Setup では、セットアップ処理はユーザーの目に見えないところで実行されます。

従来の方法では、ユーザーは AP を電源および有線ネットワークへ接続して起動します。ユーザーは、この有線ネットワークに接続されているコンピュータで Web ブラウザを立ち上げて管理ページへログインし、AP にアクセスします。管理ページではネットワーク名を割り当てて SSID を設定し、次にセキュリティページで適用するセキュリティのタイプを指定します。セキュリティ設定の有効化が完了するとパスフレーズの入力を求められます。AP はこのパスフレーズを使い、通信環境を保護するセキュリティ キーを生成します。この一連の手順は、システムのセットアップや構成設定についてユーザーに普通以上の知識がなければ実行できません。

これらの手順の後、ユーザーはデバイスのコントロール パネルを通じて無線インターフェイスを起動すると共に WLAN 接続を有効化し、ネットワークへの接続設定を行います。クライアント デバイスは範囲内で検出したすべての WLAN のネットワーク名（SSID）をユーザーに提供するので、ユーザーは先ほど設定したネットワーク名を選択し、ネットワークに接続します。次に、前の手順で作成したパスフレーズを入力します。これで、クライアントと AP はセキュリティ識別情報を交換し、セキュリティ下でこの新しいデバイスが WLAN に追加されます。

ほとんどの場合、Wi-Fi Protected Setup によって手作業による処理の多くが不要になります。また、他の必要な一部のタスク（例えば SSID とパスフレーズの生成）を簡素化できるようになります。

このように、Wi-Fi Protected Setup によってユーザーは AP とクライアント デバイスを簡単に起動し、AP のメーカーが提供する PIN 番号を入力するか（PIN の場合）AP とクライアント デバイス上のボタンを押すことで（PBC の場合）、セキュリティ下で設定を実行することが可能になります。セキュリティ コードは自動的に有効化、通信されるので、ユーザーがパスフレーズの設定に関わる必要はありません。

このように SSID および WPA2-Personal セキュリティ キーが自動で適切に設定されるだけでなく、Wi-Fi Protected Setup は正しい PIN 番号を入力しないユーザーによるネットワークへのアクセスを防止する無線セキュリティ環境を提供します。また Wi-Fi Protected Setup にはタイムアウト機能も実装されているので、セキュリティの識別情報が一定の時間内に伝送されなかった場合に設定プロセスは自動的に取り消されます。

© 2020 Wi-Fi Alliance. All rights reserved.

Wi-Fi Protected Setup では、従来のようにユーザーが自分で作成するパスフレーズ（パスワード）よりも強力なパスフレーズが自動生成されるので、無線ネットワークのセキュリティも高くなります。Wi-Fi Protected Setup 以前の環境では、ユーザーはパスフレーズを定義して AP に入力しなければならず、ネットワーク セキュリティを確保するためにはネットワークへ新しいデバイスを追加するたびにこのパスフレーズを再利用する必要がありました。このためほとんどのユーザーは自分の子供やペットの名前など覚えやすい短いパスフレーズを使っていました —— このようなパスフレーズは覚えやすい反面、誰でも簡単に推測できるという危険性を持っています。

Wi-Fi Protected Setup の具体的な内容

Wi-Fi Protected Setup は、ベンダー間で一貫した検出プロトコルに基づいて、既存のネットワークへ新たなデバイスを追加できる、シンプルで一貫した環境を提供します。この手順では、ネットワークへ追加するデバイスの識別情報をレジストラが自動的に発行します。すべての Wi-Fi Protected Setup の Wi-Fi CERTIFIED アクセス ポイント（AP）にはレジストラ機能が実装されています。レジストラはネットワーク上のどのデバイスにあっても構いません。AP 内のレジストラは「内部レジストラ」と呼ばれ、ネットワーク上の他のデバイスにあるレジストラは「外部レジストラ」と呼ばれます。Wi-Fi Protected Setup ネットワークは、単一のネットワークに複数のレジストラが存在する環境もサポートしています。

WLAN で新しいデバイスを設定するプロセスでは、まず設定ウィザードを開始して PIN を入力するかプッシュボタンを押します。この時点でユーザーはアクセスを求めています。

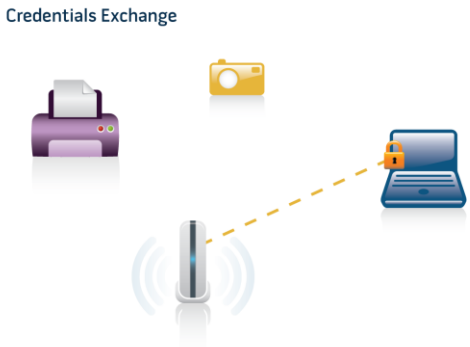
Wi-Fi Protected Setup はデバイスとレジストラ間の情報交換を開始し、レジストラはクライアントの参加を認証するためのネットワーク識別情報（SSID とセキュリティ キー）を発行します。これで、接続が認められた新しいデバイスは侵入者の不正アクセスを心配することなくネットワーク全体を通じてデータをセキュリティ下でやり取りできるようになります。いったん Wi-Fi Protected Setup プロトコルが完了してネットワーク アクセスが認められた後は、ユーザーはネットワークへアクセスするたびにこの設定手順を繰り返す必要はありません。デバイスの電源を入れるとネットワークへのアクセスが自動的に検出されます。

Wi-Fi Protected Setup ネットワークはデータを暗号化し、各デバイスを認証します。このような暗号化なしにオープン ネットワークで利用することもできます。 ネットワーク内における情報およびネットワーク識別情報は WPA2-Personal の認証プロトコルの 1 つ EAP-WSC（Extensible Authentication Protocol）を使ってセキュアな無線環境でやり取りされます。次に各デバイスがお互いに認証し合い（「ハンドシェイク」）、クライアントはネットワークに受け入れられます。レジストラは SSID および WPA2-Personal の PSD（pre-shared key）を伝送し、セキュリティを有効化します。無作為の PSK を使うことで推測が可能であると共に知られやすいパスフレーズが不要になるため、セキュリティが高められます。

従来のインストール方法では、ユーザーは WPA2-Personal を受け入れるように AP を自分で設定し AP とクライアントの両方へ SSID と PSK を手入力しなければなりませんでしたが、このアプローチには常にミスタイプや PSK と SSID の間違いなどユーザーのエラーが発生する恐れが伴いました。これに対して Wi-Fi Protected Setup の場合、識別情報をやり取りするプロセスで初期の設定処理（PIN を入力するかプッシュボタンを押せばネットワーク名と PSK が自動発行されるので、ユーザーによる処理はほとんど必要ありません。

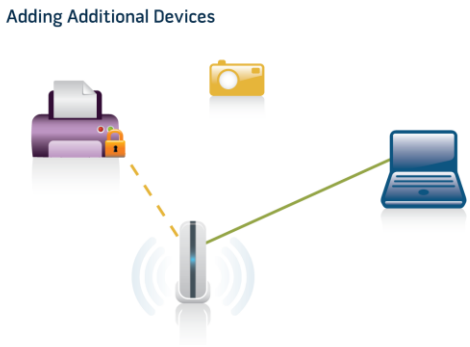
下記の各図は Wi-Fi Protected Setup によるネットワークの設定を図示したもので、金色の線は識別情報のやり取りを表し、緑色の線はセキュリティが有効な W-Fi 接続における通信を表します。

© 2020 Wi-Fi Alliance. All rights reserved.



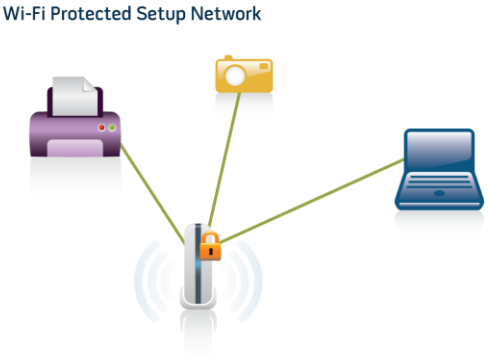
識別情報のやり取り

情報は Wi-Fi ネットワーク上でやり取りされます。このような識別情報のやり取りは、プッシュボタンの場合は AP とクライアントのボタンを押した後に実行され、PIN 入力の場合は追加するクライアント デバイスの GUI でユーザーが PIN 番号を入力した後に実行されます。



新しいデバイスの追加

既存のネットワークへ新しいクライアントを追加する場合は PIN またはプッシュボタンのいずれかを使って設定します。どちらの方法を使うのかは、対象のクライアント デバイスがサポートしている設定方法によって変わります。



幅広い数多くのデバイスに最適な Wi-Fi Protected Setup

PIN またはプッシュボタンを使うことで、幅広い範囲の多様なデバイスを Wi-Fi Protected Setup ネットワークへ追加できます。

Wi-Fi ネットワークのセキュリティ

WPA2 によって、Wi-Fi CERTIFIED 機器は世界中のエンタープライズ企業、一般住宅、モバイル ユーザーに先進のセキュリティ ツールを提供し、その範囲は常に広がりつつあります。すべての新しい Wi-Fi CERTIFIED デバイスとアクセス ポイントは WPA2 機能をサポートしており、毎日のように多くの Wi-Fi ユーザーがそのセキュリティ機能を有効化し、活用しています。

WPA2 は、(1)米国を含む各国政府が機密情報の保護に使用し、企業が WLAN のセキュリティに使用している暗号化プロトコル Advanced Encryption Standard(AES)と、(2)企業ネットワークで幅広く使用され、堅牢な認証機能と高度なネットワーク アクセス コントロール機能を提供する標準規格 IEEE 802.1X の 2 つの主要プロトコルを基盤に構築されています。IEEE 802.11i を基盤にしている WPA2 は、128-bit AES ベースの暗号化機能を提供するとともに、PSK(事前共有鍵、WPA2-Personal モード)および IEEE 802.1X / EAP(WPA2-Enterprise モード)との相互認証機能を提供します。

© 2020 Wi-Fi Alliance. All rights reserved.

2004 年に Wi-Fi Alliance は WPA2 認定プログラムを導入し、2007 年に Wi-Fi Protected Setup を導入したことで、一般住宅のネットワークで簡単に WPA2-Personal を有効化できる環境を実現し、普及を後押ししました。

相互認証。WPA2 は、IEEE 802.1X（WPA2-Enterprise）および PSK（WPA2-Personal）を使用して相互認証を行います。一方通行の認証では、クライアント デバイスが認証情報を送信し、この情報に基づいてアクセスが認められると、クライアント デバイスはネットワークに接続されます。相互認証では、クライアント デバイスは接続を確立する前にネットワーク認証情報を検証することで、ユーザーが不正アクセス ポイントへ接続してしまうことを防ぎます。

強力な暗号化機能。米国連邦情報処理標準（Federal Information Processing Standard）の FIPS Publication 197 として規定される AES は、米国政府の機密情報保護要件を満たす初めての公開暗号化メカニズムです[1]。現在に至るまで、AES の幅広い使用に触発された既知の数多くの攻撃に対しても卓越した防御性を有していることが実証されています。WPA2 ネットワーク内でやり取りされるデータは AES とともに CCMP（Cipher Block Chaining Message Authentication Code Protocol）アルゴリズムのカウンター モードによって暗号化されます。これら両方の組合せにより、WPA2 は現時点において最先端の標準ベースのデータ暗号化環境を提供します。AES のサポートは、世界中のエンタープライズ ネットワークで使用されている多くのプロトコルおよびアプリケーションで必須条件となっています。

相互運用性。WPA2 は、2006 年以降に認定テストを通っているすべての Wi-Fi CERTIFIED 機器がサポートしている、標準ベースのセキュリティ ソリューションです。WPA2 は、機器のメーカーやブランドに関係なく、WPA2 をサポートしているすべての AP（アクセス ポイント）とクライアント デバイスのセッションで有効化できます。これによって WPA2 の可用性の幅が大きく広がり、ネットワーク オペレータとユーザーはネットワーク、デバイスおよびデータフローが場所に関係なく常に保護されているという信頼感を手にできます。

使いやすさ。WPA2 はユーザーを保護する強力な Wi-Fi ツールであるだけでなく、Wi-Fi Protected Setup によって簡単に有効化できます。

セキュリティに関する FAQ（よくある質問）は、後述の付録を参照してください。

まとめ

一般消費者が複数のデジタル デバイスとアプリケーションを使いこなし、それぞれの間でコンテンツを共有している今日のデジタル ライフスタイルにおいて、これらの接続設定に伴う複雑さが二の足を踏む要因になることもあります。Wi-Fi Protected Setup デバイスでは、すべての接続およびセキュリティの設定処理がほとんどシームレスにユーザーの目に触れないところで行われます。一般住宅や小規模オフィスなどの無線ネットワークでの設定に、技術的な知識を持っている友人やすべての「接続方法」を知っている親類を呼んだりする必要はもうありません。

Wi-Fi Protected Setup は Wi-Fi Alliance が提供するオプション（任意）の認定プログラムで、WLAN（無線 LAN）におけるセキュリティの簡単なセットアップと構成設定の支援を目的に考えられています。Wi-Fi Alliance が 2007 年はじめに発表したこのプログラムは、一般住宅および小規模オフィス環境を対象に、業界全体を網羅したネットワーク セットアップ ソリューションを提供します。例えば従来の Wi-Fi 構成設定やセキュリティ設定に対する知識がほとんどない一般ユーザーでも、Wi-Fi Protected Setup によっ

[1] 秘密情報には 128-bit AES を利用可能。 重要機密情報には 192- または 256-bit AES が必須

© 2020 Wi-Fi Alliance. All rights reserved.

て新しい無線ネットワークを簡単に設定し、新しいデバイスをネットワークへ加えたりセキュリティを有効化したりすることができます。

Wi-Fi Protected Setup は PIN 番号の入力またはプッシュボタンによる設定など、分かりやすい共通のセットアップ アプローチを提供します。これらのアプローチによってユーザーは新しい Wi-Fi CERTIFIED デバイスの設定を簡単に実行できると共に、一般住宅や小規模オフィス環境の Wi-Fi ネットワークでセキュリティを有効化できます。この仕様は、Wi-Fi CERTIFIED デバイスによって既成の枠にとらわれない柔軟な環境の質をさらに高めベンダーのテクニカル サポートへの依存を軽減すると共に、小売レベルではユーザーの満足度を高め製品の返品率を下げられるように考えられています。Wi-Fi Protected Setup によって、例えば PSK や SSID などのコンセプトをユーザーが理解する必要をなくすと共に PSK の手入力など手間のかかる処理を排除することで、ネットワークの設定が大幅に簡素化され、簡単に実行できるようになります。

拡張性を念頭に置いて作成されている Wi-Fi Protected Setup は、2.4 GHz および 5 GHz の周波数帯のサポートを通じて 802.11a/b/g/n/ac の Wi-Fi CERTIFIED デバイスをサポートしています。この認定はオプションですが、マルチバンドを含む一般住宅および小規模オフィス向けのデバイスに適用できます。

Wi-Fi Protected Setup および他の Wi-Fi CERTIFIED プログラムに関する詳細、また認定製品の一覧は Wi-Fi Alliance の Web サイト www.wi-fi.org をご覧ください。

Wi-Fi Alliance®について

www.wi-fi.org

Wi-Fi Alliance®（ワイファイ アライアンス）は、世界中のユーザーに Wi-Fi®を届ける、企業の世界的なネットワークです。このコラボレーション フォーラムを構成している Wi-Fi エコシステムの企業は、あらゆる場所ですべての人とモノをつなぎながら、可能な限り最高のユーザー体験を提供するというビジョンを共有しています。2000 年以来、Wi-Fi Alliance が認定した製品は 50,000 を超えています。Wi-Fi CERTIFIED™ は実証済の相互接続性、バックワードの互換性、最高の業界標準のセキュリティ保護を実装した製品の証として広く認められています。今日、Wi-Fi は広がり続ける多種多様なアプリケーション環境でやり取りされている膨大なインターネット トラフィックの半分以上をサポートしています。これからも Wi-Fi Alliance は、世界数十億のユーザーが日々活用している Wi-Fi の普及と進化発展に不断の姿勢で取り組んでいきます。

Wi-Fi®、Wi-Fi ロゴ、Wi-Fi CERTIFIED ロゴ、Wi-Fi Protected Access® (WPA)、Wi-Fi Protected Setup ロゴ、Wi-Fi Direct®、Wi-Fi Alliance®、WMM®、Miracast®、Wi-Fi CERTIFIED Passpoint®、Passpoint®は、Wi-Fi Alliance の登録商標です。Wi-Fi CERTIFIED™、Wi-Fi Protected Setup™、Wi-Fi Multimedia™、WPA2™、Wi-Fi CERTIFIED WPA3™、WPA3™、Wi-Fi CERTIFIED Miracast™、Wi-Fi ZONE™、the Wi-Fi ZONE logo、Wi-Fi Aware™、Wi-Fi CERTIFIED HaLow™、Wi-Fi HaLow™、Wi-Fi CERTIFIED WiGig™、Wi-Fi CERTIFIED Vantage™、Wi-Fi Vantage™、Wi-Fi CERTIFIED Location™、Wi-Fi Location™、Wi-Fi CERTIFIED Home Design™、Wi-Fi Home Design™、Wi-Fi CERTIFIED Agile Multiband™、Wi-Fi Agile Multiband™、Wi-Fi CERTIFIED Optimized Connectivity™、Wi-Fi Optimized Connectivity™、Wi-Fi CERTIFIED EasyMesh™、Wi-Fi EasyMesh™、Wi-Fi CERTIFIED Enhanced Open™、Wi-Fi Enhanced Open™、Wi-Fi CERTIFIED Easy Connect™、Wi-Fi Easy Connect™、Wi-Fi CERTIFIED 6™、the Wi-Fi CERTIFIED 6 logo、Wi-Fi CERTIFIED Data Elements™、Wi-Fi Data Elements™、Wi-Fi Alliance ロゴは、Wi-Fi Alliance の商標です。

© 2020 Wi-Fi Alliance. All rights reserved.

用語の説明

- アクセス ポイント（AP）: 無線デバイスをネットワークに接続するデバイスで、一般的にはWi-Fiルーター。
- AES（Advanced Encryption Standard）: 対称的ブロック データ暗号化法を使った商業/政府が推奨する暗号化標準規格。WPA2の実装で使用します (802.11i,WPA2を参照)。
- 認証: ネットワークへのアクセスを認めるために無線デバイスやエンドユーザーを識別・検証するプロセス。
- 識別情報: ネットワークへのアクセス認証のためにレジストラがクライアントに発行するデータ構造。
- デバイス: LAN（構内通信網）やWAN（広域通信網）環境で他のデバイスと通信することができる独立した物理的または論理的実体。
- クライアント: ネットワークに接続し、ネットワーク上のサーバーや他のデバイスのファイルおよびサービス（ファイル、印刷機能）にアクセスできるすべてのデバイス。
- 発見プロトコル: クライアントおよびレジストラがネットワーク上のデバイスの存在と能力を認識するために使う方法の1つ。
- EAP（Extensible Authentication Protocol）: 無線と有線両方のイーサネット エンタープライズ ネットワークに認証のフレームワークを提供するプロトコル。
- ゲスト: WLAN（無線LAN）への一時的アクセス権のみが認められた識別情報を有するメンバー。
- 802.11a/b/g/n: 最大11Mbps (b)または54Mbps (a, g)または75-600Mbps (n)の速度で2.4 GHz (b/g/n)または5 GHz (a/n)で稼動する無線ネットワークを対象としたIEEE標準規格。
- LAN（Local Area Network: 構内通信網）: インターネット接続、プリンタ、ファイル、ドライブなどのリソースの共有を目的として物理的に近接した同じ領域内にあるコンピュータおよび他のデバイスを接続するシステム。Wi-Fiを使ってデバイスを接続しているLANを特にWLAN（無線LAN）と呼びます。
- ネットワーク名: 無線ネットワークを識別するための名称。無線標準規格ではSSID（service set identifier）と呼ばれます。
- PIN（Personal Identification Number:個人暗証番号）: WLANへ特定のクライアント デバイスを接続させるために必要な無作為に生成される複数桁の数字（Wi-Fi Protected Setupプログラムの場合、PIN番号は4桁または8桁）。
- PSK（Pre-Shared Key）: WPA/WPA2 セキュリティを有効化するための仕組みの1つで、ユーザーが入力したキーやパスワードを使用。
- プッシュボタン: 設定を行う方法の1つで、ネットワークへ接続するデバイスおよびレジストラに実装されている物理的ボタンまたは論理的ボタンを押すことによって実行。
- レジストラ: ドメイン識別情報の発行/取り消しの権限を有する論理的実体で、アクセス ポイントを含め、あらゆるデバイスに統合することが可能。レジストラにはWLAN機能を有しているレジストラとないレジストラがあると共に、指定のドメインにレジストラが複数存在することもあります。
- 登録プロトコル: ネットワークに接続するデバイスへ識別情報を割り当てる際に使うプロトコルで、接続するデバイスとレジストラの間で使用します。
- 外部レジストラ: アクセス ポイントとは別のデバイス上で実行されるレジストラ。
- 内部レジストラ: アクセス ポイントに統合されているレジストラ。

© 2020 Wi-Fi Alliance. All rights reserved.

- WEP: Wired Equivalent Privacyの略で、旧世代のセキュリティ テクノロジー。現在はWPAとWPA2。
- Wi-Fi CERTIFIED™: Wi-Fi Allianceが規定、管理する相互接続性テスト要件に合格したIEEE 802.11ベースの製品であることを認める標準規格に準拠している製品を表します。
- ネットワーク、無線LAN（WLAN）: 無線デバイスのLAN。
- Wi-Fi Protected Access® 2 (WPA2): 無線ネットワーク向けのセキュリティ プロトコル／セキュリティ管理手法で、WPAよりもさらに強力なデータ保護およびネットワーク アクセス コントロール機能を提供します。
- 無線ルーター:　無線デバイスからネットワークへの接続を受け入れるデバイスで、セキュリティのためのネットワーク ファイヤウォールを含むと共にローカル ネットワーク アドレスを提供します。

頭字語の説明

- AES: Advanced Encryption Standard
- AP: アクセスポイント
- EAP: 拡張認証プロトコル
- LAN: Local Area Network（構内通信網）
- PDA: Personal Digital Assistant: 携帯（個人）情報端末
- PIN: Personal Identification Number（個人暗証番号）
- PSK: Pre-Shared Key（事前共有鍵）
- SOHO: Small Office-Home Office（スモール オフィス、ホーム オフィス）
- SSID: サービスセット識別子
- TKIP: Temporal Key Integrity Protocol
- WLAN: 無線LAN
- WPA™: Wi-Fi Protected Access®
- WPA2™: Wi-Fi Protected Access® 2

© 2020 Wi-Fi Alliance. All rights reserved.