

**D-Link Business Cloud
D-Link DBA-1510P**

**D-Link Business Cloud
Business Cloud Wi-Fi Access Point**

ユーザマニュアル



D-Link[®]
Building Networks for People

安全にお使いいただくために

ご自身の安全を確保し、システムを破損から守るために、以下に記述する安全のための指針をよくお読みください。

安全上のご注意

必ずお守りください

本製品を安全にお使いいただくために、以下の項目をよくお読みになり必ずお守りください。

 危険	この表示を無視し、間違った使い方をすると、死亡または重傷を負うおそれがあります。
 警告	この表示を無視し、間違った使い方をすると、火災や感電などにより人身事故になるおそれがあります。
 注意	この表示を無視し、間違った使い方をすると、傷害または物的損害が発生するおそれがあります。

記号の意味  してはいけない「**禁止**」内容です。  必ず実行していただく「**指示**」の内容です。

危険

 **禁止** 分解・改造をしない
火災、やけど、けが、感電などの原因となります。

 **禁止** ぬれた手でさわらない
感電の原因となります。

 **禁止** 水をかけたり、ぬらしたりしない
内部に水が入ると、火災、感電、故障の原因となります。

 **禁止** 水などの液体（飲料水、汗、海水、ペットの尿など）
でぬれた状態で触ったり、電源を入れたりしない
火災、やけど、けが、感電、故障の原因となります。

 **禁止** 各種端子やスロットに水などの液体（飲料水、汗、海水、
ペットの尿など）をいれない。万が一、入ってしまった場合は、
直ちに電源プラグをコンセントから抜く
火災、やけど、けが、感電、故障の原因となります。

 **禁止** 油煙、湯気、湿気、埃の多い場所、高温になる場所や
熱のこもりやすい場所（火のそば、暖房器具のそば、
こたつや布団の中、直射日光の当たる場所、炎天下の車内、
風呂場など）、振動の激しい場所では、使用、保管、放置しない
火災、やけど、けが、感電、故障の原因となります。

 **禁止** 内部に金属物や燃えやすいものを入れない
火災、感電、故障の原因となります。

 **禁止** 砂や土、泥をかけたり、直に置いたりしない。
また、砂などが付着した手で触れない
火災、やけど、けが、感電、故障の原因となります。

 **禁止** 電子レンジ、IH 調理器などの加熱調理機、
圧力釜など高圧容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。

警告

 **禁止** 落としたり、重いものを乗せたり、強いショックを
与えたり、圧力をかけたりしない
故障の原因となります。

 **禁止** 発煙、焦げ臭い匂いの発生などの異常状態のまま
使用しない
感電、火災の原因となります。
使用を止めて、ケーブル/コード類を抜いて、煙が出なくなって
から販売店に修理をご依頼ください。

 **禁止** 表示以外の電圧で使用しない
火災、感電、または故障の原因となります。

 **禁止** たこ足配線禁止
たこ足配線などで定格を超えると火災、感電、または故障の
原因となります。

 **指示** 設置、移動のときは電源プラグを抜く
火災、感電、または故障の原因となります。

 **禁止** 雷鳴が聞こえたら、ケーブル/コード類にはさわらない
感電の原因となります。

 **禁止** ケーブル/コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いもの下敷きなどは、
ケーブル/コードや端子の破損の原因となり、火災、感電、
または故障の原因となります。

 **指示** 本製品付属の AC アダプタもしくは電源ケーブルを
指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。

 **禁止** 各光源をのぞかない
光ファイバケーブルの断面、コネクタおよび本製品のコネクタや
LED をのぞきますと強力な光源により目を損傷するおそれがあります。

 **禁止** 各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を
接触させたり、ほごりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。

 **禁止** 使用中に布団で覆ったり、包んだりしない
火災、やけどまたは故障の原因となります。

 **指示** ガソリンスタンドなど引火性ガスが発生する可能性のある場所や
粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。

 **禁止** カメラのレンズに直射日光などを長時間あてない
素子の退色、焼付きや、レンズの集光作用により、
火災、やけど、けがまたは故障の原因となります。

 **指示** 無線製品は病院内で使用する場合は、
各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。

 **禁止** 本製品の周辺に放熱を妨げるようなもの
（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。

 **指示** 耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。

 **指示** 無線製品をご使用の場合、医用電気機器などを
装着している場合は、医用電気機器メーカーもしくは、
販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。

 **指示** 高精度な制御や微弱な信号を取り扱う
電子機器の近くでは使用しない
電子機器が誤作動するなど、悪影響を及ぼすおそれがあります。

 **指示** ディスプレイ部やカメラのレンズを破損した際は、
割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。

 **指示** ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。

 **禁止** コンセントに AC アダプタや電源ケーブルを
抜き差しするときは、金属類を接触させない
火災、やけど、感電または故障の原因となります。

 **禁止** AC アダプタや電源ケーブルに
海外旅行用の変圧器等を使用しない
発火、発熱、感電または故障の原因となります。

警告

-  ACアダプタもしくは電源プラグについたほこりは、拭き取るほこりが付着した状態で使用すると、火災、やけど、感電または故障の原因となります。
-  ACアダプタや電源ケーブルをコンセントにさしこむときは、確実に差し込む。確実に差し込まないと、火災、やけど、感電もしくは故障の原因となります。
-  接続端子が曲がるなど変形した場合は、直ちに使用を中止する。また、変形をもとに戻しての使用も行わない。端子のショートにより、火災、やけど、けが、感電または故障の原因となります。
-  各種接続端子を機器本体に接続する場合、斜めに差したり、差した状態で引っ張ったりしない。火災、やけど、感電または故障の原因となります。
-  使用しない場合は、ACアダプタもしくは電源ケーブルをコンセントから抜く。電源プラグを差したまま放置すると、火災、やけど、感電または故障の原因となります。
-  お手入れの際は、ACアダプタもしくは電源ケーブルをコンセントから抜く。抜かずに行うと、火災、やけど、感電または故障の原因となります。
-  SD や MicroSD カード、USB メモリの使用中は、カードやメモリを取り外したり、本製品の電源を切ったりしない。データの消失、機器本体の故障の原因となります。
-  磁気カードや磁気を帯びたものを本製品に近づけない。磁気カードのデータが消えてしまうおそれもしくは機器本体の誤作動の原因となります。
-  ディーリンクジャパンが販売している無線機器は国内専用のため、海外で使用しない。海外では国によって電波使用制限があるため、本製品を使用した場合、罰せられる場合があります。海外から持ち込んだディーリンク製品や並行輸入品を日本国内で使用する場合も同様に、罰せられる場合があります。

注意

-  乳幼児の手の届く場所では使わない。やけど、ケガまたは感電の原因となります。
-  静電気注意。コネクタや電源プラグの金属端子に触れたり、帯電したものを近づけますと故障の原因となります。
-  コードを持って抜かない。コードを無理に曲げたり、引っ張ると、コードや機器本体の破損の原因となります。
-  振動が発生する場所では使用しない。故障の原因となります。
-  付属品の使用は取扱説明書に従う。本製品の付属品は、取扱説明書に従い、他の製品に使用しないでください。機器の破損の原因となります。
-  破損したまま使用しない。火災、やけどまたはけがの原因となります。
-  ぐらついた台の上や傾いた場所などの不安定な場所や高所には置かない。落下して、けがなどの原因となります。
-  子供が使用する場合は、保護者が取扱いの方法を教え、誤った使い方をさせない。けがや故障などの原因となります。
-  本製品を長時間連続使用する場合は、温度が高くなることがあるため、注意する。また、使用中に眠ってしまうなどして、意図せず長時間触れることがないようにする。温度の高い部分に直接長時間触れるとお客様の体質や体調によっては肌の赤みやかゆみ、かぶれ、低温やけどの原因となります。
-  コンセントにつないだ状態で、ACアダプタや電源コンセントに長時間触れない。やけど、感電の原因となります。
-  一般の電話機やコードレス電話、テレビ、ラジオなどをお使いになっている近くで使用しない。近くで使用すると、本製品が悪影響を及ぼす原因となる場合があるため、なるべく離れた場所で使用してください。
-  D-Link が指定したオプション品がある場合は、指定オプション品を使用する。不正なオプション品を使用した場合、故障、破損の原因となります。

電波障害自主規制について

本製品は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。

この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

ご使用上の注意

けがや感電、火災および装置の破損のリスクを減らすために、以下の注意事項を遵守してください。

- マニュアルなどに記載されている以外の方法での使用はやめてください。
- 食べ物や飲み物が本製品にかからないようにしてください。また、水気のある場所での運用は避けてください。
- 本製品の開口部に物をさしこまないでください。火事や感電を引き起こすことがあります。
- 付属の AC アダプタもしくは電源ケーブルのみを使用してください。
- 感電を防止するために、本製品と周辺機器の電源ケーブルは、正しく接地された電気コンセントに接続してください。
- やむなく延長コードや電源分岐回路を使用する場合においても、延長コードと電源分岐回路の定格を守ってください。延長コードまたは電源分岐回路に差し込まれているすべての製品の合計定格アンペア数が、その延長コードまたは、電源分岐回路の定格アンペア限界の 8 割を超えないことを確認してください。
- 一時的に急激に起こる電力の変動から本製品を保護するためには、サージサプレッサ、回線調整装置、または無停電電源装置（UPS）を使用してください。
- ケーブルと電源コードは慎重に取り付けてください。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
 - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
 - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
 - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られている製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

静電気は、本製品内部の精密なコンポーネントを損傷する恐れがあります。静電気による損傷を防ぐため、本製品に触れる前に、身体から静電気を逃がしてください。

さらに、静電気放出（ESD）による損傷を防ぐため、以下の手順を実行することをお勧めします。

1. 機器を箱から取り出すときは、機器をシステム等に取り付ける準備が完了するまで、本製品を静電気防止包装から取り出さないでください。静電気防止包装から取り出す直前に、必ず身体の静電気を逃がしてください。
2. 静電気に敏感な部品を運ぶ場合、最初に必ず静電気対策を行ってください。
3. 静電気に敏感な機器の取り扱いは、静電気のない場所で行います。可能であれば、静電気防止床パッド、作業台パッド、および帯電防止接地ストラップを使用してください。

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

無線 LAN について

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。

WLAN は家庭やオフィス環境のみならず、空港やコーヒESHOP、または大学など公共の施設においても幅広く利用されるようになってきました。この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。

ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

WLAN 技術を利用するさまざまな理由

可動性

WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。

低い実現コスト

WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします

簡単な設置と拡張

煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。

低コストのソリューション

無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。本製品は設定可能な複数のモードで多機能性を提供し、コスト削減を行います。

柔軟性

配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術

無線機器は、IEEE 802.11b、IEEE 802.11g、IEEE 802.11n および IEEE 802.11ac に準拠しています。

● IEEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、最大 866.7bps までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。

● IEEE 802.11n 規格

IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 300Mbps までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM(Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク（干渉）の発生を抑えることが可能です。

IEEE 802.11n 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。

WPA/WPA2 には企業向けの「Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「Pre-Shared Key（事前共有鍵）」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認され条件が満たされた時にアクセスが認められます。

「WPA-Enterprise」と「WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「WPA2-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。

EAP（Extensible Authentication Protocol）は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワークにおけるすべてのデバイスの EAP タイプを同一にする必要があります。

重要

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバーヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

無線に関するご注意

電波に関するご注意

本製品は、電波法に基づく小電力データ通信システムの無線製品として、技術基準適合証明を受けています。従って、本製品の使用する上で、無線局の免許は必要ありません。

本製品は、日本国内でのみ使用できます。

以下の注意をよくお読みになりご使用ください。

- 本製品を以下の場所では使用しないでください。
 - ・ 心臓ペースメーカー等の産業・科学・医療用機器の近くで使用すると電磁妨害を及ぼし、生命の危険があります。
 - ・ 工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を必要とする無線局）および特定小電力無線局（免許を必要としない無線局）
 - ・ 電子レンジの近くで使用すると、電子レンジによって無線通信に電磁妨害が発生します。
 - ・ 電気製品、AV 機器、OA 機器などの磁気を帯びているところや電磁波が発生しているところで使用すると下記のような影響があります。
 - 時期や電気雑音の影響を受けると雑音が大きくなったり、通信ができなくなったりすることがあります。
 - テレビ、ラジオなどに近いと受信障害の原因となったり、テレビ画面が乱れたりすることがあります。
 - 近くに複数の無線 LAN アクセスポイントが存在し、同じチャンネルを使用していると、正しく検索できない場合があります。
- 本製品は技術基準適合証明を受けています。本製品の分解、改造、および裏面の製品ラベルをはがさないでください。

2.4GHz 帯使用の無線機器の電波干渉に関するご注意

本製品の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用している移動体識別用の構内無線局（免許を必要とする無線局）および特定小電力無線局（免許を必要としない無線局）並びにアマチュア無線局（免許を必要とする無線局）が運用されています。

- 本製品を使用する前に、近くで移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局が運用されていないことを確認してください。
- 万一、本製品から移動体識別用の構内無線局に対して有害な電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか、または電波の発射を停止してください。
- その他、本製品から移動体通信用の特定小電力無線局に対して電波干渉の事例が発生した場合など、何かお困りのことが起きたときは、弊社サポート窓口へお問い合わせください。

使用周波数帯域	2.4GHz 帯
変調方式	DS-SS 方式 / OFDM 方式
想定干渉距離	40m 以下
周波数変更可否	全帯域を使用し、かつ移動体識別用の構内無線局および特定小電力無線局並びにアマチュア無線局の帯域を回避可能

5GHz 帯使用に関するご注意

無線 LAN の 5.2/5.3GHz（W52/W53）をご利用になる場合、電波法の定めにより屋外ではご利用になれません。

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

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、以下の通信内容を盗み見られる可能性があります。

- 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

- 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、以下の行為を行う可能性があります。

- 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）

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。

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。

このたびは、弊社製品をお買い上げいただきありがとうございます。

本書は、製品を正しくお使いいただくための取扱説明書です。

必要な場合には、いつでもご覧いただけますよう大切に保管してください。

また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。

<https://www.dlink-jp.com/support/info/product-assurance-provision.html>

- 本書の記載内容に逸脱した使用の結果発生した、いかなる障害や損害において、弊社は一切の責任を負いません。あらかじめご了承ください。
- 弊社製品の日本国外でご使用の際のトラブルはサポート対象外になります。
- 弊社は、予告なく本書の全体または一部を修正・改訂することがあります。
- 弊社は改良のため製品の仕様を予告なく変更することがあります。

なお、本製品の最新情報やファームウェアなどを弊社ホームページにてご提供させていただく場合がありますので、ご使用前にご確認ください。

製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。

<https://www.dlink-jp.com/support>

警告 本書の内容の一部、または全部を無断で転載したり、複写することは固くお断りします。

目次

安全にお使いいただくために.....	2
ご使用上の注意.....	4
静電気障害を防止するために.....	4
電源の異常.....	4
無線 LAN について.....	5
WLAN 技術を利用するさまざまな理由.....	5
無線に関するご注意.....	6
はじめに	11
本マニュアルの対象者.....	11
表記規則について.....	12
D-Link Business Cloud の更新について.....	13
第 1 章 設定のながれ (DBA-1510P / D-Link Business Cloud)	15
第 2 章 クラウド AP のご利用にあたって (DBA-1510P)	16
ご利用のための条件.....	16
システム要件.....	16
製品概要.....	17
サポートする機能.....	17
無線 LAN について.....	18
ポートについて.....	19
前面パネル.....	19
背面パネル.....	20
第 3 章 クラウド AP の設置 (DBA-1510P)	21
パッケージの内容.....	21
ネットワーク接続前の準備.....	21
DBA-1510P の設定・設置.....	22
DBA-1510P の接続方法.....	22
DBA-1510P の設置.....	23
イーサネットケーブル/ コンソールケーブルの接続.....	25
IP アドレスの設定について.....	25
電源の投入.....	25
第 4 章 クラウド AP の手動設定 (DBA-1510P)	26
Web ベース設定ユーティリティ (Web GUI) の設定.....	26
Web GUI への接続.....	26
Web GUI 設定画面へのログイン.....	26
ステータス (クラウド AP の手動設定).....	27
一般設定 (クラウド AP の手動設定).....	28
コマンドラインインタフェース (CLI) の設定.....	29
コンソールポートへの接続.....	29
端末をコンソールポートに接続する.....	29
CLI コマンド一覧.....	30
第 5 章 D-Link Business Cloud 概要	31
D-Link Business Cloud について.....	31
D-Link Business Cloud 対応機器.....	32
D-Link Business Cloud 基本仕様.....	33
デバイス・グルーピングについて.....	34
設定の管理について (設定).....	35
モニタ機能について (モニタ).....	36
管理機能について (管理).....	37
メンテナンス機能について (メンテナンス).....	37
ライセンス形態について.....	38

第 6 章 クラウドの基本設定 (D-Link Business Cloud)	40
クラウドユーザインタフェースについて	40
クラウドアカウントの作成とライセンスの登録	41
ログイン	42
ライセンスの登録	42
デバイスグループの作成	43
Wi-Fi ポリシーの設定	44
デバイスの登録	47
直接登録	47
CSV ファイルによる登録	49
アクセスポイントのクラウドへの接続	50
アクセスポイントの接続	51
設定の変更	52
ログインユーザの詳細設定	54
ユーザプロファイル	54
権限	55
ログアウト	55
第 7 章 「モニタ」メニュー (D-Link Business Cloud)	56
概要 (モニタ)	57
地図とフロアマップ	58
マップ管理	58
マップ表示	60
デバイス	61
クライアント	62
不正 AP	63
ホワイトリスト	64
イベント	65
フィルタ (イベント)	66
レポート	67
ダウンロードできる CSV レポート	68
第 8 章 「設定」メニュー (D-Link Business Cloud)	70
SSID プロファイル	71
SSID の追加方法	71
SSID プロファイル編集	72
無線設定	78
基本	78
チャンネル	79
電波出力	80
高度な設定 (2.4GHz)	81
高度な設定 (5GHz)	82
RADIUS 設定	83
RADIUS サーバの編集 / 新しい RADIUS サーバ	84
LDAP 設定	85
LDAP サーバの編集 / 新しい LDAP サーバ	85
キャプティブポータル	86
キャプティブポータル編集 / 新しいキャプティブポータル	87
DHCP プール設定	89
DHCP プール編集 / 新しい DHCP プール	89
一般設定	90
ブッシュ設定	91
デバイスの設定	92
ステータス	92
IP アドレス設定	93
SSID(s)	94
バンド	95
設定	96
ツール	97
環境	98

第 9 章 「メンテナンス」メニュー (D-Link Business Cloud)	99
MAC データベース.....	100
IP データベース.....	101
ローカル DB.....	102
スプラッシュページ編集.....	103
スプラッシュページ編集ボックス.....	104
ファイル管理.....	105
ファームウェア.....	106
組織スケジュール.....	106
デバイスグループスケジュール.....	107
デバイスグループアップグレード.....	108
設定の複製.....	109
第 10 章 「管理」メニュー (D-Link Business Cloud)	110
ダッシュボード.....	111
新しいグループの作成.....	112
デバイスの事前登録.....	112
概要 (管理).....	113
インベントリ.....	114
一括インポート.....	115
一括インポート用エクセルファイルの設定.....	115
タグ.....	117
Admin 管理.....	118
管理者の追加 / 編集.....	119
デバイスグループ / タグ権限.....	120
SAML ロールの追加 / 編集.....	121
ライセンス.....	122
ライセンス状態.....	122
履歴.....	123
ライセンス追加.....	123
ライセンスインポート.....	124
ライセンスインポート用エクセルファイルの設定.....	124
システムログ.....	125
組織設定.....	125
付録 A 工場出荷時設定に戻す	126
付録 B 基本的なネットワークの設定	126
IP アドレスのチェック.....	126
固定 IP アドレスの割り当て.....	127
付録 C コマンドラインで Wi-Fi の設定を確認する場合	128
端末とコンソールポートの接続について.....	128
Telnet の有効化について (Telnet 経由での確認の場合).....	128
設定情報取得モード 有効化手順.....	128
CLI コマンドについて.....	129
SSID 名と PSK を確認する.....	129
チャンネルを確認する.....	130
付録 D 機器故障の際は	131

はじめに

DBA-1510P/D-Link Business Cloud ユーザマニュアルは、DBA-1510P と D-Link Business Cloud の設定および操作方法を例題と共に記述しています。

第1章 設定のながれ (DBA-1510P / D-Link Business Cloud)

- クラウド AP、D-Link Business Cloud を使用する上での基本的な設置、設定のながれです。

第2章 クラウド AP のご利用にあたって (DBA-1510P)

- クラウド AP の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

第3章 クラウド AP の設置 (DBA-1510P)

- クラウド AP の設置方法、接続方法について説明します。

第4章 クラウド AP の手動設定 (DBA-1510P)

- D-Link Business Cloud を使用せずに DBA-1510P へ直接接続、手動での設定方法について説明します。

第5章 D-Link Business Cloud 概要 (D-Link Business Cloud)

- D-Link Business Cloud の概要、対応機器、基本仕様、設定可能な機能やライセンス形態について説明します。

第6章 クラウドの基本設定 (D-Link Business Cloud)

- D-Link Business Cloud の運用上、基本となる設定、操作手順について説明します。

第7章 「モニタ」メニュー (D-Link Business Cloud)

- D-Link Business Cloud の「モニタ」メニューについて説明します。

第8章 「設定」メニュー (D-Link Business Cloud)

- D-Link Business Cloud の「設定」メニューについて説明します。

第9章 「メンテナンス」メニュー (D-Link Business Cloud)

- D-Link Business Cloud の「メンテナンス」メニューについて説明します。

第10章 「管理」メニュー (D-Link Business Cloud)

- D-Link Business Cloud の「管理」メニューについて説明します。

付録 A - D 「D-Link Business Cloud」の利用に関する付録の情報を記載します。

本マニュアルの対象者

本マニュアルは、本製品の設置および管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワーク管理者を対象としています。

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、特長や技術についての詳細情報を記述します。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

表 1 に、本マニュアル中での字体・記号についての表記規則を表します。

表 1 字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」 ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に " (13 ページ) をご参照ください。
courier フォント	CLI 出力文字、ファイル名。	(switch-prompt) #
courier 太字	コマンド、ユーザによるコマンドライン入力。	show network
<i>courier</i> 斜体	コマンド項目 (可変または固定)。	<i>value</i>
< >	可変項目。< > にあたる箇所には値または文字を入力します。	<value>
[]	任意の固定項目。	[value]
[< >]	任意の可変項目。	[<value>]
{ }	{ } 内の選択肢から 1 つ選択して入力する項目。	{choice1 choice2}
(垂直線)	相互排他的な項目。	choice1 choice2
Menu Name > Menu Option	メニュー構造を示します。	Device > Port > Port Properties は、「Device」メニューの下の「Port」メニューの「Port Properties」メニューオプションを表しています。

D-Link Business Cloud の更新について

本項目では、D-Link Business Cloud の更新状況と新機能、その概要について説明します。

Ver: 1.8.5 (2025/3/27 更新)

新機能	概要
最終接続日時の追加	管理 > Admin 管理に「最終接続日時」を追加
SAML ロール管理の追加	管理 > Admin 管理に「SAML ロール管理」セクションを追加
変更点	概要
パスワードルールの変更	クラウドアカウントのパスワードにおいて、パスワードの文字数を 8 文字以上から 10-16 文字以内に

Ver: 1.7.1 - 1.8.4

新機能	概要
スプラッシュページの名前 / 説明の編集	スプラッシュページ一覧のアクション欄に編集アイコン追加 (名前と説明の編集)
2 ファクタ認証	ユーザプロファイルに「2 ファクタ認証」設定を追加
インベントリの一括登録削除の追加	インベントリ画面に「一括登録削除」ボタンを追加
スプラッシュページの TOU 編集	スプラッシュページ編集画面に TOU タブを追加 (Terms of Usage 画面編集)
サブユーザ表示項目	管理 > Admin 管理に「サブユーザ」表示項目を追加
変更点	概要
項目名の更新	クラウド画面の一部ローカライズ (日本語項目名) を更新
検索ボックスの削除	画面右上の検索ボックスを削除
スプラッシュページでのスペルチェックの削除	スプラッシュページ編集でスペルチェック項目を削除

Ver: 1.7.0 (2018/9/20 更新)

変更点	概要
Weibo アカウントの追加	キャプティブポータルでの認証タイプで「Social Login」を選択したとき、Weibo アカウントを追加。
E メール認証機能の追加	キャプティブポータルでの認証タイプで「Social Login」を選択したとき、E メール認証機能も追加。
LLMNR 設定の追加	設定 > 一般設定にて、LLMNR の有効 / 無効を切り替えるチェックボックスを追加。
Telnet 設定の追加	管理 > 組織にて、Telnet の有効 / 無効を切り替えるチェックボックスを追加。

Ver: 1.3.0 (2017/4/7 更新)

新機能	概要 / 該当項目
クライアント接続履歴 (CSV ファイル) のダウンロード	・「モニタ > レポート」からダウンロード
遷移チャネル (オートチャネル機能で遷移するチャネルの設定)	・「設定 > 無線設定 > チャネル」で設定
LDAP サーバ (LDAP サーバを利用したキャプティブポータルでのユーザ認証)	・「設定 > LDAP 設定」で設定
DHCP プール設定	・「設定 > DHCP プール設定」で設定、「設定 > SSID プロファイル」で使用
タイムゾーン設定	・「設定 > 一般設定 (ローカル設定を優先)」で設定
一括インポート	・「管理 > 一括インポート」で設定
ライセンスインポート	・「管理 > ライセンス > ライセンスインポート」で設定
デバイス UID インポート	・「管理 > インベントリ > 読み込み」で設定
変更点	概要
キャプティブポータル認証タイプの変更	キャプティブポータルでの認証タイプに「Social Login」(SNS 認証機能。Google/Facebook アカウントでのログイン) と「LDAP」(LDAP サーバでのユーザ認証) の追加。
キャプティブポータルでのセッションタイムアウト / セッションリミットの追加	キャプティブポータルでの接続時間 / 接続回数 の設定追加。
スプラッシュページ編集	スプラッシュページタイプに「Sign-On-Third-Party」、「Social-Login」の追加。

Ver: 1.2.0 (2015/3/28 更新)

新機能	概要 / 該当項目
Web リダイレクション機能 ^{*1}	・「設定 > SSID プロファイル」で設定
「キャプティブポータル」ローカル DB 認証 ^{*1}	・「メンテナンス > スプラッシュページ編集」、「メンテナンス > ローカル DB」、「設定 > キャプティブポータル」、「設定 > SSID プロファイル」で設定

はじめに

「キャプティブポータル」クリックスルー ^{※1}	・「メンテナンス > スプラッシュページ編集」、「設定 > キャプティブポータル」、「設定 > SSID プロファイル」で設定
管理者招待機能	・「管理 > Admin 管理」で設定
同一 ID 同時ログイン禁止機能	・「ユーザ名 > ユーザプロファイル」で設定
管理 GUI アイドルタイムアウト	・「ユーザ名 > ユーザプロファイル」で設定
変更点	概要
デバイスオフライン判定基準の変更	オフライン状態が 5 分間継続した場合、オフライン判定となるように変更。

※1 本機能を利用する場合は、DBA-1510P にファームウェアバージョン 1.20 以上がインストールされている必要があります。

Ver. 1.1.0 (2015/1/28 更新)

新機能	概要 / 該当項目
ゲストアクセスモード ^{※1}	・「設定 > SSID プロファイル」で設定
NAT モード ^{※1}	・「設定 > SSID プロファイル」で設定
IP フィルタリング ^{※1}	・「メンテナンス > IP データベース」、「設定 > SSID プロファイル > IP フィルタリング」で設定
ローカル設定優先機能 ^{※1}	・「設定 > 一般設定 (グループ設定)」、または「設定 > デバイスの設定 > 設定 (デバイス個別設定)」で設定
プロキシ経由でのクラウド接続機能	・「設定 > 一般設定 (グループ設定)」、または「設定 > デバイスの設定 > IP アドレスの設定 (デバイス個別設定)」で設定
変更点	概要 / 該当項目
権限 (組織内管理者 / モニタ管理者) の追加	・「管理 > Admin 管理」で設定

※1 本機能を利用する場合は、DBA-1510P にファームウェアバージョン 1.01 以上がインストールされている必要があります。

第1章 設定のながれ (DBA-1510P / D-Link Business Cloud)

クラウド AP、D-Link Business Cloud をはじめに使用する上での基本的な設置、設定方法です。

まず「D-Link Business Cloud」へアクセスし、クラウドアカウントの作成とライセンスを登録します。その後クラウドでデバイスグループの設定、Wi-Fi ポリシーの設定を行い、管理するクラウド AP (DBA-1510P) を登録 (デバイスの登録) します。それがクラウドでの基本的な初期設定の作業になります。そしてクラウド AP (DBA-1510P) を設置、クラウドへの接続 (ネットワークへの接続) を行いクラウドとクラウド AP の基本的な初期設定の作業は完了です。

注意 「D-Link Business Cloud」にアクセスする際、URL はライセンス証書に記載されています。ライセンス証書をご確認ください。

以下が基本的な初期設定の作業のながれになります。



- ・「①クラウドアカウント作成とライセンス登録」は第6章「[クラウドアカウントの作成とライセンスの登録](#)」を参照ください。
- ・「②デバイスグループの作成」は第6章「[デバイスグループの作成](#)」を参照ください。
- ・「③ Wi-Fi ポリシーの設定」は第6章「[Wi-Fi ポリシーの設定](#)」を参照ください。
- ・「④デバイスの登録」は第6章「[デバイスの登録](#)」を参照ください。
- ・「⑤クラウド AP の設置」は「[第3章 クラウド AP の設置 \(DBA-1510P\)](#)」を参照ください。
- ・「⑥クラウド AP のクラウドへの接続」は第6章「[アクセスポイントのクラウドへの接続](#)」を参照ください。
- ・D-Link Business Cloud の各メニューの詳細設定については第7章以降、各メニューの章を参照ください。

第2章 クラウド AP のご利用にあたって (DBA-1510P)

- ご利用のための条件
- 製品概要
- サポートする機能
- 無線 LAN について
- ポートについて
- 前面パネル
- 背面パネル

ここでは、クラウド AP の概要とその機能について説明します。また、前面、背面の各パネルと LED 表示について説明します。

ご利用のための条件

本製品を使用するためには、幾つかの基本的な条件があります。下記をご確認ください。

- ・ 使用許諾ライセンス（別途有償）が必要です。
- ・ DBA-1510P 単体では動作しません。
- ・ 継続してご利用になる場合、ライセンスの使用期限が来る前に、ライセンスを購入し、更新する必要があります。
- ・ ライセンスを本製品から非適用にした場合、本製品は通信が停止します。

システム要件

クラウド利用にあたりルータまたはファイアウォールで、以下のプロトコルがご利用可能かどうかご確認ください。

プロトコル	用途・備考
TCP 80 (HTTP)	ファームウェアのアップデート用
TCP 443 (SSL)	クラウドサーバとの通信用
UDP 123 (NTP)	スケジュール機能用

以下の3つのプロトコルもまた許可されている必要があります。

プロトコル	用途・備考
UDP 67 (DHCP)	Static IP を使った場合は不要
UDP 53 (DNS)	
TCP 53 (DNS)	

補足事項

以下の機能が許可されていない場合、一部の機能がご利用になれません。予めご了承ください。

- ・ Ping (ICMP)
- ・ Traceroute (UDP 33435 から昇順で使用)
- ・ RADIUS

システム要件 (管理 PC)

クラウドにアクセスをする管理 PC には、以下のシステム条件が必要です。

- ・ 最新バージョンの Google Chrome ™
- ・ イーサネットへの接続

製品概要

D-Link DBA-1510P は Wi-Fi をクラウドから一元管理する次世代ソリューション「D-Link Business Cloud」に対応した Wi-Fi アクセスポイントです。手間のかかる Wi-Fi コントローラや Wi-Fi 監視システムの設定・運用が不要になり、各所にある DBA-1510P のネットワークを一カ所から一元的に設定・管理することが可能です。さらに IEEE802.3at に準拠した PoE 受電機能 (PoE+)、IEEE802.11ac 準拠、2.4GHz/5GHz デュアルバンド同時利用対応、信頼性の高いセキュリティ機能など、あらゆる環境で充実した機能と安全性を提供します。ワイヤレスネットワーク上での不正アクセスを防止する無線セキュリティ機能を搭載、アクセスポイントとして必要十分なセキュリティを確保し、安心で安全、そして安定したワイヤレスネットワークの構築を実現することができます。

D-Link Business Cloud 対応

本製品は「D-Link Business Cloud」に対応、Wi-Fi アクセスポイントの設定ポリシーをグループ単位で適用できるため、各所にある大量の AP を一括して設定・管理することができます。さらにクラウド管理 Wi-Fi AP である本製品は、インターネットに接続されると、自動的にクラウドへアクセスし、設定ポリシーを自動的にダウンロードして自らに適用するため、常に最新の設定ポリシーをネットワークで共有することが可能です。

様々な環境への対応

2.4GHz：2dBi、5GHz：3dBi 同時デュアルバンド無線ネットワークを構築することができる本製品は、2.4GHz、5GHz の両帯域において広範囲な無線領域を実現します。さらに 802.3at PoE 受電機能の搭載により電源供給の難しい場所、屋内のあらゆる場所への設置、導入が可能です。

高速無線通信

10/100/1000BASE-T ポートを搭載、2.4GHz、5GHz の両帯域の同時利用に対応しており、さらに先進の 802.11ac 高速ワイヤレス通信を最大 1300Mbps の転送速度で実現します。

優れた管理性とセキュリティ

本製品は基本的なワイヤレスセキュリティをサポートし、安全なワイヤレスネットワークを維持・提供します。加えて不正 AP 検知や MAC アドレスフィルタリング機能でネットワークのさらなる安全性を高めることができます。マルチ SSID (最大 16 個) をサポートし、さらに WLAN クライアントパーティション機能によりクライアント間の通信を制限することもでき、管理性とセキュリティの両方において充実したアクセスポイントです。

サポートする機能

- ・「D-Link Business Cloud」対応 / クラウド管理
- ・高速無線ネットワーク規格の IEEE 802.11ac 準拠により最大 1.3Gbps(理論値) までの無線転送速度を提供します。
- ・IEEE 802.11n に対応し 2.4GHz/5GHz 周波数範囲において最大 450Mbps(理論値) までの無線転送速度を提供します。
- ・IEEE 802.11b に対応し、最大 11Mbps までの無線データ転送速度を供給しているため、システムの接続性を損なうことなく、IEEE 802.11n および IEEE 802.11g に移行できます。
- ・IEEE 802.11g 規格と互換性があり、2.4GHz 周波数範囲において最大 54Mbps の無線転送速度を提供します。
- ・IEEE 802.11a 規格と互換性があり、5GHz 周波数範囲において最大 54Mbps の無線転送速度を提供します。
- ・WPA による強固なセキュリティ
従来の規格よりさらに高度な暗号化方式である WPA(Wi-Fi Protected Access) を採用し、クライアントとネットワークを安全に接続します。
- ・OFDM(Orthogonal Frequency Division Multiplexing) 技術の採用。
- ・10/100/1000M イーサネットポート x 1
- ・CONSOLE ポートからの設定 / 管理
- ・Web GUI による設定 / 管理 (簡易のみ)
- ・802.3at PoE 準拠
- ・MAC アドレスフィルタリング
- ・マルチ SSID (最大 16 個)
- ・2.4 ~ 2483.5GHz、5.15 ~ 5.35GHz、5.47 ~ 5.725GHz 周波数範囲で作動。

注意 最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバーヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

注意 最大の無線信号速度は IEEE 802.11 仕様書を参考にしています。実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバーヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

無線 LAN について

業界標準に基づく弊社の無線 LAN 製品は、ご家庭や職場または公共の施設において、使いやすく互換性の高い高速の無線接続を提供します。これらを使用して時間や場所に関わらず必要なデータにアクセスすることができます。

WLAN は家庭やオフィス環境のみならず、空港やコーヒESHOP、または大学など公共の施設においても幅広く利用されるようになってきました。この WLAN 技術を用いることにより、仕事やコミュニケーションがさらに効率的に行えるようになってきています。無線技術により可動性が増し、配線や固定のインフラが減少したことでユーザに大きなメリットが生まれました。

ノート型やデスクトップ型 PC に使用する無線アダプタはイーサネットのアダプタカードと同じプロトコルをサポートしており、無線ユーザは有線ネットワークと同じアプリケーションを利用できるようになりました。

WLAN 技術を利用するさまざまな理由

- 可動性
WLAN の動作範囲内のどこからでもデータにアクセス可能であり、生産性を向上します。また、リアルタイムな情報に基づく管理により作業効率が向上します。
- 低廉な導入コスト
WLAN は設置、管理、変更、移転のすべてが簡単です。このような WLAN の扱いやすさはネットワークの変更が頻繁に要求される環境に適しています。WLAN は有線ネットワークでは困難であった場所へのネットワーク導入を可能にします。
- 簡単な設置と拡張
煩わしい複雑なケーブル配線作業、特に壁や天井へのケーブル敷設の必要がないため、手早く簡単にシステムの設置を行うことができます。無線技術は、ネットワークを家庭やオフィスを超えて拡張することで、さらなる多用途性を提供します。
- 低コストのソリューション
無線 LAN デバイスは、従来のイーサネット用機器とほぼ同等の価格設定となっています。
- 柔軟性
配置する無線 LAN デバイスの数によって、ピアツーピアのネットワークが適している小さなユーザグループから、100 ~ 1000 人のユーザを収容する大規模なインフラネットワークまで、自由自在に構築することができます。

世界基準対応の技術

DBA-1510P 無線アクセスポイントは、IEEE 802.11ac、IEEE 802.11a、IEEE 802.11b、IEEE 802.11g、および IEEE 802.11n に準拠しています。IEEE 802.11ac 規格の無線通信速度は、最大 1.3Gbps (理論値) までと高速化されており、5GHz 帯の周波数と「OFDM」技術をサポートしています。IEEE 802.11n 規格は、従来の IEEE 802.11a、IEEE 802.11b および IEEE 802.11g の機能を拡張した規格です。無線通信速度は、最大 450Mbps (理論値) までと高速化され、2.4GHz 帯および 5GHz 帯の周波数を利用し、こちらも「OFDM」技術をサポートしています。

これらにより、多くの環境化において、無線サービスエリア内でネットワークによる大容量の送受信や遅延の少ない MPEG 形式の映像の視聴などが可能になります。OFDM (Orthogonal Frequency Division Multiplexing) という技術により、この大容量のデジタルデータの高速伝送を無線で行うことができます。OFDM では、無線信号を小さいサブ信号に分割し、それらを同時に異なる周波数で送信します。OFDM により、信号伝送時のクロストーク (干渉) の発生を抑えることが可能です。

本製品は自動的に最適な通信速度を検出し、高速で広範囲の通信エリアを確保します。

IEEE 802.11 規格は、「WPA」を含む現在最も先進的なネットワークセキュリティ機能を提供します。WPA/WPA2 には企業向けの「Enterprise」とホームユーザ向けの「Personal」の 2 種類があります。「WPA-Personal」と「WPA2-Personal」はユーザ認証に必要なサーバ機器を持たないホームユーザを対象としています。その認証方法は、無線ルータやアクセスポイントに「Pre-Shared Key (事前共有鍵)」の定義を行うという点で WEP と似ています。クライアントとアクセスポイントの両方において、事前共有鍵が確認された条件が満たされた時にアクセスが認められます。暗号化には、パケット単位の動的なハッシングを行う「TKIP (Temporal Key Integrity Protocol)」と呼ばれる方式を採用しています。また、インテグリティチェック機能により無線通信時のデータの改ざんを防止します。

「WPA-Enterprise」と「WPA2-Enterprise」は既にセキュリティ用にインフラが整備されている企業を対象としています。ネットワーク内のサーバを中心にネットワーク管理とセキュリティの実施を行うような環境を想定しています。

ネットワーク管理者は、RADIUS サーバ上で 802.1X を使用し、無線 LAN へのアクセスを許可するユーザのリストを定義します。「WPA-Enterprise」または「WPA2-Enterprise」を実装した無線 LAN にアクセスする場合、ユーザはユーザ名とパスワードの入力を要求されます。ユーザがネットワーク管理者によってアクセスを許可されており、正しいユーザ名とパスワードを入力すると、ネットワークへのアクセスが可能になります。例えば、ある社員が会社を辞めるというような場合、ネットワーク管理者がアクセス許可者のリストからその社員のデータを削除すれば、ネットワークを危険にさらすことは避けることができます。

EAP (Extensible Authentication Protocol) は Windows OS に実装されています。802.1X の機能を使用する際には、ネットワーク内のすべてのデバイス上の EAP タイプを同一のものにする必要があります。

注意

最大の無線信号速度は理論値であり、実際のデータスループットは異なります。ネットワーク条件と環境には、ネットワークトラフィック量、建築材料や工事、ネットワークオーバーヘッドが含まれ、実際のデータスループット速度は低くなります。環境条件は無線信号範囲に悪影響を与えます。

ポートについて

- ・ エンドステーション、サーバ、ハブなどのネットワークデバイスとの接続および設定・管理用に 1 ポートの UTP (Auto MDI/MDI-X) (PoE 受電) ポートと 1 ポートのシリアルコンソールポートを有します。
- ・ UTP ポートは 10Mbps/100M/1000Mbps、半二重 / 全二重間のオートネゴシエーション機能、フローコントロール、PoE 受電機能をサポートしています。

前面パネル

DBA-1510P の前面パネルには、ステータスを表示する Power LED、D-Link クラウド LED、2.4/5GHz LED および LAN ポート LED が配置されていて、前面の縁にセキュリティスロットとリセットボタンを搭載しています。

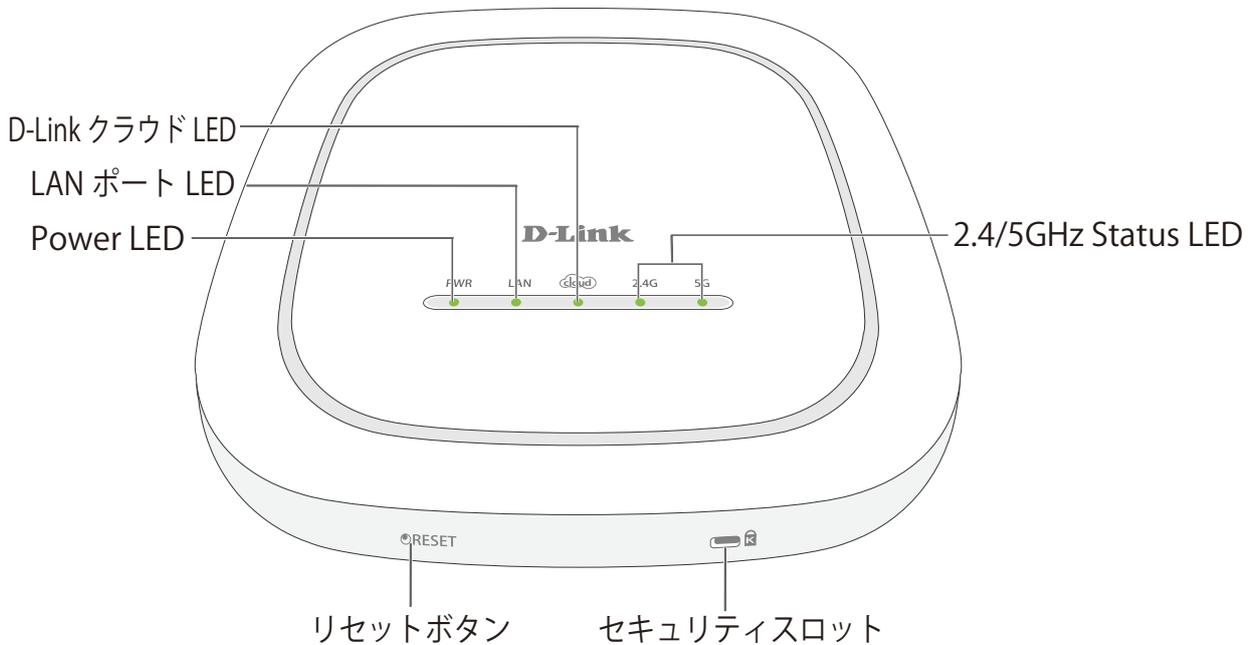


図 2-1 前面パネル

ステータス LED は以下の状態を表示します。

DBA-1510P LED 一覧

LED	色	状態	状態説明
Power	緑	点灯	電源が供給され正常に動作しています。
	橙	点灯	起動中です。
2.4/5 GHz	緑	点灯	各帯域において無線 LAN による通信が可能な状態です。
		点滅	各帯域において無線 LAN によりデータを送受信しています。
LAN	緑	点灯	ネットワークにリンクしています。
		点滅	ネットワーク上でデータを送受信しています。
	—	消灯	リンクが確立していません。
Cloud	緑	点灯	クラウドによる管理モードで動作しています。
	橙	点灯	クラウドに接続中です。
	赤	点灯	AP は正しく動作していません。

DBA-1510P 前面パネル一覧

インタフェース	説明
リセットボタン	機器のリセットボタンです。ボタンを押す時間の長さにより動作は異なります。 <ul style="list-style-type: none"> ・ 再起動 - 2~5 秒ボタンを押し続けます。 ・ 初期化 - 6~15 秒ボタンを押し続けます。製品の設定が初期化されます。 ・ 起動ファームウェア変更 - 15 秒以上ボタンを押し続けると、ファームウェアアップデート前に使用していた旧ファームウェアバージョンで再起動します。
セキュリティスロット	市販のセキュリティロックを使用して機器に鍵をかけることが可能です。

背面パネル

DBA-1510P の背面パネルには、電源コネクタ、コンソールポートおよび LAN ポート (PoE) (10BASE-T/100BASE-TX/1000BASE-T) ポートが配置されています。

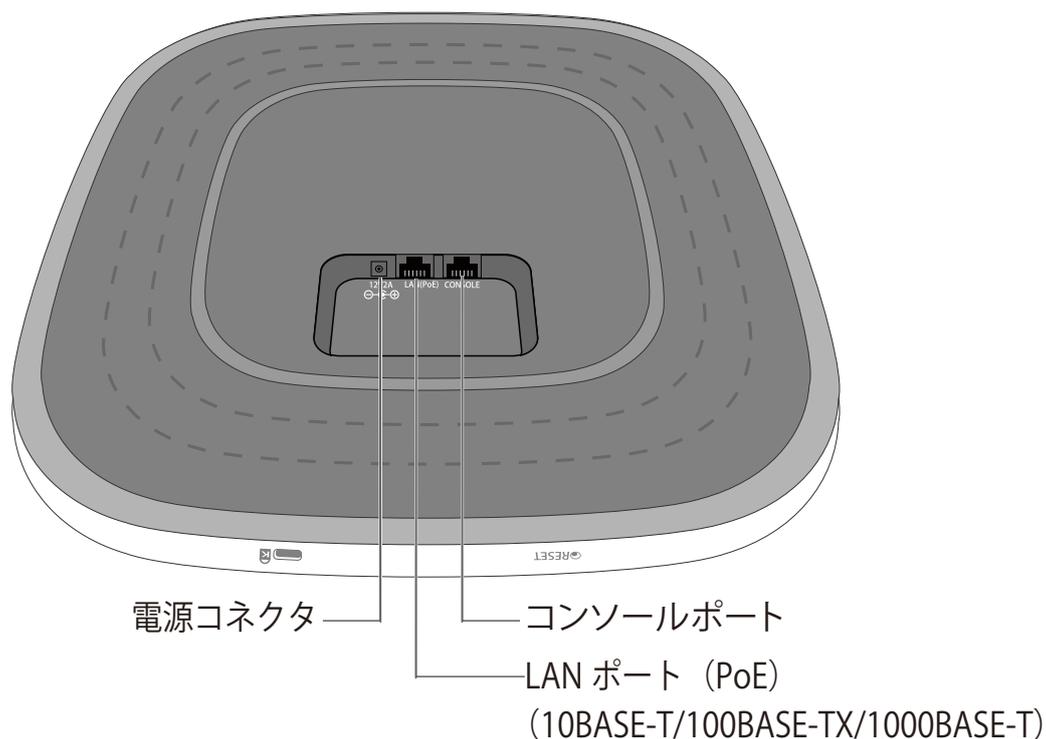


図 2-2 背面パネル

DBA-1510P 背面パネル一覧

部位	機能
LAN ポート (PoE) (10/100/1000BASE-T)	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T イーサネットへの接続が可能です。また、PoE スイッチを使用して受電します。IEEE802.3at に準拠した PoE (PoE+) での受電が可能です。10BASE-T の場合はカテゴリ 3 以上、100BASE-TX の場合はカテゴリ 5 以上、1000BASE-T の場合はエンハンストカテゴリ 5 以上の UTP/STP ケーブルを接続します。PoE により受電する場合はカテゴリ 5 以上の UTP ストレートケーブルを接続します。
コンソールポート	付属のコンソールケーブルを接続します。
電源コネクタ	付属の AC アダプタを接続します。

第3章 クラウドAPの設置 (DBA-1510P)

- パッケージの内容
- ネットワーク接続前の準備
- DBA-1510P の設定・設置

パッケージの内容

ご購入いただいた製品の梱包箱を開け、同梱物を注意して取り出してください。以下のものが同梱されています。

- ・ 本体 x 1
- ・ ACアダプタ x 1
- ・ イーサネットケーブル x 1
- ・ コンソールケーブル (RJ-45/RS-232) x 1
- ・ ゴム足 x 4
- ・ マウントキット
 - マウンティングリング x 1
 - ネジ x 3
 - アンカー x 3
- ・ クイックインストールガイド x 1
- ・ PLシート x 1

不足しているものや損傷を受けているものがありましたら、サポート窓口までご連絡ください。

ネットワーク接続前の準備

アクセスポイントの設置場所が性能に大きな影響を与えます。以下のガイドラインに従って本製品を設置してください。

設置にあたっての注意

本製品の使用により、動作範囲内にて無線でネットワークアクセスが可能になりますが、壁や天井など無線信号が通過する物体の数や厚さ、場所などにより、動作範囲が制約を受ける場合があります。一般的には、構造物の材質や設置場所での無線周波数のノイズが動作範囲に影響を与えます。

1. 本製品と他のネットワークデバイスとの間に入る壁や天井の数をできるだけ少なくしてください。一枚の壁や天井の影響により、本製品の動作範囲は1～30メートルの範囲となります。間に入る障害物の数を減らすようデバイスの位置を工夫してください。
2. ネットワークデバイス間の直線距離にご注意ください。厚さ50センチの壁を45度の角度で無線信号が通過する時、通り抜ける壁の厚みは約1メートルになります。2度の角度で通過すると、通り抜ける厚みは14メートルになります。信号が障害物をなるべく直角に通過するような位置にデバイスを設置し、電波を受信しやすくしてください。
3. 無線信号の通過性能は建築材料により異なります。金属製のドアやアルミの金具などは動作範囲を小さくする可能性があります。無線LANデバイスや無線LANアダプタ使用のコンピュータの設置は、信号がなるべく乾式壁か開放された戸口などを通るような位置に設置してください。
4. 周波数ノイズを発生する電気機器や家電製品からは、最低でも1、2メートル離してデバイスを設置してください。
5. 2.4GHzのコードレス電話またはX-10（シーリングファン、ライト、およびホームセキュリティシステムなどの無線製品）を使っている場合、ご使用の無線接続は著しく性能が低下するか、または完全に切断される可能性があります。2.4GHz電話の親機は可能な限りご使用の無線機器から離れていることを確認してください。電話を使用していない場合でも、親機は信号を送信します。
6. ACアダプタは必ず付属のACアダプタをご使用ください。

DBA-1510P の設定・設置

DBA-1510P の接続方法

クラウド AP である DBA-1510P の設定や管理は、インターネットに接続することでクラウド側から自動的に行われます。管理する PC をインターネットに接続しクラウドでの Wi-Fi ポリシーの設定を行うことで、登録した複数の DBA-1510P を一度に設定、管理することができます。インターネット環境にある DBA-1510P はクラウドに自動的に接続、設定をダウンロードして適合するネットワークに参加します。

注意 DBA-1510P は自動的に LAN 内の DHCP サーバから IP アドレスを取得しクラウドへ接続しますが、LAN 内で固定 IP アドレスを割り振らなければならない場合や、VLAN を設定する必要がある場合、インターネットを介してクラウドに接続することができない場合には、DBA-1510P に直接アクセスする事で手動で IP アドレスや VLAN などを設定する事ができます。

クラウド経由で接続（DBA-1510P の全ての設定が可能）

クラウド経由で DBA-1510P とコンピュータを接続します。複数の DBA-1510P を一度に設定、管理することができます。

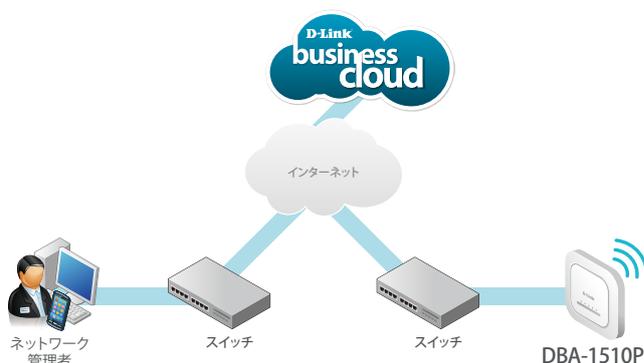


図 3-1 接続方法（クラウド）

イーサネットケーブルを使って直接接続（DBA-1510P の IP アドレス、VLAN 等の基本設定のみ可能）

イーサネットケーブルを使って DBA-1510P とコンピュータを直接接続します。



図 3-2 接続方法（直接接続）

ブラウザのアドレス欄に DBA-1510P のホスト名を入力し、Enter を押下します。ホスト名の初期値は「DBA-1510P-XXXX」で、XXXX は DBA-1510P の底面にあるデバイスラベルに記載されている MAC アドレスの最後の 4 ケタになります。

ローカルネットワークで接続（DBA-1510P の IP アドレス、VLAN 等の基本設定のみ可能）

DBA-1510P とコンピュータを同じスイッチもしくはルータに接続します。



図 3-3 接続方法（ローカルネットワーク接続）

ブラウザのアドレス欄に DBA-1510P のホスト名を入力し、Enter を押下します。ホスト名の初期値は「DBA-1510P-XXXX」で、XXXX は DBA-1510P の底面にあるデバイスラベルに記載されている MAC アドレスの最後の 4 ケタになります。

SSID「DBA-1510P-XXXX」から無線で接続（DBA-1510PのIPアドレス、VLAN等の基本設定のみ可能）

SSID「DBA-1510P-XXXX」を介してDBA-1510Pに無線でコンピュータを接続します。



図 3-4 接続方法（無線接続（SSID））

ブラウザのアドレス欄にDBA-1510Pのホスト名を入力し、Enterを押下します。ホスト名の初期値は「DBA-1510P-XXXX」で、XXXXはDBA-1510Pの底面にあるデバイスラベルに記載されているMACアドレスの最後の4ケタになります。

クラウドを使用せずに直接DBA-1510Pを設定する詳細方法については「[第4章 クラウドAPの手動設定（DBA-1510P）](#)」を参照ください。

DBA-1510Pの設置

DBA-1510P本体の設置方法について説明します。

壁面への設置

本製品を壁面に設置するために以下のものをご用意ください。

- ・マウンティングリング（付属）
- ・ネジとアンカー（付属）
- ・ドリル（壁面に穴をあける器具）
- ・ドライバー

1. 設置する場所（壁もしくは天井）にマウンティングリングを合わせます。ネジを差し込む場所をマークして、マウンティングリングを外します。

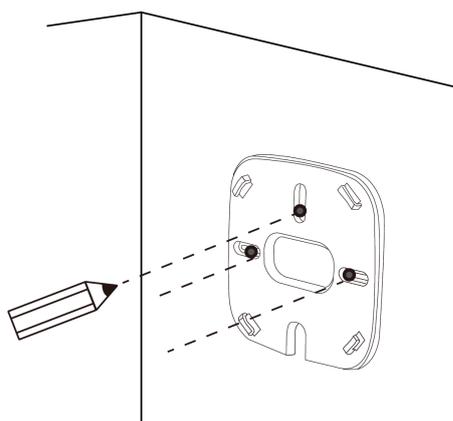


図 3-5 位置確認（壁面設置）

2. マークした箇所にドリルで穴をあけ、アンカーを挿入します。

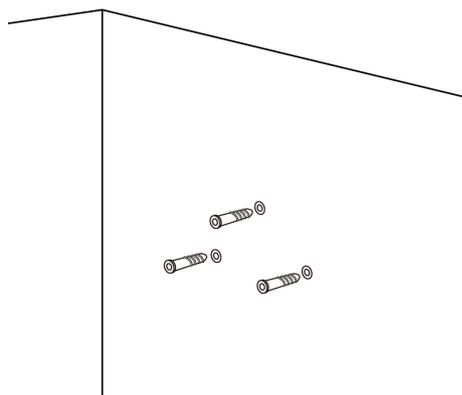


図 3-6 アンカー挿入

3. 壁にマウンティングリングを、同梱のネジを使って取り付けます。

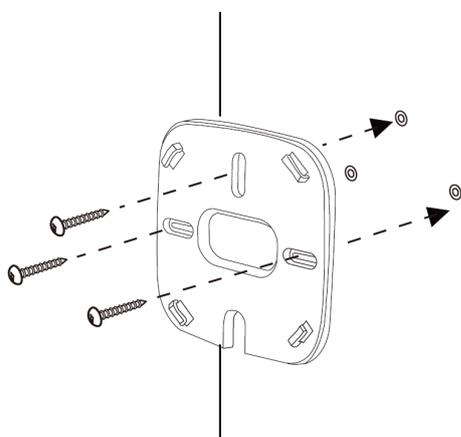


図 3-7 マウンティングリングネジ止め

4. DBA-1510P の LAN ポートにイーサネットケーブルを接続します。
5. DBA-1510P と一緒に PoE 給電スイッチもしくはルータを使わない場合は、DBA-1510P の電源プラグに電源ケーブルを接続します。
6. マウンティングリングブラケットに DBA-1510P を合わせ、DBA-1510P を時計回りに回してロックします。

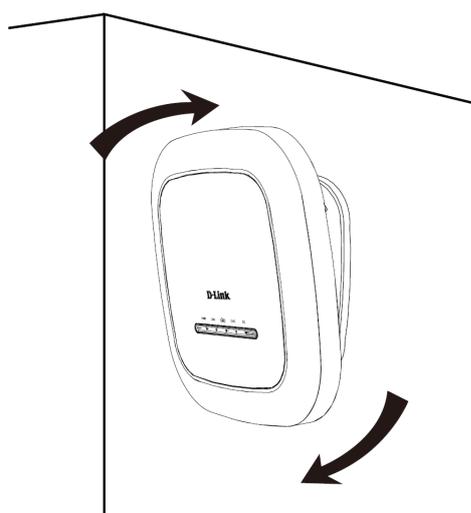


図 3-8 機器の設置

注意 取り付け位置はアンテナの長さを考慮し、障害物や天井にぶつからない場所にしてください。

注意 石膏ボードやベニヤなどに設置する場合は、あらかじめ壁の厚さを確認の上、きりやドリルで穴をあけて付属のアンカーボルトを埋め込んだ後にネジを取り付けてください。

デスクトップでの使用

本製品をデスクトップで使用するために以下のものをご用意ください。

- ・ ゴム足

1. DBA-1510P の背面にある穴に、同梱のゴム足を取り付けてください。

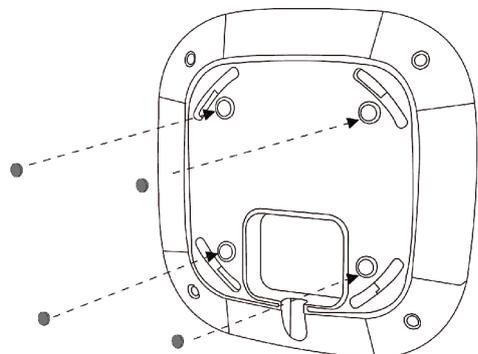


図 3-9 位置確認

2. DBA-1510P の LAN ポートにイーサネットケーブルを接続します。
3. DBA-1510P と一緒に PoE 給電スイッチもしくはルータを使わない場合は、DBA-1510P の電源プラグに電源ケーブルを接続します。

イーサネットケーブル / コンソールケーブルの接続

- ・ 付属のイーサネットケーブルの一端を本製品の背面にある RJ-45 コネクタ (LAN(PoE)) に接続し、もう一端をルータ、スイッチ等のネットワーク機器に接続します。
- ・ 付属のコンソールケーブルの一端を本製品の背面にある RJ-45 コネクタ (CONSOLE) に接続し、もう一端を管理 PC などに接続します。

IP アドレスの設定について

DBA-1510P の電源を入れると機器に内蔵の DHCP クライアントが IP アドレス取得のためのネットワーク内の DHCP サーバを検索します。もし IP アドレスを自動的に取得できない場合、Web ベースユーティリティ (Web GUI) を使用して手動で IP アドレスを割り振ったり、必要なネットワーク設定を行う事などが可能です。

クラウドを使用せずに直接 DBA-1510P を設定する詳細方法については「[第 4 章 クラウド AP の手動設定 \(DBA-1510P\)](#)」を参照ください。

注意 DBA-1510P が LAN 内の DHCP サーバから IP アドレスを取得できる場合はこの設定不要です。

注意 ネットワークに DHCP サーバがない場合や設置する予定のない場合は、まず製品の接続方法を「DHCP」から「Static」に変更し、手動で IP アドレスを指定する必要があります。

注意 ログインの際の初期「ID/パスワード」は Web ベースユーティリティ、CLI ともに「admin/admin」または「admin/password」になります。これらの設定は「D-Link Business Cloud」から変更することが可能です。

電源の投入

1. 付属の AC アダプタを接続し、AC アダプタのプラグを電源コンセントに接続します。
2. 本製品に電源が供給されると、Power LED が点灯します。

PoE 給電機器を使用しての電源の投入

1. イーサネットケーブルの一端を本製品の背面にある RJ-45 コネクタに接続し、もう一端を PoE スイッチ等の PoE 給電機能のあるネットワーク機器に接続します。
2. 本製品に電源が供給されると、Power LED が点灯します。

第4章 クラウド AP の手動設定 (DBA-1510P)

ここでは、D-Link Business Cloud を使用せずに DBA-1510P へ直接接続、手動設定をする Web GUI について説明します。

注意 DBA-1510P がクラウドに接続できる場合は、この設定は必要ありません。

注意 DBA-1510P(ファームウェアバージョン 1.01 以上)を直接手動設定する場合、クラウドのデフォルトの設定では、DBA-1510P に直接手動設定した内容が優先される設定となっています。ファームウェアバージョン 1.00 では、常にクラウドの設定が優先されます。

- [Web ベース設定ユーティリティ \(Web GUI\) の設定](#)

Web ベース設定ユーティリティ (Web GUI) の設定

クラウド AP である DBA-1510P の設定、管理は基本的に「D-Link Business Cloud」を使用して行いますが、一部の設定は、機器に実装されている Web ベース (HTML) インタフェース経由で手動設定することができます。標準的なブラウザを使用してネットワーク上のリモートステーションから本製品を管理できます。ブラウザがシンプルなアクセスツールの役割をし、HTTP プロトコルを使用して直接通信することが可能です。Web ベースの管理モジュールとコンソールプログラム (CLI) は、異なるインタフェースを経由して同じクラウド AP 内部のソフトウェアにアクセスし、その設定を行います。

Web GUI への接続

ここでは D-Link の Web ベースインタフェースの利用方法について説明します。

接続前の準備

1. 管理する PC のプロキシサーバ機能を無効にします。Windows の「スタート」-「コントロールパネル」-「インターネットオプション」-「接続」タブ-「LAN の設定」の順にクリックし、「LAN にプロキシサーバを使用する」のチェックを外します。
2. 使用する Web ブラウザのポップアップブロックが無効になっていることを確認してください。ポップアップブロックが有効な場合、画面が開けない場合があります。

有線で接続する場合

DBA-1510P を管理する PC とイーサネットケーブルで直接接続、または同じスイッチもしくはルータに接続します。

無線で接続する場合

管理側 PC から無線で DBA-1510P に接続する場合は、ブラウザのアドレス欄に DBA-1510P のホスト名を入力し、Enter を押下します。ホスト名の初期値は「DBA-1510P-XXXX」で、XXXX は DBA-1510P の底面にあるデバイスラベルに記載されている MAC アドレスの最後の 4 ケタになります。

Web GUI 設定画面へのログイン

ここでの DBA-1510P の設定は AP に直接アクセスした PC から行います。ここでは、Windows OS で動作する画面で説明します。手順と画面は、他の Windows OS についても同じです。

1. Web ブラウザ (Google Chrome) を起動します。
2. Web ブラウザのアドレス欄に DBA-1510P のホスト名を入力し、「Enter」キーを押下します。「DBA-1510P のホスト名」は「DBA-1510P-XXXX」となっていて「XXXX」には機器背面に貼付されている MAC アドレスの 4 ケタの数字になります。
3. 接続に成功すると、以下のログイン画面が表示されます。

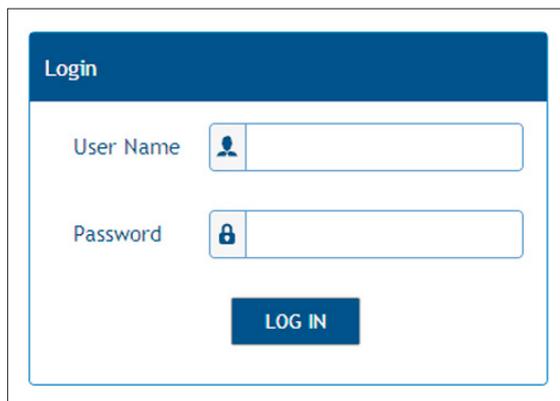


図 4-1 LOGIN 画面

4. 「User Name」(ユーザ名)と「Password」(パスワード)に「admin/admin」または「admin/password」を入力し、「ログイン」ボタンをクリックします。

ステータス（クラウド AP の手動設定）

「ステータス」では「ネットワーク状態」「クラウド接続状況」「機器についての情報」など DBA-1510P についての様々な情報を参照できます。以下の画面でステータスページでの項目や設定オプションについて説明します。

The screenshot shows the 'Status' page for a D-Link Business Cloud Access Point (DBA-1510P). The page is divided into sections: '概要' (Summary), 'ネットワーク状態' (Network Status), and 'インターネット' (Internet). The '概要' section lists device information such as Access Point Name (DBA-1510P), MAC Address, Serial Number, and Firmware Version (1.01b03). It also shows the Device UID, Cloud Registration Status (Yes), and Registration Date (2015-4-16). The 'ネットワーク状態' section indicates successful connections to the local network, internet, and cloud. The 'インターネット' section shows successful internet connection details including IP address, mask, default gateway, primary DNS, and secondary DNS.

図 4-2 ステータス画面

本画面には以下の項目があります。

項目	説明
概要	
アクセスポイント名	機器名
MAC アドレス	機器の MAC アドレス (例: C0:A0:BB:6E:0A:B3)
シリアル番号	機器のシリアル番号
ファームウェアバージョン	現在のファームウェアバージョン
デバイス UID	「D-Link ビジネスクラウド」で使用される機器の ID
IP アドレス (クラウド)	イーサネット IP アドレス
クラウド登録状態	「D-Link ビジネスクラウド」の登録状況について <ul style="list-style-type: none"> • Yes - D-Link ビジネスクラウドに登録済みです。 • No - D-Link ビジネスクラウドに未登録です。
登録日	「D-Link ビジネスクラウド」の登録日
ネットワーク状態	
ローカルネットワーク	ローカルネットワークでの接続状況
インターネット	インターネットへの接続状況
クラウドへの接続	「D-Link ビジネスクラウド」への接続状況

一般設定 (クラウド AP の手動設定)

「一般設定」では接続したクラウド AP の「IP アドレス」「接続タイプ」「DNS サーバ」「管理 VLAN」「タグ VLAN」の設定や「ファームウェアの更新」が行えます。

The screenshot shows the 'General Settings' (一般設定) page for a D-Link Business Cloud AP. The interface includes the following sections and fields:

- IP アドレス**: IP address field.
- 接続タイプ**: Connection type dropdown menu, currently set to 'DHCP'.
- DNS サーバ**: DNS server settings. Includes radio buttons for '自動取得' (selected) and '手動で指定する'. Below are two input fields for IP addresses, both set to '0.0.0.0'.
- 管理 VLAN ID**: Management VLAN ID input field, set to '1'.
- VLAN 有効**: VLAN enabled checkbox, currently unchecked.
- VLAN モード**: VLAN mode radio buttons for 'タグ付き' and 'タグなし' (selected).
- NTP サーバ 1/2/3**: Three input fields for NTP server addresses: 'ntp1.dlink.com', 'ntp.dlink.com.tw', and '0.jp.pool.ntp.org'.
- IPv6 有効**: IPv6 enabled radio buttons for '有効' (selected) and '無効'.
- 保存 & 再起動** or **キャンセル**: Save and restart or cancel buttons.
- ファームウェア更新**: Firmware update section. Shows '現在のファームウェアバージョン' as '1.01b03'. Includes a '参照' (Browse) button and an '更新' (Update) button. A dashed box indicates where to drag and drop the firmware file.
- プロキシ設定**: Proxy settings section. Includes a 'プロキシ有効' checkbox (unchecked), and input fields for 'ホスト' and 'ポート' (set to '80'). A '保存' (Save) button is at the bottom.

図 4-3 一般設定画面

本画面には以下の項目があります。

項目	説明
IP アドレス 接続タイプ	接続の種類です。 「DHCP」を選択するとアクセスポイントは自動的に DHCP サーバから IP アドレス、サブネットマスク、DNS そしてゲートウェイを取得します。 「スタティック IP」を選択すると IP アドレス、サブネットマスク、デフォルトゲートウェイなどの情報を手動で設定する必要があります。
DNS サーバ	DNS のモードについて選択します。 「自動取得」では DNS の IP アドレスは DHCP サーバから自動的に付与されます。このオプションは「接続タイプ」で「DHCP」を選択した時のみ設定可能です。「手動で指定する」ではドメイン名の設定について手動で IP アドレスを指定する必要があります。
管理 VLAN ID	「管理 VLAN」は本機器にアクセスするために使用する IP に関連した VLAN です。 「管理 VLAN ID」の初期値は「1」です。ID は「1」から「4094」まで指定可能です。
VLAN 有効	VLAN を有効にする場合はチェックを入れます。
VLAN モード	VLAN のタグ付け / タグなしを選択します。 <ul style="list-style-type: none"> 「タグ付き」- タグ付き VLAN を有効にします。 「タグなし」- タグなし VLAN を有効にします。
NTP サーバ 1/2/3	機器が接続する NTP サーバを指定します。1～3 まで指定可能です。
IPv6 有効	IPv6 を有効 / 無効にします。
ファームウェア更新	「現在のファームウェアバージョン」で現在適応中のファームウェアバージョンを確認できます。 新しいファームウェアイメージを保持している場合、「参照 (Browse)」ボタンをクリックしイメージファイルの場所を指定します。または「ここにドラッグ & ドロップでファームウェア更新」でファームウェアファイルをドラッグ & ドロップし、指定することも可能です。 「更新」をクリックすると新しいファームウェアイメージの適用を開始します。「更新」をクリックするとアップグレードに関する確認と説明を行うダイアログが表示されます。「OK」をクリックしてアップグレードを開始してください。
プロキシ有効	チェックを入れるとプロキシを有効にします。 「ホスト」「ポート」に適応するプロキシ情報を入力し、「保存」をクリックして適応します。

設定の変更については「保存 & 再起動」をクリックし設定を保存、再起動で設定を適用します。

注意

ファームウェアバージョンは、D-Link ビジネスクラウド側（管理 > 概要）での各デバイスグループのファームウェアバージョン）の設定と合わせる必要があります。ファームウェアバージョンが合致していない場合、クラウド側のバージョンが優先されます。

コマンドラインインタフェース (CLI) の設定

ここでは、D-Link Business Cloud を使用せずに DBA-1510P へ直接接続、設定をするコマンドラインインタフェース (CLI) について説明します。

コンソールポートへの接続

クラウド AP である DBA-1510P の設定、管理は基本的に「D-Link Business Cloud」を使用して行いますが、一部の設定は、機器に実装されている CLI を使用しての設定が可能です。そのための RJ-45 コンソールポートを搭載しています。コンソールポートを使用するためには、以下をご用意ください。

- ・ ターミナルソフトを操作するシリアルポート搭載の端末またはコンピュータ
- ・ 同梱の RJ-45/RS-232C 変換ケーブル

端末をコンソールポートに接続する

1. 同梱の変換ケーブルのオス RS-232 コネクタを端末またはターミナルソフトが動作するコンピュータのシリアルコネクタに接続、次に RJ-45 コネクタを製品のコンソールポートに接続します。
2. 以下の手順でターミナルソフトを設定します。
3. 「接続の設定」画面の「接続方法」で、適切なシリアルポート (COM ポート) を選択します。
4. 選択したポートの「プロパティ」画面で「115200」ビット / 秒にデータ速度を設定します。
5. 「データビット」は「8」、「ストップビット」は「1」、「パリティ」は「なし」に設定します。
6. 「フロー制御」は「なし」に設定します。
7. 「エミュレーションモード」を「VT100」に設定します。
8. 「ファンクションキー」、「方向キー」、「Ctrl キー」の使い方で「ターミナルキー」を選択します。「ターミナルキー」(Windows キーではない) の選択を確認します。

注意 Microsoft® Windows® 2000 でハイパーターミナルを使用する場合は、Windows 2000 Service Pack 2 以降がインストール済みであることを確認してください。Windows 2000 Service Pack 2 以降でないとハイパーターミナルの VT100 端末で矢印キーは使用できません。Windows 2000 service pack に関する情報はマイクロソフト社のホームページでご確認ください。

9. 端末設定の完了後、本製品に電源ケーブルを接続し、電源プラグをコンセントに接続します。端末でブートシーケンスが始まります。
10. ブートシーケンスが完了すると、コンソールのログイン画面が表示されます。
11. 購入後はじめてログインする場合は、ユーザ名 (User Name) プロンプトで「admin」を入力し、「Enter」キーを押します。本製品には、パスワード (Password) の初期値はありません。既にユーザアカウントを作成している場合は、ユーザ名 (User Name) とパスワード (Password) を入力してログインし、続けて本スイッチの設定をします。
12. コマンドを入力して設定を行います。コマンドの多くは管理者レベルのアクセス権が必要です。次のセクションでユーザアカウントの設定について説明します。
13. 管理プログラムを終了する場合は、logout コマンド使用するか、ターミナルソフトを終了します。

端末上で接続に問題が発生した場合は、ターミナルソフトの設定で「エミュレーション」が「VT-100」となっていることを確認してください。「エミュレーション」は「ハイパーターミナル」画面の「ファイル」メニューから「プロパティ」をクリックし、「設定」タブにて設定します。何も表示されない場合はスイッチの電源を切り、再起動してください。

コンソールに接続すると、コンソール画面が表示されます。ここでコマンドを入力し、管理機能を実行します。

CLI コマンド一覧

以下の CLI コマンドを使用してネットワークの状態やクラウドの接続状況など様々な情報を参照することが可能です。全てのパラメータでコマンドの適用には「apply」が必要になります。CLI へのログインはユーザ名/パスワードともに「admin」を入力します。

基本コマンド

コマンド	動作
get system	システム情報について表示します。
get system model	モデル名について表示します。
get management mac	MAC アドレスを表示します。
get system serial-number	シリアル番号について表示します。
get system version	ファームウェアバージョンについて表示します。
get configured-mode	設定モードについて表示します。
get system device-uid	機器の UID について表示します。
get management ip	イーサネット IP アドレスについて表示します。
get system cloud-registration	システムクラウド登録情報について表示します。
get system date-of-registration	クラウド登録日について表示します。
get system local-network-status	ローカルネットワークの状況について表示します。
get system internet-status	インターネットの状況について表示します。
get system cloud-connect-status	接続状況について表示します。

アクセスポイントのローカル設定コマンド

動作	コマンド
get management	現在の有線インターナルインタフェースの状況について表示します。
get management dhcp-status	DHCP の接続状況について表示します。
set management dhcp	接続方法について DHCP を選択します。
set management static	接続方法について手動 (Static IP) を選択します。
static-ip ip_address mask netmask gateway ip_address	スタティック IP、サブネットマスク、デフォルトゲートウェイ
get host	DNS の設定情報を表示します。
get host dns-via-dhcp	DNS を DHCP で取得したのか、スタティックに設定されたのかを表示します。
get host dns	設定されている DNS 名を表示します。
set host static-dns-1 ip_address	DNS 名にスタティック IP アドレスを使用します。
set host static-dns-1 ip_address static-dns-2 ip_address	
set host dns-via-dhcp {up down}	DNS 名に DHCP IP アドレスを使用します。
get management vlan-id	VLAN についての情報を表示します。
get management vlan-tagging-enable	
get management vlan-tagging-mode	
set management vlan-tagging-enable {up down}	VLAN タグを有効 / 無効にします。
set management vlan-id value	「VLAN ID」を表示します。
set management vlan-tagging-mode {tagged untagged}	VLAN モードを有効 / 無効に指定します。
get management ipv6-enable	IPv6 設定を表示します。
get management proxy-enable	プロキシ設定を表示します。
get management proxy-host	プロキシのホスト設定を表示します。
get management proxy-port	プロキシのポート設定を表示します。
set management ipv6-enable	ローカル GUI アクセス用の IPv6 インターフェースを有効 / 無効にします。
set management proxy-enable	プロキシ設定を有効 / 無効にします。
set management proxy-host	プロキシのホストの設定をします。
set management proxy-port	プロキシのポートの設定をします。
apply	設定を適用します。
exit	コマンドラインからログアウトします。
reboot	システムを再起動します。

第5章 D-Link Business Cloud 概要

- D-Link Business Cloud について
- D-Link Business Cloud 対応機器
- D-Link Business Cloud 基本仕様
- ライセンス形態について

ここでは、「D-Link Business Cloud」の概要、対応機器、基本仕様、設定可能な機能やライセンス形態について説明します。

D-Link Business Cloud について

D-Link Business Cloud (以下、クラウド) は、クラウドからネットワーク機器を管理・監視することができるクラウド型のサービスです。クラウド対応ネットワーク機器は、クラウドとの間で管理用トンネルセッションを維持し、クラウド経由でのポリシー設定、モニタリング、ファームウェアのアップデートなどを実施することができるため、ネットワーク管理者は、クラウド経由でネットワーク機器のオペレーションをすることができます。

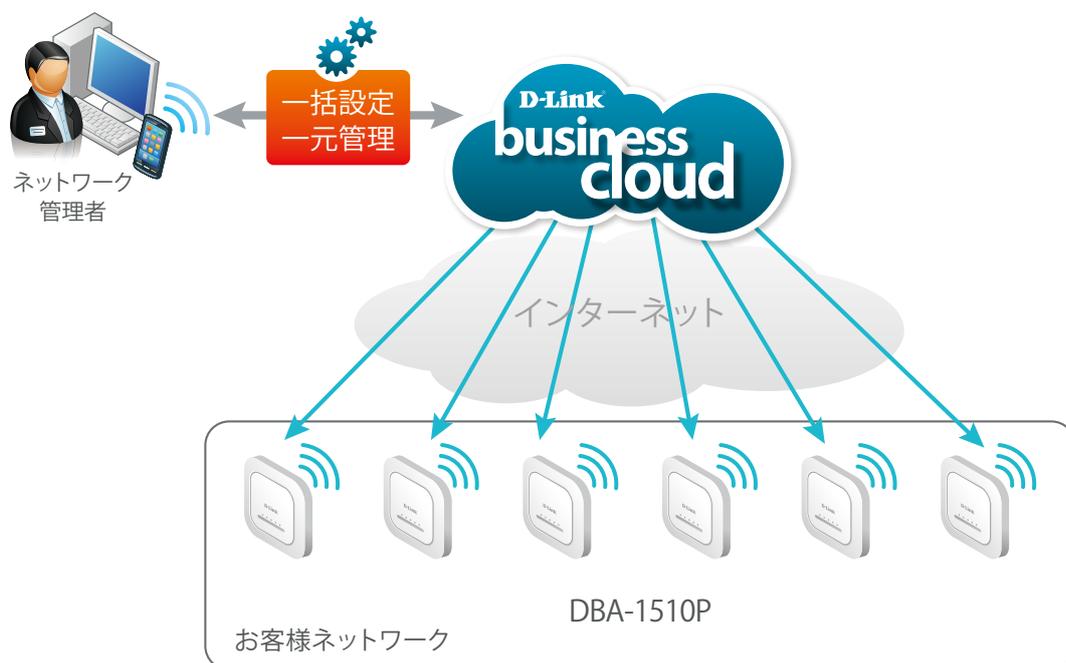


図 5-1 D-Link Business Cloud 概要

D-Link Business Cloud 対応機器

D-Link Business Cloud では以下の機器をサポートしています。

DBA-1510P (802.11a/b/g/n/ac 対応 デュアルバンドアクセスポイント)

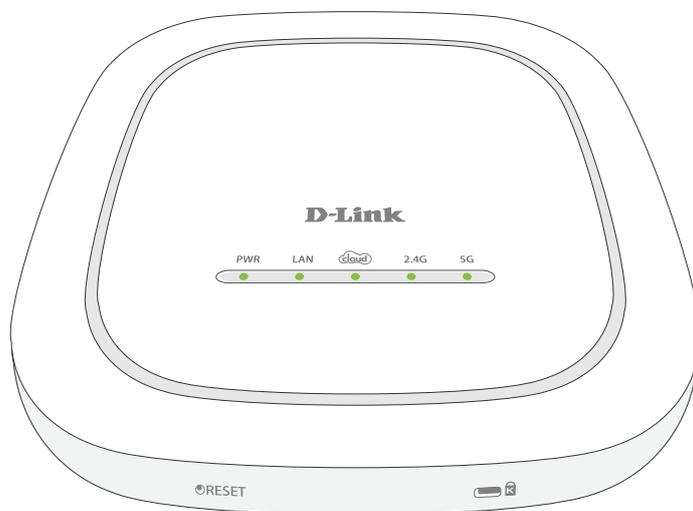


図 5-2 DBA-1510P 外観図

D-Link Business Cloud 基本仕様

クラウド AP である DBA-1510P は、リンクアップをし IP アドレスを取得するとクラウドとの間で SSL セッションを確立します。この時点で DBA-1510P とクラウドとの間で、「TCP : 443 ポート」と名前解決のための DNS が許可されている必要があります。DBA-1510P がクラウドとの接続を完了すると、クラウドに設定済みのファームウェア、コンフィグレーションの同期が自動的に開始されます。この処理が終了すると、DBA-1510P はクラウド AP として動作を開始します。クラウド管理用 SSL セッションは維持され、クラウドからのモニタリング、設定変更、ファームウェアのバージョンアップなど、クラウドから DBA-1510P を管理する用途で利用されます。

クラウド利用にあたり、ルータ / Firewall で以下がご利用可能かどうかご確認下さい。

プロトコル	用途・備考
TCP 80 (HTTP)	ファームウェアのアップデート用
TCP 443 (SSL)	クラウドサーバとの通信用
UDP 123 (NTP)	スケジュール機能及びモニタ機能用

以下の 3 つのプロトコルもまた許可されている必要があります。

プロトコル	用途・備考
UDP 67 (DHCP)	Static IP を使った場合は不要
UDP 53 (DNS)	
TCP 53 (DNS)	

「D-Link Business Cloud」でサポートされている主な機能は下記の通りとなります。

デバイス・グルーピング

- ・ デバイスグループの作成
- ・ タグの作成
- ・ 管理グループの作成

コンフィグレーション管理

- ・ SSID プロファイル設定
- ・ 無線設定
- ・ RADIUS 設定
- ・ キャプティブポータル
- ・ プッシュ設定 (コンフィグレーションの配信)
- ・ デバイスの設定 (デバイス個別設定)

モニタリング機能

- ・ 概要 (Top10 リスト)
- ・ クラウド AP のモニタリング
- ・ 無線 LAN クライアントのモニタリング
- ・ 地図とフロアマップ
- ・ 不正 AP (クラウド AP が検知したクラウド管理外の無線 LAN アクセスポイント)
- ・ ホワイトリスト (クラウド AP が検知したクラウド管理外の無線 LAN アクセスポイントだが、管理者が許可しているアクセスポイント)
- ・ イベント
- ・ 指定クラウド AP の LED (クラウド) を点滅させる機能
- ・ Ping (指定ホストへクラウド AP から Ping する機能)
- ・ Traceroute (指定ホストへクラウド AP から Traceroute する機能)
- ・ 再起動
- ・ 環境 (近隣アクセスポイントをスキャン・検出する機能)
- ・ クラウド UI からの IP アドレス変更
- ・ 筐体毎の無線設定
- ・ 筐体毎の SSID 設定

管理機能

- ・ 組織全体の管理
- ・ デバイスグループの管理
- ・ 登録デバイスの管理
- ・ タグの管理
- ・ 管理者権限の管理
- ・ クラウドライセンスの管理
- ・ ログの管理

メンテナンス機能

- ・ MAC アドレスフィルタリング機能のデータベース設定
- ・ キャプティブポータルの Web 認証用ページの編集
- ・ ファームウェアアップデートポリシーの設定
- ・ 設定ポリシーの複製機能

デバイス・グルーピングについて

D-Link Business Cloud において「デバイス」は「クラウド AP (DBA-1510P)」、「デバイスグループ」はクラウド AP (DBA-1510P) の集合体を意味します。D-Link Business Cloud では、管理するネットワーク機器をグループ化することで、管理性を向上させています。グループは、「デバイスグループ」「タグ」「組織」の3種類で構成され、各々役割が異なります。D-Link Business Cloud で管理されるネットワーク機器は、グルーピングの最小単位であるデバイスグループに所属する必要があります。デバイスグループには、タグを自由に付与することができ、デバイスグループに複数のタグを付与する事も可能です。デバイスグループとタグは、特定の1つの管理グループ「組織」に所属します。「デバイスグループ」「タグ」「組織」の相関関係は、下図の通りとなります。

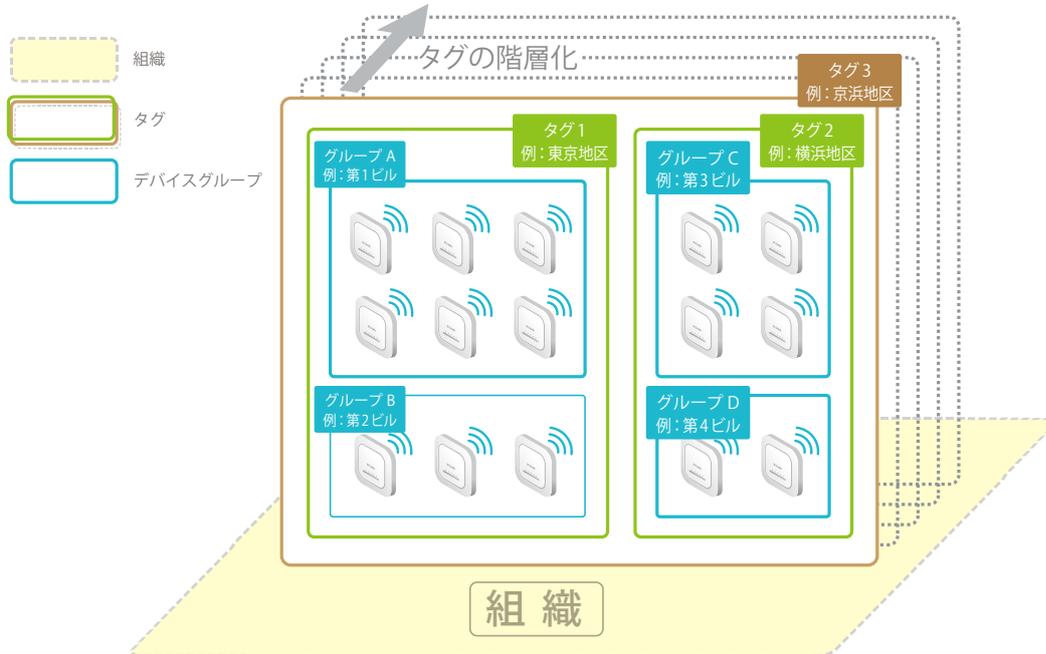


図 5-3 デバイス・グルーピング概要

- デバイスグループは、グループの最小単位で、同一デバイスグループに、異なる機種を所属させる事はできません。設定情報、ファームウェアのアップデートスケジュールはデバイスグループ内で共有されます。
- タグは、デバイスグループに自由に付与することができます。デバイスグループに複数のタグを付与することができるため、階層的にタグを管理することができます。クラウドを使用するための権利(ライセンス)は、1つの組織に登録・適用されます。

グループ種別	内容・特徴
デバイスグループ	<ul style="list-style-type: none"> • グループの最小単位 • 同一機種のみ所属 • 設定情報ポリシーを保持 • F/W ポリシーを保持 • 最大管理デバイス登録数：100
タグ	<ul style="list-style-type: none"> • デバイスグループに付与 • 階層的な付与が可能
組織	<ul style="list-style-type: none"> • ライセンスポリシーを保持 • 最大管理者数：100

設定の管理について（設定）

D-Link Business Cloud では、デバイスグループに対して Wi-Fi ポリシーの設定を行います。同一のデバイスグループに所属するクラウド AP には、デバイスグループに適用された同一の Wi-Fi ポリシーが適用されます。Wi-Fi ポリシーの設定はクラウドの「設定」メニューで行うことが可能です。デバイスグループを選択し、既存のデバイスグループを切り替えて設定を行います。デバイスグループ内のデバイスへの設定の適用には設定の配信（プッシュ設定）を行う必要があります。以下はクラウドで行うことが可能な設定管理の主な内容になります。

■ SSID プロファイルの作成、設定（設定 > SSID プロファイル）

デバイス（クラウド AP）上の SSID の作成、設定を行います。

■ 無線設定（設定 > 無線設定）

デバイスグループの内のデバイス（クラウド AP）に対しチャンネルや無線出力の設定を行います。

■ RADIUS サーバの設定（設定 > RADIUS 設定）

新規 RADIUS サーバの追加、既存・新規 RADIUS サーバの設定編集、そして RADIUS サーバの状況や設定情報の表示などを行います。

■ LDAP サーバの設定（設定 > LDAP 設定）

新規 LDAP サーバの追加、既存・新規 LDAP サーバの設定編集、そして LDAP サーバの状況や設定情報の表示などを行います。

■ キャプティブポータル作成、編集（設定 > キャプティブポータル）

無線クライアントのユーザによるクラウド AP へのアクセスの前に、Web ページ（スプラッシュページ）を経由させ、アクセスの前に指定の情報をユーザに表示、対応させる機能です。

■ DHCP プール設定（設定 > DHCP プール設定）

NAT モードで利用するための DHCP アドレスプールの設定を行います。

■ ユーザ名とパスワードの設定（設定 > 一般設定）

ユーザ名とパスワードの設定を行います。

■ コンフィグレーションの配信（設定 > プッシュ設定）

ビジネスクラウドに保存されたデバイス（クラウド AP）の設定を、デバイスグループ内のすべてのデバイスに適用します。

■ 各デバイス（クラウド AP）の個別設定（設定 > デバイスの設定）

デバイスグループ内のデバイス（クラウド AP）の状態や使用率などを確認することができます。加えて各デバイス（クラウド AP）の設定も個別に行う事が可能です。

モニタ機能について（モニタ）

D-Link Business Cloud では、管理下のクラウド AP、近隣無線 LAN アクセスポイント、無線 LAN クライアントのモニタリング機能を利用することができます。クラウドの「モニタ」メニューでデバイス（クラウド AP）やクライアント、デバイスグループ、タグ、登録 / 未登録ユーザの動作状況や動作履歴を表示します。統計や警告などの情報をフロアマップなどでデバイス（クラウド AP）の位置などを視覚的に確認することも可能です。以下はクラウドで行うことができるモニタ機能の主な内容です。必要に応じて、設定 / 変更 / 修正を行ってください。

■デバイスグループの概要（モニタ > 概要）

選択されたデバイスグループシステムの詳細 / 概要を表示します。

■地図とフロアマップの表示（モニタ > 地図とフロアマップ）

デバイス（クラウド AP）の物理的な設置場所や設置要件を視覚的に表示します。無線クライアントの物理的な設置場所やデータ消費環境などを、ネットワーク管理者が把握することができます。

■デバイス（クラウド AP）の状態を確認（モニタ > デバイス）

デバイスグループ内のデバイス（クラウド AP）について状態や使用率などを確認します。

■クライアントの確認（モニタ > クライアント）

デバイスグループのデバイス（クラウド AP）に帰属している無線 LAN クライアントを確認します。

■不正 AP の確認（モニタ > 不正 AP）

不正が疑われる近隣のアクセスポイントの情報を表示します。

■発生イベントの確認（モニタ > イベント）

デバイスグループ内で発生したイベントについて表示します。

■レポートのダウンロード（モニタ > レポート）

デバイス（クラウド AP）単位やデバイスグループ単位でのログを CSV 形式のファイルでダウンロードします。

管理機能について（管理）

D-Link Business Cloud の管理上のタスクを実行します。

組織やデバイスグループ、デバイス（クラウド AP）の情報の表示やグループの作成やデバイス（クラウド AP）の登録、削除などとともに、デバイスグループへのタグ付与、管理者の管理と権限内容の編集などを行います。デバイスグループやタグにも関連した権限を付与することが可能です。更にライセンスの確認、履歴、ライセンス追加なども管理機能として有しており、システムログの詳細について表示、ダウンロードなども行うことが可能です。

以下はクラウドで行うことが可能な管理機能の主な内容になります。

■クラウドの主な情報表示（管理 > ダッシュボード）

組織の重要な情報などをサマリ形式で確認することができ、更にデバイスグループの作成やデバイス（クラウド AP）の登録など管理上のタスクなどを実行することも可能です。（D-Link Business Cloud の初期画面になります。）

■デバイスグループの概要表示（管理 > 概要）

デバイス（クラウド AP）数、ファームウェアバージョン、グループのパラメータを含むデバイスグループの主要な情報を表示します。

■各デバイス（クラウド AP）の表示、設定（管理 > インベントリ）

登録済のデバイス（クラウド AP）の一覧とその情報を表示します。デバイス（クラウド AP）の事前登録、読み込み、削除なども可能です。

■タグの付与（管理 > タグ）

様々な方法や形式でデバイスグループにタグを付与することができます。

■管理者と権限の設定（管理 > Admin 管理）

クラウドの管理者とその権限内容について管理します。デバイスグループやタグにも関連した権限を付与することが可能です。

■ライセンスの設定（管理 > ライセンス）

組織に紐づいているライセンス状態の確認、ライセンス履歴、ライセンス追加などを行います。

■システムログのダウンロード（管理 > システムログ）

ビジネスクラウドのデバイスグループ内で発生したイベント（システムログ）の詳細について表示、CSV ファイル形式でのダウンロードを行います。

■組織の管理（管理 > 組織設定）

組織についての管理項目です。組織の状態を確認、組織の削除なども行います。

メンテナンス機能について（メンテナンス）

D-Link Business Cloud のメンテナンス機能として MAC アドレスリストによる認証管理やキャプティブポータル用のスプラッシュページ作成、フォームウェアの管理、設定の複製などを行います。

以下はクラウドで行うことが可能なメンテナンス機能の主な内容になります。

■MAC アドレスリストによる SSID でのアクセス認証（メンテナンス > MAC データベース）

特定のデバイスグループの SSID プロファイルに MAC アドレスのリストを設定し、MAC アドレスでのアクセス認証を SSID に適用します。

■キャプティブポータル用スプラッシュページ（メンテナンス > スプラッシュページ編集）

キャプティブポータルなどで使用するスプラッシュページの作成、編集または削除を行います。

■ファームウェアアップグレード（メンテナンス > ファームウェア）

デバイス（クラウド AP）の新しいファームウェアをアップグレードできます。「ファームウェア管理」ではファームウェアのアップグレードとともに、対応可能なファームウェアバージョンの選択などを行います。

■デバイスグループ間の設定の複製（メンテナンス > 設定の複製）

デバイスグループで設定した設定内容（グループコンフィグ）を他のデバイスグループ（新規 / 既存）にも適用します。

ライセンス形態について

D-Link Business Cloud のご利用にあたっては、ライセンスのご購入が必要となります。ライセンスは DBA-1510P の機器価格に含まれています。概念：クラウドライセンスは、ビジネスクラウドを使用するにあたり、使用許諾をお客様に付与するものです。

注意 ライセンスが無いと、クラウドおよび AP は利用できません。継続してご利用になる場合、ライセンスの有効期限が来る前に、ライセンスを購入し、更新する必要があります。ライセンスが有効期限を迎える「2 か月前」「1 か月前」「7 日前」「3 日前」「1 日前」に管理者に E-mail で通知します。

DBA-1510P 機器・ライセンス一覧

	型番	仕様
機器	DBA-1510P	D-Link Business Cloud 対応 11ac (3 ストリーム) 無線 LAN アクセスポイント ※ 別途クラウド用有償ライセンスの購入が必要
バンドル用ライセンス	DBA-1510P-LC1	DBA-1510P 本体と同時発注時限定 ライセンスパッケージ (1 年間 / 65 ポイント分)
	DBA-1510P-LC2	DBA-1510P 本体と同時発注時限定 ライセンスパッケージ (2 年 / 125 ポイント分)
	DBA-1510P-LC3	DBA-1510P 本体と同時発注時限定 ライセンスパッケージ (3 年 / 185 ポイント分)
	DBA-1510P-LC4	DBA-1510P 本体と同時発注時限定 ライセンスパッケージ (4 年 / 245 ポイント分)
	DBA-1510P-LC5	DBA-1510P 本体と同時発注時限定 ライセンスパッケージ (5 年 / 305 ポイント分)
個別用ライセンス	DBA-1510P-LCR	追加一括更新用パッケージライセンス ※ 年単位での更新用パッケージ (60 ポイント分)
	DBC-LCP	追加用ポイント ※ 短期延長用の 1 ポイントから購入可能なライセンス

Organization とライセンス Key およびポイントについて

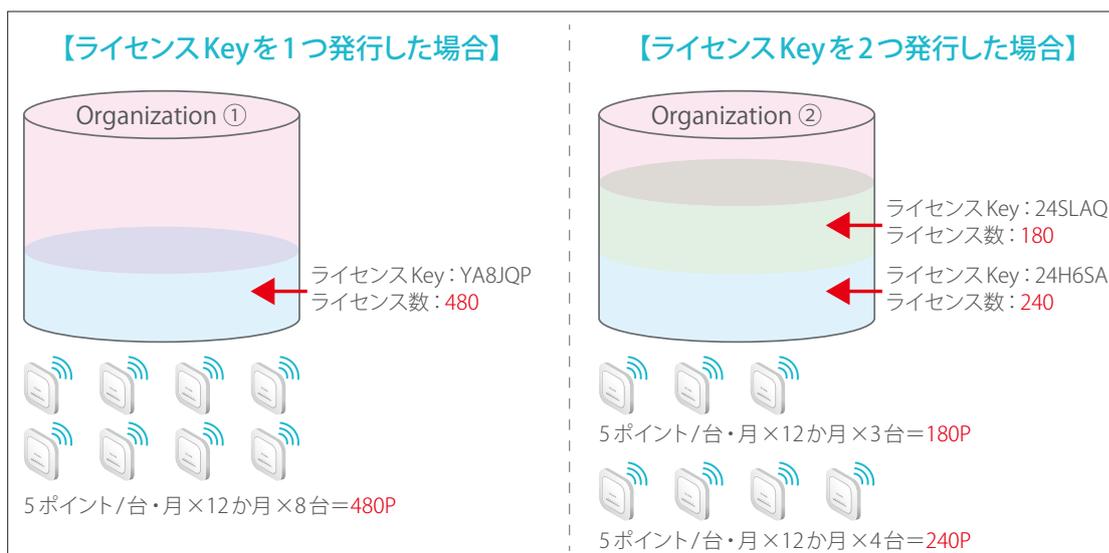


図 5-4 Organization とライセンス Key およびポイント

- ① Organization に対して、ライセンス Key を登録。
- ② ライセンス Key はユニーク。異なる Organization で共有不可。
- ③ Organization 配下の AP は、ライセンス Key と紐づいたポイント数を消費。

- Organization はポイントを貯めておくバケツのようなもの。
- ライセンス Key 単位でのポイント追加

Organization 単位でのグループライセンス方式

Organization 単位でのグループライセンス方式を採用しており、クラウド利用期間は Organization 内の AP 全てで共有されます。

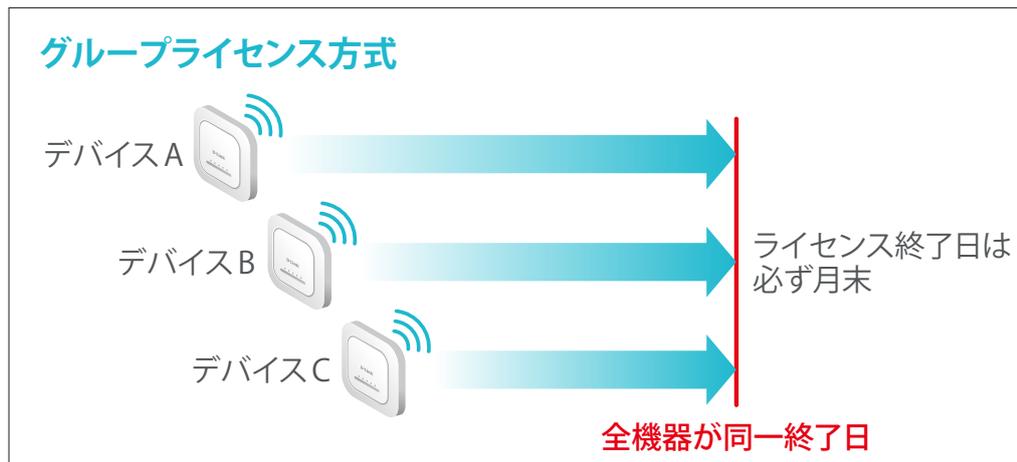


図 5-5 Organization 単位でのグループライセンス方式

① 同じ Organization 所属の機器は、有効期限は全て同じ日で終了。

② DBA-1510P は 1 台あたり月 5 ポイント消費されます。

③ 毎月月末に、以下の処理が行われます。

(1) 当月使用ポイントを、総ポイントから差し引きます。

(2) 翌月必要ポイントが不足している場合、継続してご利用になる際は、ライセンスの有効期限が来る前にライセンスを購入し、更新する必要があります。

※ 管理者の方には事前にアラートメールが送信されます。

月ごとのポイント計算の仕組み

・ 計算方法：「月間消費ポイント＝月間利用台数×月間利用ポイント×（月間のべ利用日数合計） / （月間利用台数×計算月日数）」

※ 原則小数点以下は切り捨て

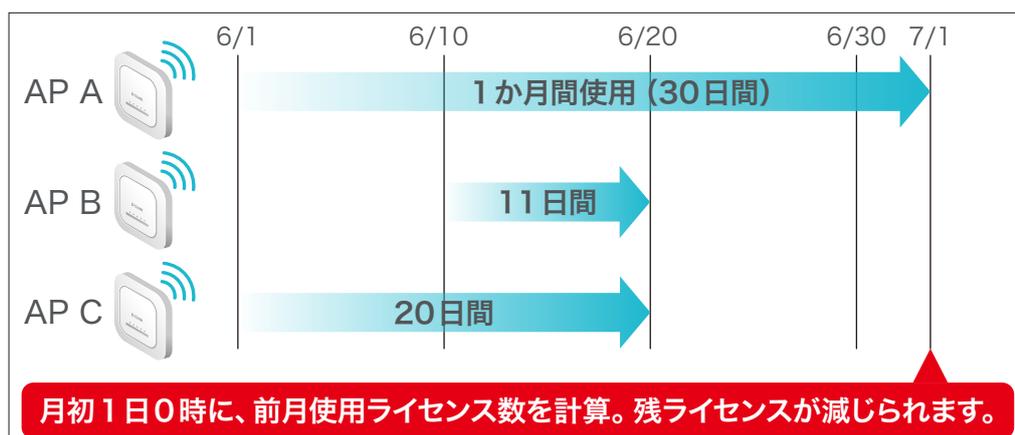


図 5-6 同月内で開始日が異なる 3 台のポイント計算例

AP	AP 使用期間	月間使用ポイント
A	30日間	5
B	11日間	1.83
C	20日間	3.33
	のべ61日間	10ポイント

図 5-7 1 ヶ月間、複数台を異なる開始時から利用した場合の計算式

3 台 × 5 ポイント × (30 日 + 11 日 + 20 日) / (3 台 × 30 日) = 10.1667 ポイント

※ 原則小数点以下は切り捨て

第 6 章 クラウドの基本設定（D-Link Business Cloud）

本章では D-Link Business Cloud の運用上、基本となる設定、操作手順について説明します。

- クラウドユーザインタフェースについて
- クラウドアカウントの作成とライセンスの登録
- デバイスグループの作成
- デバイスの登録
- Wi-Fi ポリシーの設定
- アクセスポイントのクラウドへの接続
- 設定の変更
- ログインユーザの詳細設定

クラウドユーザインタフェースについて

D-Link Business Cloud にログイン後、クラウドインタフェースでの管理画面にアクセスし、パフォーマンス状況やシステム状態をグラフィック表示で参照できます。以下の画面はクラウドインタフェース上部に常に表示される項目です。



図 6-1 クラウドインターフェース画面

次の表では「クラウドインターフェース」について説明します。

項目	説明
①メニュー情報	現在表示しているメニュー画面になります。
②組織	現在表示している組織になります。右横の「▼」をクリックすると、他の組織を選択、または新しい組織を作成することができます。
③デバイスグループ	現在表示しているデバイスグループになります。右横の「▼」をクリックすると、他のデバイスグループを選択、または新しいデバイスグループやタグを作成することができます。
④設定メニュー	設定機能のメニュー項目になります。「モニター」「設定」「メンテナンス」「管理」の 4 項目があります。設定内容については各メニューに対応している各章を参照ください。
⑤ログインユーザ	現在ログインしているユーザになります。右横の「▼」をクリックすると、当該ユーザの「ユーザプロファイル」「権限」の設定、ログアウトなどができます。詳しくは「 ログインユーザの詳細設定 」を参照ください。
⑥言語	現在表示している言語になります。右横の「▼」をクリックすると、言語を変更できます。

注意 「D-Link Business Cloud」においてインタフェース上に表示される「デバイス」は、主に「DBA-1510P (クラウド AP)」を意味し、「デバイスグループ」も「DBA-1510P (クラウド AP)」のグループとなります。7 章からのメニュー設定以後の通称に関してはインタフェース表示に合わせ「デバイス」とのみ記載します。

注意 1 デバイスグループあたりの最大登録管理デバイス数は 100 です。

注意 1 組織あたりの最大管理者数は 100 です。

クラウドアカウントの作成とライセンスの登録

クラウドアカウントの作成とライセンスの登録を行います。

注意 「D-Link Business Cloud」の URL は、ライセンス証書をご確認下さい。

1. Web ブラウザで、「D-Link Business Cloud」の URL にアクセスし、下図「アカウントの新規作成」をクリックします。

図 6-2 ログイン（アカウントの新規作成）画面

2. 表示される必要項目を入力し、「アカウントの新規作成」をクリックして、D-Link Business Cloud の管理者アカウント作成します。パスワードは、10-16 文字以内で、大文字英字、小文字英字、数字を組み合わせる必要があります。

図 6-3 アカウントの新規作成 画面

以上の操作でアカウント作成は終了です。クラウドでのアカウント作成後、登録されたメールアドレスにクラウドから認証メールが送信されます。メール内に記載されたアクティベーション用の URL をクリックする必要があります。

ログイン

「D-Link Business Cloud」のログインについて説明します。

1. 「D-Link Business Cloud」ログイン画面にて、アクティベーション済みユーザアカウントのユーザ名、パスワードを入力し、「ログイン」をクリックします。



図 6-4 ログイン画面

2. ビジネスクラウド管理画面（ダッシュボード画面）が表示されます。

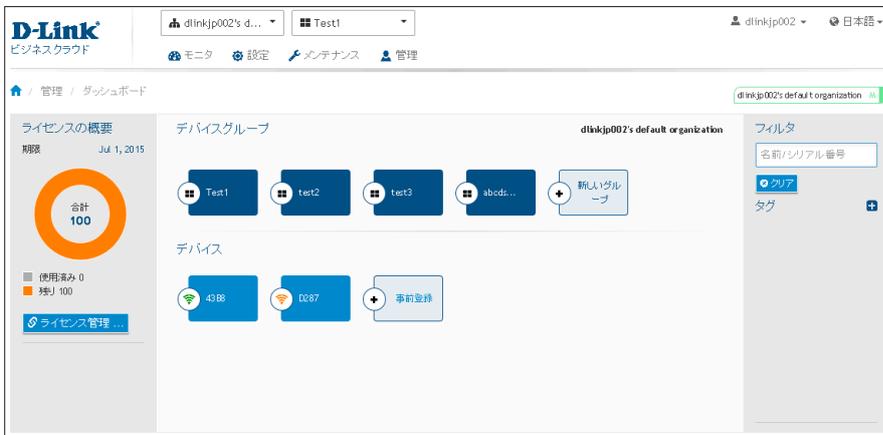


図 6-5 ビジネスクラウド管理画面（ダッシュボード画面）

注意 ブラウザ（Google Chrome）の設定により「サイトのパスワード保存」に関するダイアログが表示される場合がありますが、「使用しない」（保存しない）をクリックしてください。



図 6-6 パスワード保存の確認メッセージ

ライセンスの登録

アカウント作成後、ライセンスを登録します。

管理 > ライセンス > ライセンス追加をクリックし、以下の画面を表示します。



図 6-7 ライセンス追加画面

ライセンスキーを入力し、「ライセンス追加」をクリックする事でクラウドライセンスを登録は完了です。

デバイスグループの作成

デバイスグループを作成します。ここではデバイスグループの基本的な作成手順を説明します。

注意 1 デバイスグループあたりの最大 DBA-1510P 登録数は 100 です。

管理 > ダッシュボードをクリックし、以下の画面を表示します。

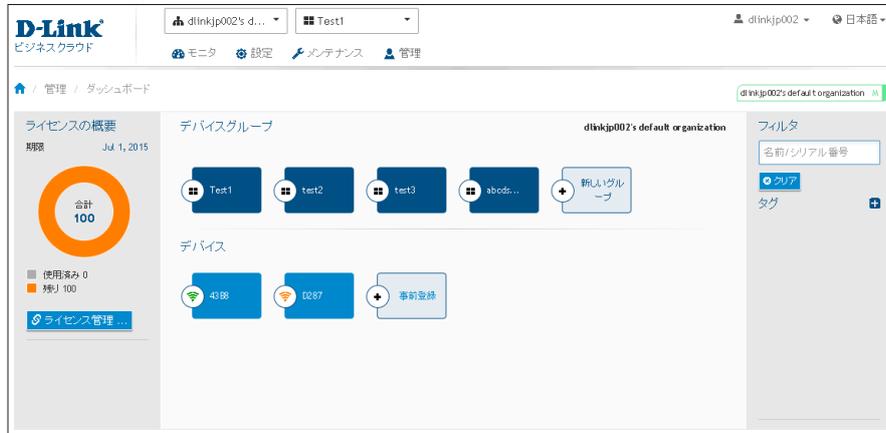


図 6-8 ダッシュボード画面

1. 「新しいグループ」を選択します。



図 6-9 新しいグループ（ダッシュボード）画面

2. 「デバイスグループ」に任意のデバイスグループ名を入力します。「モデル」には DBA-1510P を選択します。



図 6-10 新しいデバイスグループ画面

3. 作成したデバイスグループがダッシュボードに表示されている事を確認します。



図 6-11 作成デバイスグループ確認（ダッシュボード）画面

以上でデバイスグループの作成は終了です。

Wi-Fi ポリシーの設定

クラウド AP の Wi-Fi ポリシーを設定します。

ここではデバイスグループに設定する Wi-Fi ポリシーの基本的な設定手順を説明します。

1. 画面上部にて Wi-Fi ポリシーの設定を適用するデバイスグループを選択します。



図 6-12 デバイスグループ選択画面

2. 設定 > SSID プロファイルをクリックします。



図 6-13 SSID プロファイル選択画面

3. 既存の SSID の設定を編集します。または画面左下の「新しい SSID」をクリックし作成した SSID の設定を編集することも可能です。新しい SSID を作成する場合は「新しい SSID」をクリック、「SSID」に SSID 名、「バンド選択」で帯域を選択し、「保存」をクリックします。

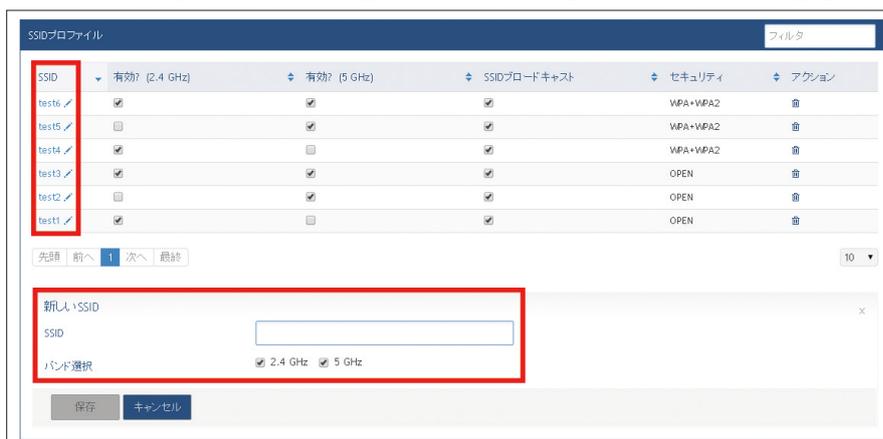


図 6-14 SSID プロファイル画面

4. リストに表示されている SSID 名をクリックします。「SSID プロファイル」「基本」画面が表示されます。基本設定として以下の項目を設定します。
 - ・「SSID」に任意の SSID 名を入力します。
 - ・「セキュリティ」にて無線のセキュリティ方式を選択します。

5. 選択したセキュリティ方式に基づき表示される項目を入力、選択します。

SSIDプロフィール

基本 MACフィルタリング IPフィルタリング スケジュール 高度な設定

SSID: SSIDプロフィール 1 - 32

VLAN有効

ゲストアクセスモード

NATモードを有効

バンド選択 2.4 GHz 5 GHz バンドステアリング

SSIDブロードキャスト

SSID内パーティション

キャプティブポータル: None

セキュリティ: WPA+WPA2

認証方式: PSK

暗号化方式: AES

事前共有鍵: 8 - 63

文字列を表示

グループキー更新間隔: 3600

URLリダイレクトを有効

保存 キャンセル SSIDプロフィールに戻る

図 6-15 セキュリティ (SSID プロファイル) 画面

6. 「保存」をクリックし、変更した設定をクラウドに保存します。

保存 キャンセル SSIDプロフィールに戻る

図 6-16 セキュリティ - 保存 (SSID プロファイル) 画面

7. 「スケジュール」タブを選択し SSID の有効・無効をスケジューリングすることができます。

SSIDプロフィール

基本 MACフィルタリング IPフィルタリング スケジュール 高度な設定

曜日の有効/無効

曜日	時刻の有効	時刻の無効	開始時刻	終了時刻
<input checked="" type="checkbox"/> 日曜日	<input type="checkbox"/> 時刻の有効	<input type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 月曜日	<input checked="" type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 火曜日	<input type="checkbox"/> 時刻の有効	<input type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 水曜日	<input type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 木曜日	<input type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 金曜日	<input type="checkbox"/> 時刻の有効	<input type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM
<input checked="" type="checkbox"/> 土曜日	<input type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 時刻の無効	12:00 AM	11:59 PM

12 : 00 AM

保存 キャンセル SSIDプロフィールに戻る

図 6-17 スケジュール (SSID プロファイル) 画面

下記のように設定することで、平日 7:00AM ~ 11:00PM の間だけ、当該 SSID を有効化する事ができます。

曜日の有効/無効	時刻の有効	終日	開始時刻	To	終了時刻
<input checked="" type="checkbox"/> 日曜日	<input checked="" type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 月曜日	<input checked="" type="checkbox"/> 時刻の有効	<input type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 火曜日	<input checked="" type="checkbox"/> 時刻の有効	<input type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 水曜日	<input checked="" type="checkbox"/> 時刻の有効	<input type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 木曜日	<input checked="" type="checkbox"/> 時刻の有効	<input type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 金曜日	<input checked="" type="checkbox"/> 時刻の有効	<input type="checkbox"/> 終日	7:00 AM	To	11:00 PM
<input checked="" type="checkbox"/> 土曜日	<input checked="" type="checkbox"/> 時刻の有効	<input checked="" type="checkbox"/> 終日	7:00 AM	To	11:00 PM

図 6-18 スケジュール設定 (SSID プロファイル) 画面

8. 設定を保存するときは必ず左下の「保存」をクリックします。保存をしないと変更した設定は適用されません。

図 6-19 スケジュール設定 - 保存 (SSID プロファイル) 画面

9. 「高度な設定」タブでは、Wi-Fi ポリシーについて以下の高度な設定をする事ができます。

- ・「最大クライアント数」
- ・「クライアントからの最大接続リトライ数」
- ・「最大上り / 下り帯域 (Kbps)」
- ・「最大クライアント上り / 下り帯域 (Kbps)」
- ・「Bonjour パケットフォワーディング」
- ・「IGMP スヌーピング有効」
- ・「最大マルチキャスト帯域 (Kbps)」
- ・「RTS 閾値」
- ・「フラグメント閾値」
- ・「強制ローミング」

注意 最大クライアント帯域 (上り / 下り) と最大帯域 (上り / 下り) の双方の設定をした場合、最大クライアント帯域の設定が優先されます。最大帯域を有効にしたい場合は、最大クライアント帯域を「0」に設定してください。

最大クライアント数	<input type="text" value="64"/>	1 - 64
クライアントからの最大接続リトライ数	<input type="text" value="5"/>	1 - 10
最大上り帯域(Kbps)	<input type="text" value="0"/>	0 - 900000
最大下り帯域(Kbps)	<input type="text" value="0"/>	0 - 900000
最大クライアント上り帯域(Kbps)	<input type="text" value="0"/>	0 - 900000
最大クライアント下り帯域(Kbps)	<input type="text" value="0"/>	0 - 900000
Bonjour/パケットフォワーディング	<input type="checkbox"/>	
IGMPスヌーピング有効	<input type="checkbox"/>	
最大マルチキャスト帯域(Kbps)	<input type="text" value="0"/>	0 - 900000
RTS閾値	<input type="text" value="2347"/>	256 - 2347
フラグメント閾値	<input type="text" value="2346"/>	257 - 2346
強制ローミング	<input type="checkbox"/>	

図 6-20 高度な設定 (SSID プロファイル) 画面

注意 デバイスグループへの Wi-Fi ポリシーの設定、SSID プロファイルについて、詳しくは「第 8 章 「設定」メニュー (D-Link Business Cloud)」「SSID プロファイル」を参照ください。

デバイスの登録

クラウド AP (DBA-1510P) を管理するには、クラウドにデバイス (クラウド AP) を登録する必要があります。
 デバイスの登録方法については、「直接登録」と「CSV ファイルによる登録」の二つがあります。以下にデバイスの登録手順について説明します。

注意 デバイスの登録にはデバイス UID が必要です。デバイス UID は、DBA-1510P 筐体背面ラベルに記載されています。

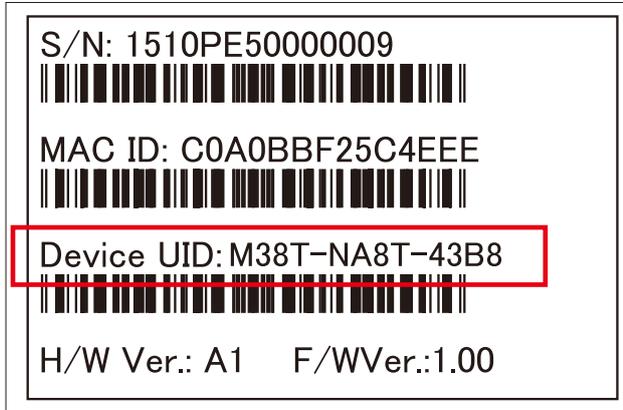


図 6-21 デバイス UID/ 筐体背面ラベル (デバイスの登録)

直接登録

デバイスをクラウドで直接登録します。

管理 > インベントリをクリックし、以下の画面を表示します。

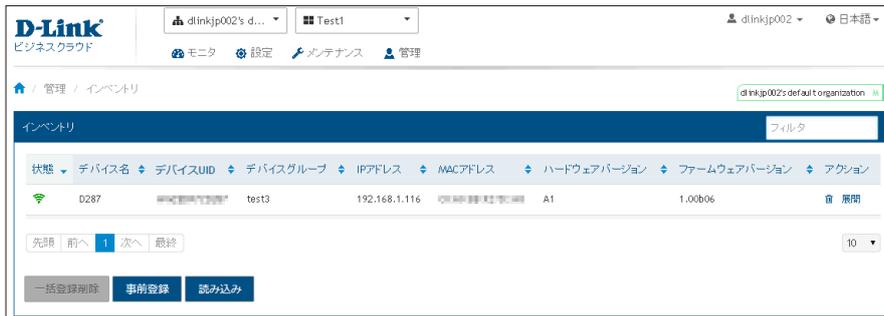


図 6-22 インベントリ画面 (管理)

1. 画面左下の「事前登録」をクリックします。



図 6-23 事前登録をクリック (インベントリ) 画面

2. 「デバイス名」に任意のデバイス名、「デバイス UID」にデバイス UID をハイフン付きで入力、「デバイスグループを選択」で、作成したデバイスグループを選択します。「New Group」を選択すると新たにデバイスグループを作成することが可能です。「デバイスグループ名」に新規デバイスグループ名を入力します。



図 6-24 事前登録（インベントリ）画面

注意 CSV ファイルを使わずに直接登録する際はハイフンも忘れずに記入してください。ハイフンを入力しないと登録できません。

3. 最後に「保存」をクリックし、設定を保存します。
4. **管理 > インベントリ** をクリックし、以下の画面を表示し、登録したデバイス（クラウド AP）が設定通りに表示されている事を確認します。



図 6-25 インベントリ画面

注意 ゴミ箱アイコンをクリックする事で登録したデバイスを削除する事ができますが、過去にクラウドと接続実績のあるデバイスの削除は、デバイスがオンライン状態にある事を確認して削除してください。デバイスをオフライン状態で削除し再度クラウドへ登録する場合、デバイスの手動での初期化が必要となります。

CSV ファイルによる登録

デバイスを CSV ファイルを使用して登録します。

1. 「デバイス UID」を記載した CSV ファイルを読み込むことで、一括でデバイス群を登録することもできます。「事前登録」右にある「読み込み」をクリックします。

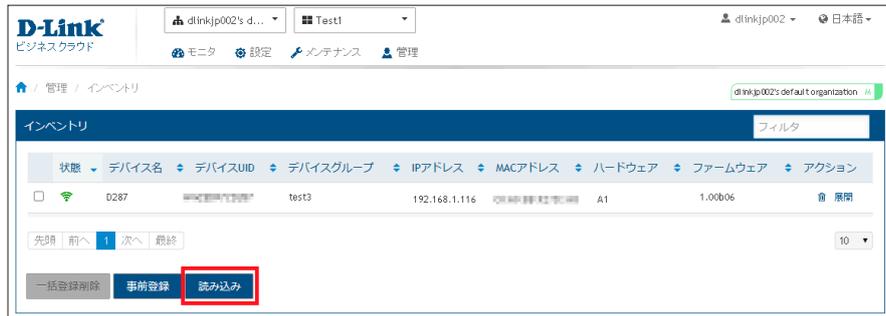


図 6-26 読み込みをクリック（インベントリ）画面

2. 「デバイス UID インポート」という項目が表示されます。「ファイルを選択（参照）」ボタンをクリック、CSV 形式の「デバイスファイル」を指定し「設定を検証」ボタンをクリックすると、CSV ファイルに設定された UID の検証が開始されます。



図 6-27 CSV ファイルのアップロードによるデバイスの読み込み（インベントリ）画面

3. 設定の検証が問題無く終了すると、「インポート実施」ボタンが有効になりますので、このボタンをクリックすることで、デバイスの登録が開始されます。

注意 CSV ファイルは以下のように作成します。右側からデバイス名、デバイスグループ、デバイス UID、組織名の順に記載をします。文字コードは UTF-8 をご利用ください。

	A	B	C	D
1	#DeviceName	#DeviceGroup	#DeviceUID	#Organization
2	csv_1	test	DJPDJPDSAA92	dlinkjp's default organization
デバイス名	csv_2	test1111	DJPDJPDSAA93	dlinkjp-1
	デバイスグループ	デバイス UID		組織名

図 6-28 CSV ファイル画面

4. 最後に「保存」をクリックし、設定を保存します。
5. 管理 > インベントリをクリックし、以下の画面を表示し、登録したデバイス（クラウド AP）が設定通りに表示されている事を確認します。



図 6-29 インベントリ 画面

注意 「デバイスの登録」について、詳しくは「第 10 章 「管理」メニュー（D-Link Business Cloud）」「デバイスの事前登録」を参照ください。

アクセスポイントのクラウドへの接続

DBA-1510P をクラウドに接続する場合、典型的なネットワーク構成は下図の通りとなります。クラウドとクラウド AP (DBA-1510P) との間では、SSL 管理用セッション (TCP:443) を利用し、クラウドからのクラウド AP (DBA-1510P) の制御を行います。DBA-1510P が NAT ルータの配下にあっても、TCP : 443、DNS が「LAN ⇒ WAN」で許可されていれば、正常に動作します。お客様ネットワークで DHCP サーバが稼働していれば、DBA-1510P は IP アドレスを DHCP サーバから取得します。DBA-1510P は、初期値で DHCP クライアント機能が有効になっています。DHCP サーバがネットワーク内に設置されていない場合、DBA-1510P に手動で IP アドレスを設定する必要があります。DBA-1510P の IP アドレスの手動設定は、DBA-1510P のローカル Web GUI で設定を行います。

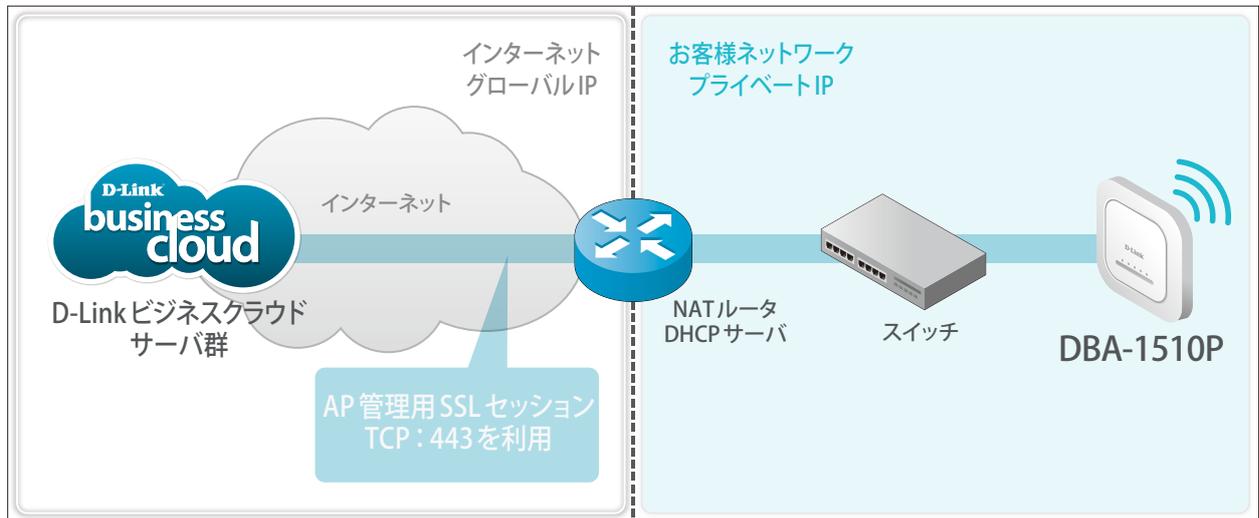


図 6-30 クラウド接続におけるネットワーク構成

プロトコルについて

クラウドサーバとの間で通信を行うプロトコルは、最低限以下の 3 つになります。

プロトコル	用途・備考
TCP 80 (HTTP)	ファームウェアのアップデート用
TCP 443 (SSL)	クラウドサーバとの通信用
UDP 123 (NTP)	スケジュール機能及びモニタ機能用

また、以下の 3 つのプロトコルが許可されている必要があります。

プロトコル	用途・備考
UDP 67 (DHCP)	Static IP を使った場合は不要
UDP 53 (DNS)	
TCP 53 (DNS)	

注意 クラウド AP (デバイス) をクラウドへ接続するには、クラウド側の「デバイスの登録」「Wi-Fi ポリシーの設定」が完了している必要があります。

アクセスポイントの接続

クラウドを利用したネットワーク環境で、DBA-1510P をクラウドへ接続する手順を下記に記載します。

1. AC アダプタ、イーサネットケーブルを下記のように接続します。

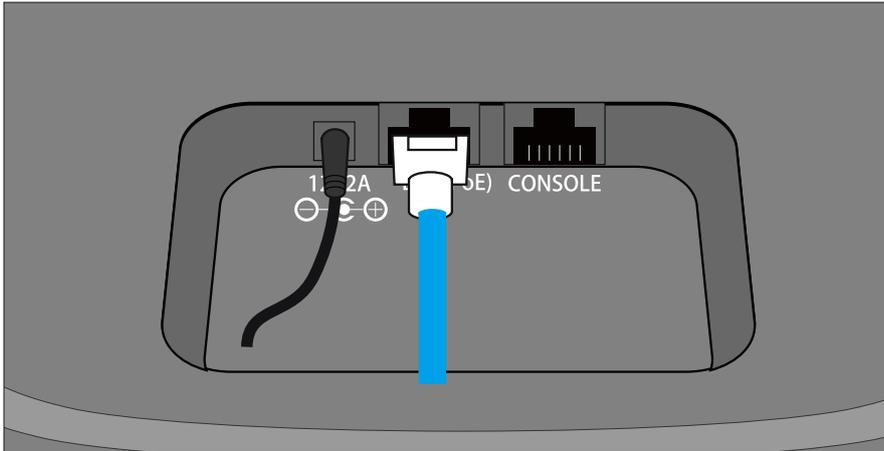


図 6-31 AC アダプタ、イーサネットケーブルの接続

DBA-1510P のイーサネットポートは、IEEE802.3at に準拠した PoE (PoE+) に対応しており、PoE で給電を行う場合には、AC アダプタは不要となります。DBA-1510P が正常に LAN に接続され、IP アドレスを DHCP サーバから取得すると、DBA-1510P は、クラウドサーバに自動で接続し、設定された Wi-Fi ポリシーを自動的にダウンロード、適用します。

2. モニタ > デバイスをクリックし、以下の画面を表示します。



図 6-32 デバイス (モニタ) 画面

クラウドに登録した DBA-1510P (デバイス) の「状態」が、緑色になっていることを確認します。

3. DBA-1510P の筐体 LED で、クラウドの LED が緑点灯している事を確認します。

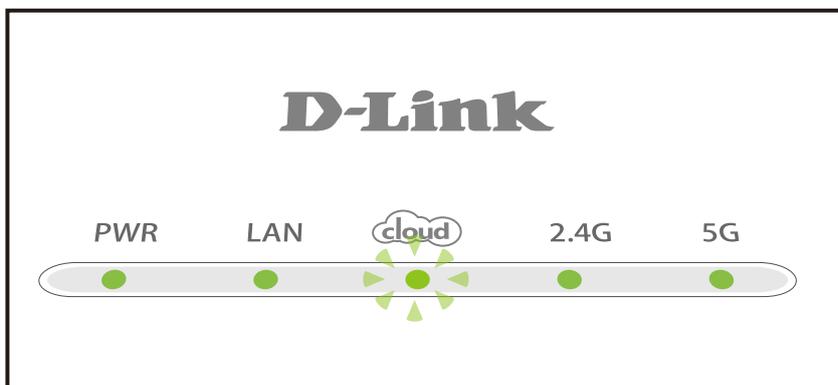


図 6-33 クラウド LED 点灯

以上で、Wi-Fi ポリシーの設定とその確認は終了です。

クライアント PC やスマートフォンなどで設定された SSID で DBA-1510P と通信ができることを確認します。

設定の変更

Wi-Fi ポリシーの設定変更を行います。

注意 設定変更をクラウド GUI に保存しても、プッシュ設定を実行しないと、DBA-1510P に変更した設定は適用されません。

注意 プッシュ設定の際には、デバイスグループ内の全ての DBA-1510P がオンライン状態になっている必要があります。

1. 画面上部にて Wi-Fi ポリシーの設定を変更するデバイスグループを選択します。



図 6-34 デバイスグループ選択画面

2. 設定 > SSID プロファイルをクリックします。



図 6-35 SSID プロファイル選択画面

3. 設定を変更する SSID 名をクリックします。



図 6-36 SSID をクリック (SSID プロファイル) 画面

4. 「SSID プロファイル」の「基本」「MAC フィルタリング」「スケジュール」「高度な設定」タブから変更する項目のタブを選択しクリックします。



図 6-37 項目選択 (SSID プロファイル) 画面

各項目の設定を編集します。デバイスグループへの Wi-Fi ポリシーの設定、SSID プロファイルについて、詳しくは「第 8 章 「設定」メニュー (D-Link Business Cloud)」「SSID プロファイル」を参照ください。

5. 設定の変更が終了したら、「保存」をクリックし、「保存に成功しました。」というメッセージが画面下に表示されることを確認します。



図 6-38 保存 (SSID プロファイル) 画面

6. 設定を保存した後、**設定 > プッシュ設定**をクリックし、以下の画面を表示します。



図 6-39 プッシュ画面

7. 「設定の更新」をクリックします。

8. クラウドからの Wi-Fi ポリシーの配信が終了すると、下記メッセージが表示されます。

Wi-Fi ポリシーの設定が各デバイス (クラウド AP) に適用された場合、「Update Completed」というメッセージが表示されます。

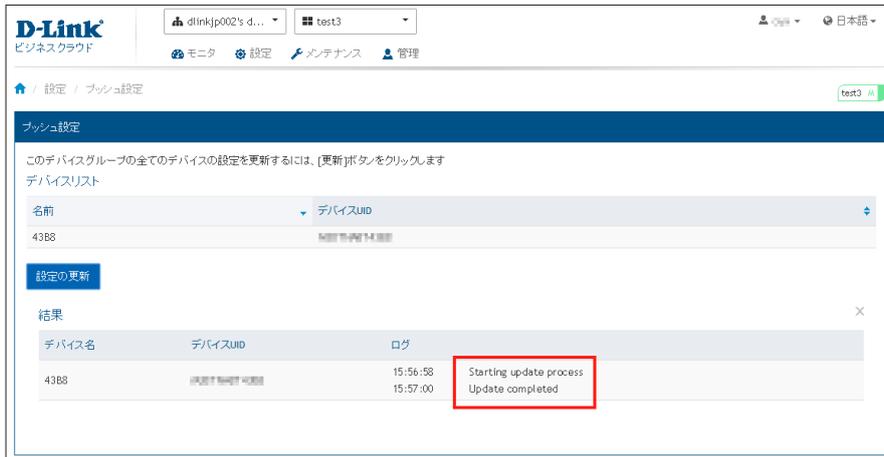


図 6-40 設定更新結果 (プッシュ) 画面

ログインユーザの詳細設定

画面上部、表示されているログイン中のユーザ名をクリックして、「ユーザプロフィール」「権限」「ログアウト」などログイン中ユーザに関する詳細設定、表示を行うことができます。

「ログインユーザの詳細設定」での設定項目

- ・「ユーザプロフィール」- ユーザ名、メールアドレス、パスワードの変更。アラート通知条件、ログイン条件、タイムアウトなどを設定できます。
- ・「権限」- 権限の確認ができます。関連タグ、参加デバイスグループごとの権限を確認できます。
- ・「ログアウト」- ログアウトします。



図 6-41 ログインユーザの詳細設定画面

ユーザプロフィール

ログイン中ユーザのユーザ名、メールアドレス、パスワードの変更。アラート通知条件、ログイン条件、タイムアウトなどを設定できます。

図 6-42 ユーザプロフィール画面

本画面には以下の項目があります。

項目	説明
名前	ユーザ名を編集します。1-64文字で指定します。
メールアドレス	ユーザのメールアドレスを編集します。1-254文字で指定します。
会社名	ユーザの会社名が表示されます。
アラート通知	警告の通知について指定します。 <ul style="list-style-type: none"> ・ デバイスオンライン - デバイスがオンライン時に通知されます。 ・ デバイスオフライン - デバイスがオフライン時に通知されます。 ・ 新しい設定の適用 - 新しい設定適用時に通知されます。 ・ IP アドレスの変更 - IP アドレス変更時に通知されます。 ・ ファームウェアのアップグレード - ファームウェアアップグレード時に通知されます。 ・ デバイスの登録 - デバイス登録時に通知されます。 ・ デバイスの登録取り消し - デバイスの登録が外れた時に通知されます。 ・ ライセンスの不足 - ライセンスの不足時に通知されます。
パスワードを変更する	パスワードを変更する場合、チェックを入れます。
新しいパスワード	パスワードを指定します。

項目	説明
パスワードの確認	確認のため、上記パスワードを指定します。
同じ ID での同時ログインを禁止	同じ ID でクラウド GUI へ同時にログインすることを禁止します。
2 ファクタ認証	2 ファクタ認証を有効にします。クラウドにログインする際、ワンタイムパスワードの入力が必要になります。
アイドルタイムアウト	指定時間 (分) の間クラウド GUI の操作が行われないと、クラウド GUI から自動的にログアウトします。 1 - 60 分の間で指定できます。
このアカウントを削除	「このアカウントを削除」をクリックするとログイン中のアカウントの削除を行うことができます。表示されるパスワード入力の画面でパスワードを入力し「削除」をクリックします。正しいパスワードを入力されていると、アカウントは削除されログインインページに戻ります。 注意 ユーザアカウント (管理者) が「組織」に関連付いている場合、アカウントの削除はできません。

「保存」をクリックして設定内容を保存します。

権限

ログイン中のアカウント (管理者) の権限の確認を行います。



図 6-43 権限 (タグ) 画面



図 6-44 権限 (デバイスグループ) 画面

本画面には以下の項目があります。

項目	説明
タグ	
タグ	関連付けられているタグを表示します。
総デバイスグループ数	所属しているデバイスグループの総数を表示します。
権限	タグ内での権限を表示します。
デバイスグループ	
デバイスグループ	所属しているデバイスグループを表示します。
デバイスグループタイプ	デバイスグループのタイプを表示します。
関連するタグ	デバイスグループに関連するタグを表示します。
権限	デバイスグループ内での権限を表示します。

ログアウト

ログアウトし、ログイン画面へ戻ります。



図 6-45 ログアウト 画面

第7章 「モニタ」メニュー（D-Link Business Cloud）

本章では「D-Link Business Cloud」の「モニタ」メニューの説明を行います。

「モニタ」メニューではデバイスやクライアント、デバイスグループ、タグ、登録/未登録ユーザの動作状況や動作履歴を表示します。統計や警告などの情報をフロアマップなどでデバイスの位置などを映像化して確認することも可能です。

以下は本章「モニタ」メニューのサブメニューの説明です。必要に応じて、設定/変更/修正を行ってください。

サブメニュー	説明
概要（モニタ）	選択されたデバイスグループの詳細/概要を表示します。
地図とフロアマップ	デバイスの物理的な設置場所や設置要件を視覚的に表示します。無線クライアントの物理的な設置場所やデータ消費環境などを、ネットワーク管理者が把握することができます。
デバイス	デバイスグループ内のデバイスについて状態や使用率などを確認します。
クライアント	デバイスグループのデバイスに帰属している無線 LAN クライアントを確認します。
不正 AP	ネットワーク管理者によって管理/承認されていない近隣のアクセスポイントの情報を確認します。
イベント	デバイスグループ内で発生したイベントについて表示します。
レポート	デバイス単位やデバイスグループ単位でのログを CSV 形式のファイルでダウンロードします。

「モニタ」メニューからサブメニューを選択します。



図 7-1 「モニタ」メニュー

概要（モニタ）

選択したデバイスグループの詳細 / 概要を表示します。

モニタ > 概要をクリックし、以下の画面を表示します。

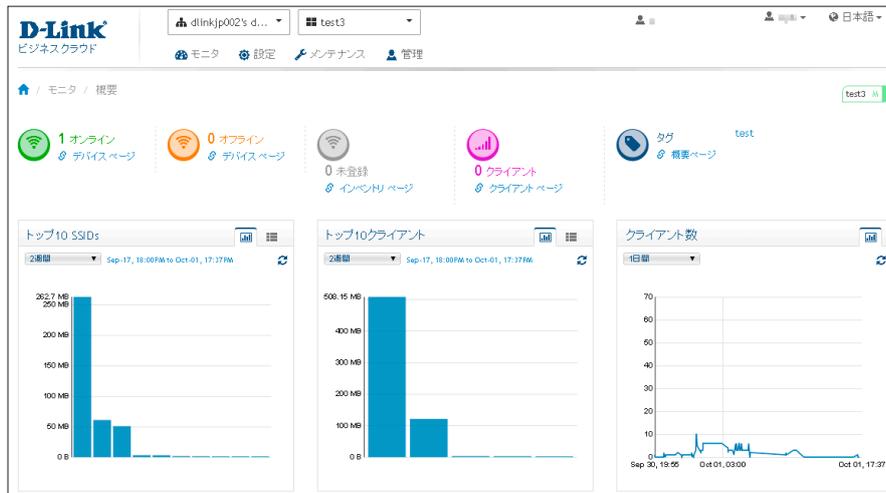


図 7-2 概要（モニタ）画面

本画面には以下の項目があります。

項目	説明
オンライン	現在オンラインのデバイスの数を表示します。
オフライン	現在オフラインのデバイスの数を表示します。
未登録	クラウド管理において未登録のデバイスの数を表示します。
クライアント	デバイスグループ内のクラウド AP と関連する無線 LAN クライアントの数を表示します。
タグ	グループ内のフィルタリング目的でデバイスに設定されたタグを表示します。
トップ 10 SSIDs	よく使用されている SSID トップ 10 を棒グラフで表示します。リストで表示することも可能です。
トップ 10 クライアント	デバイスグループ内でよく使用されているクライアントトップ 10 を棒グラフで表示します。リストで表示することも可能です。
クライアント数	デバイスグループ内のクライアント数を表示します。

注意 本機能は、クラウド AP から NTP サーバへのアクセスが正常に実行できない環境ではご利用頂けません。

地図とフロアマップ

「地図とフロアマップ」ではデバイスを配置している施設の画像を使用して、視覚的にデバイスの場所と状態を把握することが可能です。これはデバイスの物理的な設置場所や設置要件を理解する上でとても有効です。本項目により、ネットワーク管理者は各デバイスのスループットやパフォーマンス向上のために無線クライアントの物理的な設置場所やデータ消費環境などを把握することができます。

モニタ > 地図とフロアマップ をクリックし、以下の画面を表示します。

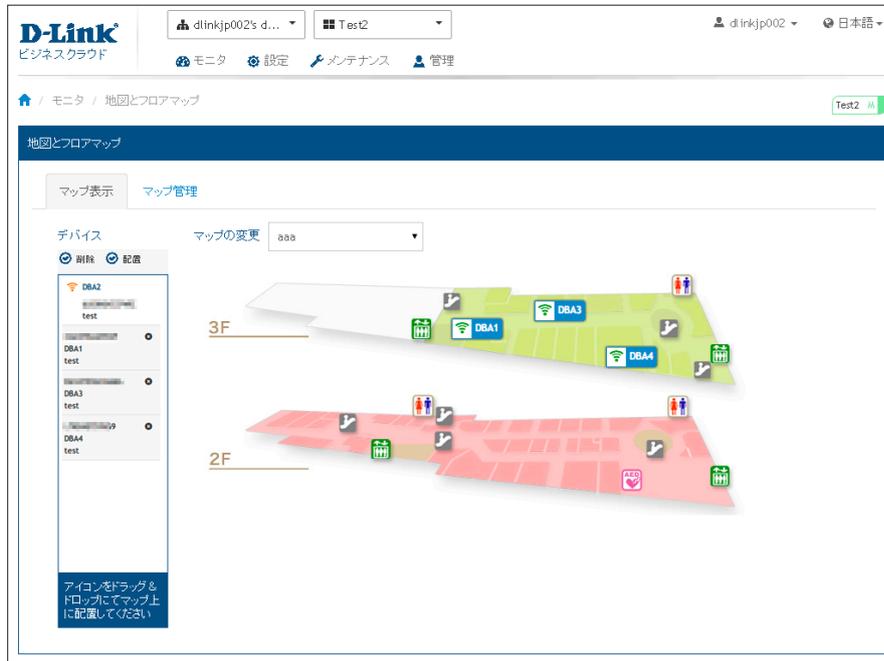


図 7-3 地図とフロアマップ画面（マップ表示）

「地図とフロアマップ」画面には「マップ管理」タブと「マップ表示」タブがあります。以下でそれぞれの画面について説明いたします。

マップ管理

「マップ管理」ではマップの管理を行います。本ページで地図の追加、削除を行います。

モニタ > 地図とフロアマップ > マップ管理 をクリックし、以下の画面を表示します。



図 7-4 地図とフロアマップ画面（マップ管理）

本画面には以下の項目があります。

項目	説明
マップ名	登録されているマップ名を表示します。
アクション	対応するマップに対する動作を実行します。🗑️（ごみ箱アイコン）をクリックするとマップの削除を行います。

フロアマップを追加する場合は「フロアマップを追加」をクリックします。

フロアマップを追加

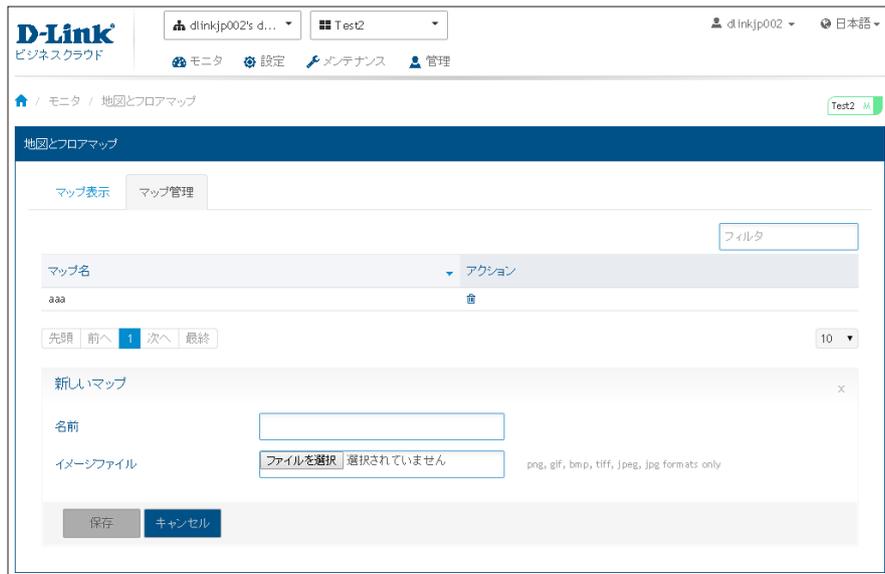


図 7-5 地図とフロアマップ 画面（フロアマップを追加）

本画面には以下の項目があります。

項目	説明
名前	追加するマップ名を指定します。
イメージファイル	追加するマップのイメージファイルを指定します。「png」「gif」「bmp」「jpg」形式ファイルが使用可能です。「ファイルを選択」をクリックしてファイルの保存場所を参照、指定します。

「名前」と「イメージファイル」を指定後、「保存」をクリックしてフロアマップを追加します。

マップ表示

「マップ表示」では「マップ管理」で登録されたマップを表示します。

モニタ > 地図とフロアマップ > マップ表示をクリックし、以下の画面を表示します。

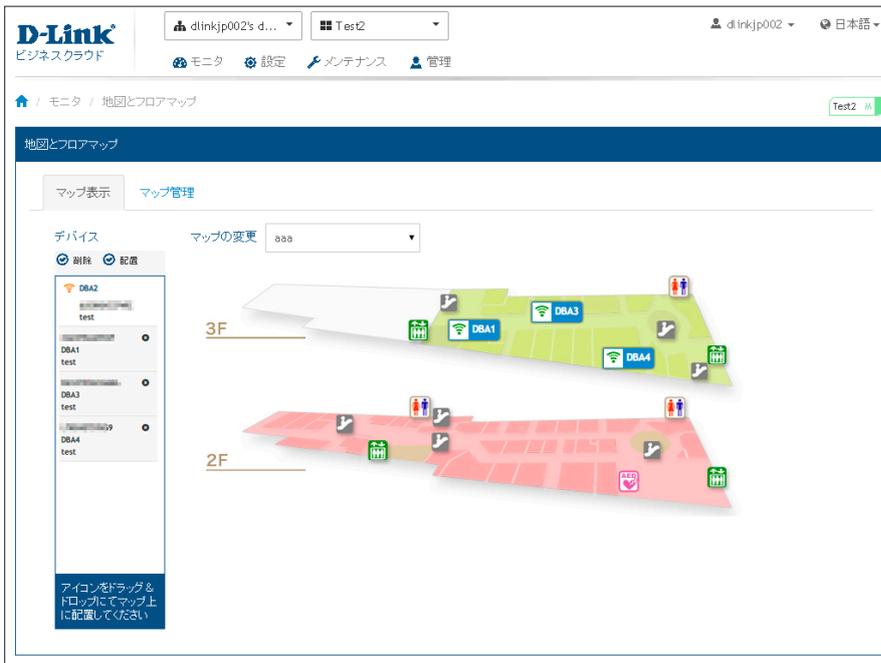


図 7-6 地図とフロアマップ画面（マップ表示）

本画面には以下の項目があります。

項目	説明
マップの変更	「マップ管理」で登録したマップを選択、変更できます。
デバイス	デバイスグループにあるデバイスの一覧です。ドラッグ&ドロップでマップ上に表示することが可能です。配置されたデバイスはドラッグ&ドロップで場所を変更することも可能です。

マップ上にデバイスを配置する

フロアマップ画面左側のデバイスグループにあるデバイスを、ドラッグ&ドロップで地図上に表示することが可能です。配置されたデバイスはドラッグ&ドロップで場所を変更することが可能です。

マップ上のデバイスを削除する

マップ上のデバイスを削除する場合は対応するデバイスの左上の「×」をクリックします。

マップ上に表示するデバイスを選択する

配置されたデバイス、もしくは配置されていないデバイスを表示するには「配置」「削除」のチェックボックスを利用して表示するデバイスをフィルタします。初期値ではすべてのデバイスが表示されます。

マップ上のデバイスの状態について

マップ上のデバイスアイコンは、その色でデバイスの状態も表示します。デバイスアイコンの色が「グレー」の場合、組織に属していないデバイスを意味しています。「緑」の場合はオンライン、「赤」の場合はオフラインを意味しています。

デバイス

「デバイス」ではデバイスグループ内の全デバイスについて状態や使用率などを確認することが可能です。各デバイスの状況については定期的にアップデートされます。

モニタ > デバイスをクリックし、以下の画面を表示します。



図 7-7 デバイス画面

本画面には以下の項目があります。

項目	説明
状態	デバイスの状態。緑はオンライン、橙はオフラインを示します。
デバイス名	デバイス名
UID	デバイスの識別 ID (デバイス UID)
IP アドレス	デバイスの IP アドレス
MAC アドレス	デバイスの MAC アドレス
ハードウェアバージョン	デバイスのハードウェアバージョン
ファームウェアバージョン	デバイスの現在のファームウェアバージョン
通信量	デバイスの通信使用量
クライアント数	デバイスと現在接続している無線クライアント数
チャンネル	デバイスの使用チャンネル
電波出力	デバイスの電波出力

「展開」をクリックするとより詳しい情報について表示します。

「詳細」をクリックすると「設定 > デバイスの設定」のページへ移動します。指定したデバイスについての詳細情報を別ページで表示、設定します。詳しくは「デバイスの設定」を参照ください。

展開（デバイス）

モニタ > デバイス > 展開をクリックし、以下の画面を表示します。



図 7-8 デバイス（展開）画面

本画面には以下の項目があります。

項目	説明
登録状況	デバイスグループへの登録状況
シリアル番号	デバイスのシリアル番号
モデル	デバイスの機種モデル
オンラインクライアント数	デバイスに接続済みのオンラインになっているクライアント数
オフラインクライアント数	デバイスに接続済みのオフラインになっているクライアント数

クライアント

「クライアント」では選択したデバイスグループのデバイスに帰属している無線 LAN クライアントを確認することができます。

モニタ > クライアントをクリックし、以下の画面を表示します。



図 7-9 クライアント画面

本画面には以下の項目があります。

項目	説明
状態	クライアントの状態。緑はオンライン、橙はオフラインを示します。
IP アドレス	クライアントの IP アドレス
MAC アドレス	クライアントの MAC アドレス
SSID	クライアントの所属する SSID
デバイス名 (UID)	クライアントが接続しているデバイス名 (デバイス UID)
チャンネル	クライアントの使用チャンネル
RSSI	クライアントの受信信号強度 (RSSI)(クライアント接続時)
通信量	クライアントとの通信量
最終閲覧	クライアントが最後に認識された日時
ベンダ	クライアントの製造ベンダ

不正 AP

「不正 AP」ではネットワーク管理者によって管理 / 承認されていない近隣アクセスポイントの管理、情報を表示します。

本クラウドにはデバイスグループ近隣の SSID のリストを検出し、当該の SSID に対して対応をすることが可能です。

基準として「-55dBm」以上の近隣 AP が「不正 AP」、それ以外は「その他 AP」と表示され、クラウド AP ではあっても設定上不具合がある AP に関しては「クラウド AP (設定不良)」と表示されます。不正 AP では、利用チャンネル及びその前後 1 チャンネルをスキャンします。スキャンボタンを押下する事で、全チャンネルをスキャンしますが、クライアント通信に影響が出る場合がありますので、ご注意ください。

モニタ > 不正 AP をクリックし、以下の画面を表示します。

The screenshot shows the '不正 AP' (Unauthorized AP) page in the D-Link Business Cloud interface. The page has a navigation bar with 'モニタ' (Monitor), '設定' (Settings), 'メンテナンス' (Maintenance), and '管理' (Management). The main content area is titled '不正 AP' and contains a table of detected APs. The table has columns for 'ステータス' (Status), '検出デバイス' (Detected Device), 'MACアドレス' (MAC Address), 'バンド' (Band), 'チャンネル' (Channel), 'SSID', 'セキュリティ' (Security), and 'RSSI'. The table lists several APs, including '不正 AP' (Unauthorized AP), 'クラウド AP (設定不良)' (Cloud AP (Misconfiguration)), and 'その他 AP' (Other AP). A 'スキャン...' (Scan...) button is located at the bottom left of the table area.

図 7-10 不正 AP 画面

本画面には以下の項目があります。

項目	説明
クラウド AP (設定不良)	チェックを入れると「クラウド AP (設定不良)」のみ表示します。チェックを入れ「更新」をクリックします。
その他 AP	チェックを入れると「その他 AP」のみ表示します。チェックを入れ「更新」をクリックします。
不正 AP	チェックを入れると「不正 AP」のみ表示します。チェックを入れ「更新」をクリックします。
ステータス	検出された AP の状態。「不正 AP」「クラウド AP(設定不良)」「その他 AP」の 3 種類に分類されます。 <ul style="list-style-type: none"> 不正 AP - クラウド AP 以外で「-55dBm」以上の近隣 AP クラウド AP(設定不良) - クラウド AP ではあっても設定上不具合が発生している AP その他 AP - 「不正 AP」以外の非クラウド AP
検出デバイス	不正 AP を検出したデバイス
MAC アドレス	不正 AP の MAC アドレス
バンド	不正 AP がブロードキャスト時の無線帯域
チャンネル	不正 AP が使用しているチャンネル
SSID	検出された AP の SSID
セキュリティ	不正 AP によって設定されているセキュリティ種別
RSSI	不正 AP の受信信号強度 (RSSI)

「展開」をクリックすると対応する AP についてより詳しい情報を表示します。

「不正 AP から除外」をクリックすると対応する AP を「不正 AP」リストから除外し、「ホワイトリスト」へ移動します。

詳しくは「ホワイトリスト」を参照ください。

展開（不正 AP）

モニタ > 不正 AP > 展開 をクリックし、以下の画面を表示します。

ステータス	検出デバイス	MACアドレス	バンド	チャンネル	SSID	セキュリティ	RSSI	
不正 AP	H48C	EGXZLNZH48C	2.4 GHz	11	2360-2	WPA2	-53	展開 ... 不正 AP から除外
UID: EGXZLNZH48C		無線 LAN 方式: b,g,n		UID: -		有線ネットワークでの検出: false		ベンダ: D-Link International BSSID: C4:A8:1D:94:D8:32

図 7-11 展開（不正 AP）画面

本画面には以下の項目があります。

項目	説明
UID	不正 AP の識別番号（デバイス UID）
無線 LAN 方式	不正 AP の無線 LAN 方式
有線ネットワークでの検出	優先ネットワークでの検出有無
ベンダ	不正 AP の製造ベンダ
BSSID	不正 AP の BSSID（Basic Service Set Identifier）

ホワイトリスト

「不正 AP」のリストで「不正 AP から除外」をクリックすると対応する AP を「不正 AP」リストから除外し、「ホワイトリスト」へ移動します。「ホワイトリスト」では AP の情報は MAC アドレスのみ表示されます。

モニタ > 不正 AP > ホワイトリスト をクリックし、以下の画面を表示します。

図 7-12 ホワイトリスト（不正 AP）画面

本画面には以下の項目があります。

項目	説明
MAC アドレス	ホワイトリストに追加された AP の MAC アドレス
アクション	ホワイトリストに追加された AP への動作。 🗑️（ごみ箱アイコン）をクリックすると対応する AP を「不正 AP」のリストに戻します。
ホワイトリストエントリへの追加	「不正 AP」リストの他の AP もホワイトリストへ追加できます。 「ホワイトリストエントリへの追加」をクリックし「MAC アドレス」の項目に追加したい AP の MAC アドレスを入力し保存をクリックします。

イベント

「イベント」ではデバイスグループ内で発生したイベントについて表示します。発生したイベントの詳細は「管理」メニューのシステムログでも参照可能です。

モニタ > イベントをクリックし、以下の画面を表示します。

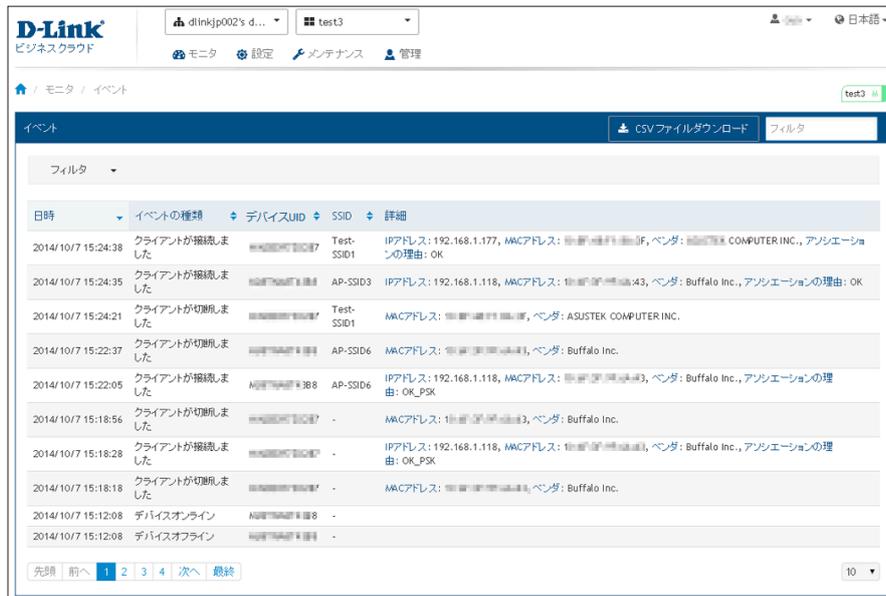


図 7-13 イベント画面

本画面には以下の項目があります。

項目	説明
日時	イベントの発生日時
イベントの種類	「クライアント追加」や「デバイスオフライン」など発生イベントの種類。
デバイス UID	発生したイベントに関連するデバイスの識別情報 (デバイス UID)
SSID	イベントが発生した SSID
詳細	発生したイベント、関連デバイスやクライアントについての詳細情報 (IP アドレス、MAC アドレス、ベンダなど)

「CSV ファイルダウンロード」をクリックすると発生イベントについてのログを CSV 形式のファイルでダウンロードします。

「フィルタ」をクリックすると条件に従い、表示されるイベントのリストを絞り込むことができます。詳しくは「[フィルタ \(イベント\)](#)」を参照ください。

注意 本機能は、クラウド AP から NTP サーバへのアクセスが正常に実行できない環境ではご利用頂けません。

フィルタ（イベント）

イベント内の「フィルタ」をクリックすると、条件に従い表示されるイベントのリストを絞り込むことができます。

モニタ > イベント > フィルタをクリックし、以下の画面を表示します。

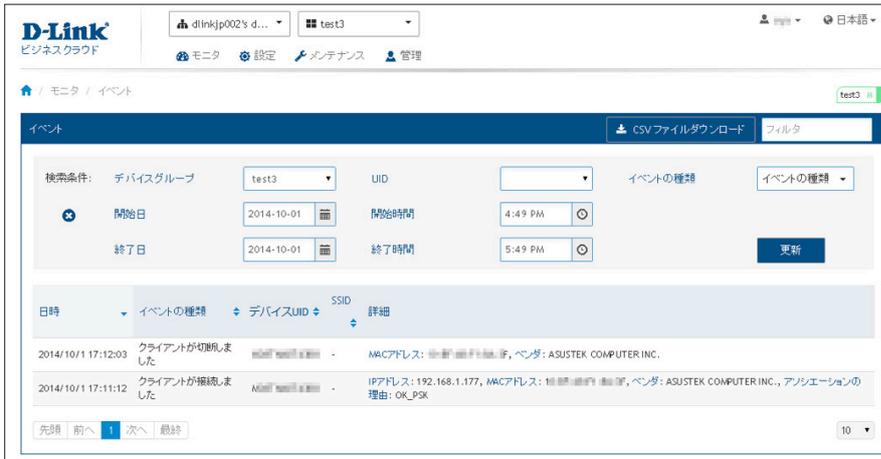


図 7-14 フィルタ（イベント）画面

本画面には以下の項目があります。

項目	説明
デバイスグループ	発生イベントのデバイスグループ
デバイス UID	発生イベントに関連するデバイスの識別番号（デバイス UID）
イベントの種類	発生イベントの種類
開始日	発生イベントの開始日
開始時間	発生イベントの開始時間
終了日	発生イベントの終了日
終了時間	発生イベントの終了時間

上記項目を指定後「更新」をクリックしてイベントリストを更新します。

レポート

「レポート」ではデバイス単位やデバイスグループ単位でのログを CSV 形式のファイルでダウンロードすることが可能です。

モニタ > レポートをクリックし、以下の画面を表示します。

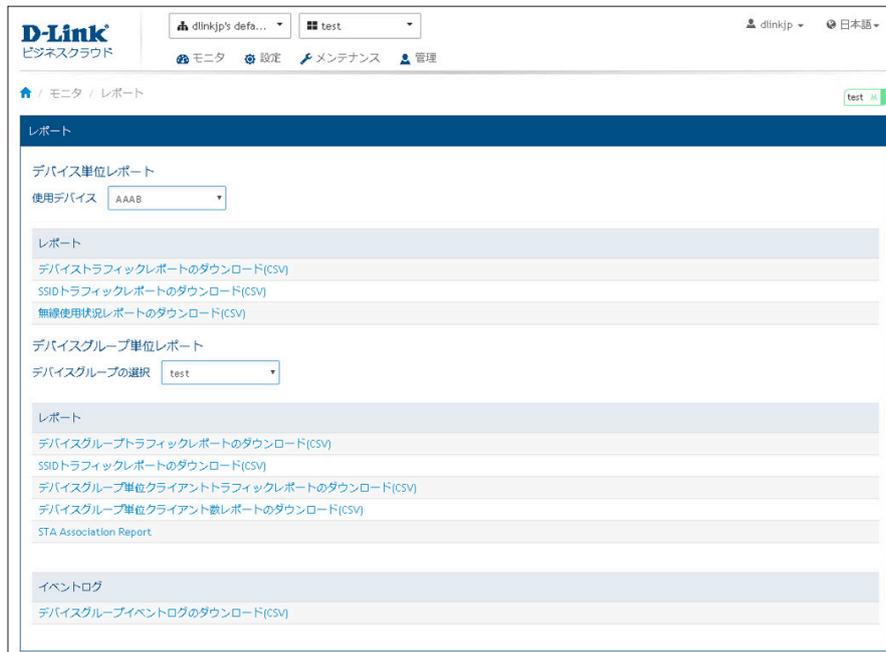


図 7-15 レポート画面

本画面には以下の項目があります。

項目	説明
デバイス単位レポート	
使用デバイス	レポートをダウンロードするデバイスを選択します。
デバイストラフィックレポートのダウンロード (CSV)	デバイストラフィックレポートをダウンロードします。
SSID トラフィックレポートのダウンロード (CSV)	SSID トラフィックレポートをダウンロードします。
無線使用状況レポートのダウンロード (CSV)	「無線使用状況レポート」をダウンロードします。
デバイスグループ単位レポート	
デバイスグループの選択	レポートをダウンロードするデバイスグループを選択します。
デバイスグループトラフィックレポートのダウンロード (CSV)	デバイスグループトラフィックレポートをダウンロードします。
SSID トラフィックレポートのダウンロード (CSV)	SSID トラフィックレポートをダウンロードします。
デバイスグループ単位クライアントトラフィックレポートのダウンロード (CSV)	「デバイスグループ単位クライアントトラフィックレポート」をダウンロードします。
デバイスグループ単位クライアント数レポートのダウンロード (CSV)	「デバイスグループ単位クライアント数レポート」をダウンロードします。
接続無線クライアントレポート	接続無線クライアントレポート (CSV) をダウンロードします。ダウンロードする際には、ダウンロードするクライアントの MAC アドレスを選択します。
イベントログ	
デバイスグループイベントログのダウンロード (CSV)	デバイスグループイベントログ (CSV) をダウンロードします。

注意 本機能は、クラウド AP から NTP サーバへのアクセスが正常に実行できない環境ではご利用頂けません。

ダウンロードできる CSV レポート

モニタ > レポートでダウンロードできる CSV レポートは下記の通りです。レポートファイルは全て CSV 形式となります。

- ・ 1 時間毎の通信量 (AP 毎 / 月次)
- ・ 1 時間毎の通信量 (SSID 毎 / 月次)
- ・ 1 時間毎の使用無線チャンネル・同一チャンネル近隣 AP 数 (AP 毎 / 月次)
- ・ 1 時間毎の通信量 (デバイスグループ毎 / 月次)
- ・ 1 時間毎の通信量 (SSID・デバイスグループ毎 / 月次)
- ・ 1 時間毎の通信量 (クライアント毎 / 月次)
- ・ 1 時間毎の接続クライアント数 (AP・デバイスグループ毎 / 月次)

1 時間毎の通信量 (AP 毎 / 月次)

1 時間毎の通信量 (AP 毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E	F
1	Timestamp	Device Name	UID	Usage		
2						
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	406896		
4						
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	3116098		
6						
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	263385403		
8						
9						
10						

図 7-16 1 時間毎の通信量 (AP 毎 / 月次) 画面

DBA-1510P の 1 時間毎の通信量 (バイト) が「Usage」に表示されます。文字コードは UTF-8 をご利用ください。

1 時間毎の通信量 (SSID 毎 / 月次)

1 時間毎の通信量 (SSID 毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E	F
1	Timestamp	Device Name	UID	SSID	Usage	
2						
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	100cloud1	406896	
4						
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	100cloud1	3116098	
6						
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	HD46	DBA-1510P-46	100cloud1	263385403	
8						
9						
10						

図 7-17 1 時間毎の通信量 (SSID 毎 / 月次) 画面

特定 AP SSID の 1 時間毎の通信量 (バイト) が「Usage」に表示されます。文字コードは UTF-8 をご利用ください。

1 時間毎の使用無線チャンネル・同一チャンネル近隣 AP 数 (AP 毎 / 月次)

1 時間毎の使用無線チャンネル・同一チャンネル近隣 AP 数 (AP 毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E	F	G	H
1	Timestamp	Device Group	Device Name	UID	Band	Channel	Number of Neighbor APs on same channel	
2								
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	5 GHz	60	1	
4								
5	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	2.4 GHz	12	0	
6								
7	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	5 GHz	60	0	
8								
9	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	2.4 GHz	12	0	
10								
11	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	5 GHz	60	0	
12								
13	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	2.4 GHz	12	0	
14								
15	Mon Oct 06 2014 18:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	5 GHz	60	0	
16								
17	Mon Oct 06 2014 18:00:00 GMT+0900 (JST)	test1	HD46	DBA-1510P-46	2.4 GHz	12	0	
18								

図 7-18 1 時間毎の使用無線チャンネル・同一チャンネル近隣 AP 数 (AP 毎 / 月次) 画面

Channel は DBA-1510P が利用していたチャンネル、「Number of Neighbor Aps on same channel」は、同一チャンネルを利用していた近隣 AP 数となります。文字コードは UTF-8 をご利用ください。

1 時間毎の通信量 (デバイスグループ毎 / 月次)

1 時間毎の通信量 (デバイスグループ毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E
1	Timestamp	Device Group	Usage		
2					
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	406896		
4					
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	3116098		
6					
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	263385403		
8					
9					
10					

図 7-19 1 時間毎の通信量 (デバイスグループ毎 / 月次) 画面

デバイスグループの 1 時間毎の通信量 (バイト) が「Usage」に表示されます。文字コードは UTF-8 をご利用ください。

1 時間毎の通信量 (SSID・デバイスグループ毎 / 月次)

1 時間毎の通信量 (SSID・デバイスグループ毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E
1	Timestamp	Device Group	SSID	Usage	
2					
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	100cloud1	406896	
4					
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	100cloud1	3116098	
6					
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	100cloud1	263385403	
8					
9					
10					

図 7-20 1 時間毎の通信量 (SSID・デバイスグループ毎 / 月次) 画面

デバイスグループに所属する SSID の 1 時間毎の通信量 (バイト) が「Usage」に表示されます。文字コードは UTF-8 をご利用ください。

1 時間毎の通信量 (クライアント毎 / 月次)

1 時間毎の通信量 (クライアント毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E
1	Timestamp	Device Group	MAC address	Usage	
2					
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	08:00:27:00:00:00	316037	
4					
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	08:00:27:00:00:00	2986566	
6					
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	08:00:27:00:00:00	257971999	
8					
9					
10					

図 7-21 1 時間毎の通信量 (クライアント毎 / 月次) 画面

デバイスグループに接続したクライアント (MAC address) の 1 時間毎の通信量 (バイト) が「Usage」に表示されます。文字コードは UTF-8 をご利用ください。

1 時間毎の接続クライアント数 (AP・デバイスグループ毎 / 月次)

1 時間毎の接続クライアント数 (AP・デバイスグループ毎 / 月次) CSV レポートサンプルは下記の通りとなります。

	A	B	C	D	E	F	G
1	Timestamp	Device Group	SSID	Device Name	UID	Band	Number of Clients on this AP
2							
3	Mon Oct 06 2014 15:00:00 GMT+0900 (JST)	test1	100cloud1	HD46	08:00:27:00:00:00	2.4 GHz	1
4							
5	Mon Oct 06 2014 16:00:00 GMT+0900 (JST)	test1	100cloud1	HD46	08:00:27:00:00:00	2.4 GHz	1
6							
7	Mon Oct 06 2014 17:00:00 GMT+0900 (JST)	test1	100cloud1	HD46	08:00:27:00:00:00	2.4 GHz	1
8							
9							
10							

図 7-22 1 時間毎の接続クライアント数 (AP・デバイスグループ毎 / 月次) 画面

「Number of Clients on this AP」(AP 上のクライアント数) は、各時間帯のクライアント接続数となります。文字コードは UTF-8 をご利用ください。

第 8 章 「設定」メニュー（D-Link Business Cloud）

本章では「D-Link Business Cloud」の「設定」メニューの説明を行います。

「設定」メニューではデバイスグループ単位での Wi-Fi ポリシーの設定を行います。デバイスグループはクラウドインタフェース画面上部からも選択可能で、既存のデバイスグループを切り替えることができます。設定を編集したデバイスグループは個別の Web ページでも表示されます。デバイスグループの設定についてはデバイスグループ内への設定の配信（プッシュ設定）を行うことで、デバイスグループへの設定の適用をコントロールします。

以下は本章「設定」メニューのサブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
SSID プロファイル	デバイス上の SSID の作成、設定を行います。
無線設定	デバイスグループの内のデバイスに対しチャンネルや無線出力の設定を行います。
RADIUS 設定	新規 RADIUS サーバの追加、既存・新規 RADIUS サーバの設定編集、そして RADIUS サーバの状況や設定情報の表示などを行います。
LDAP 設定	LDAP サーバを利用したキャプティブポータルでのユーザ認証を設定します。
キャプティブポータル	無線クライアントのユーザによるクラウド AP へのアクセスの前に、Web ページ（スプラッシュページ）を経由させ、アクセスの前に指定の情報をユーザに表示、対応させる機能です。
DHCP プール設定	NAT モードで利用するための DHCP アドレスプールの設定を行います。
一般設定	デバイスのユーザ名とパスワードの設定を行います。
プッシュ設定	ビジネスクラウドに保存されたデバイスの設定を、デバイスグループ内のすべてのデバイスに適用します。
デバイスの設定	デバイスグループ内のデバイスの状態や使用率などを確認することができます。加えて各デバイスの設定も個別に行う事が可能です。

「設定」メニューからサブメニューを選択します。



図 8-1 「設定」メニュー

SSID プロファイル

デバイスに適用される SSID の設定を行います。DBA-1510P は 16 個の SSID を各帯域（5GHz と 2.4GHz）に 8 個ずつサポートしています。デバイスグループが作成されると同時にデフォルトの SSID も作成されます。

設定 > SSID プロファイルをクリックし、以下の画面を表示します。

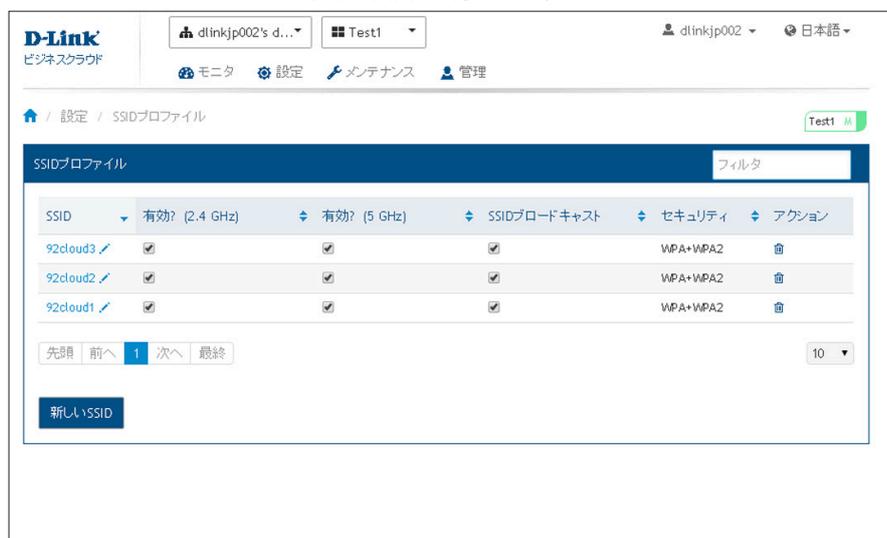


図 8-2 SSID プロファイル画面

本画面には以下の項目があります。

項目	説明
SSID	無線ネットワークを識別する 1-32 文字の固有の ID です。 各 SSID 名をクリックすると当該 SSID プロファイルの編集を行うことができます。 SSID の設定の詳細については「 SSID プロファイル編集 」を参照してください。
有効 (2.4GHz) / 有効 (5GHz)	各帯域（2.4/5GHz）の有効 / 無効を指定します。チェックボックスにチェックがある場合は有効になります。
SSID ブロードキャスト	当該の SSID をブロードキャストする場合、チェックを入れます。ブロードキャストされた SSID は無線クライアントから識別できます。追加のセキュリティ対応が必要な場合、SSID のブロードキャストは無効になります。本ネットワークに接続する無線クライアントが当該の SSID に確認される必要がある場合、有効です。
セキュリティ	クライアントとクラウド AP 間のセキュリティの種類を表示します。
アクション	当該の SSID に対する動作を実行します。  （ごみ箱アイコン）をクリックすると SSID の削除を行います。

SSID の追加方法

以下では新しい SSID のプロファイルの追加手順について説明します。

- 画面下部の「新しい SSID」をクリックし、表示された「SSID」に SSID 名、「バンド選択」に使用する帯域を指定、「保存」をクリックします。

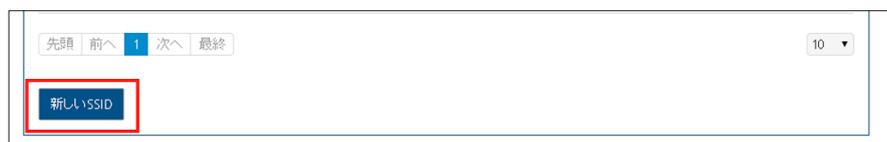


図 8-3 SSID プロファイル画面（新しい SSID）

- SSID プロファイルの設定画面が表示されます。設定内容、設定方法については「[SSID プロファイル編集](#)」を参照ください。

SSID プロファイル編集

「SSID プロファイル」画面の各 SSID 名や「新しい SSID」内の「保存」をクリックし、新規 / 既存 SSID の詳細について設定を行います。

基本 (SSID プロファイル編集)

「SSID プロファイル編集」で「基本」タブを選択します。

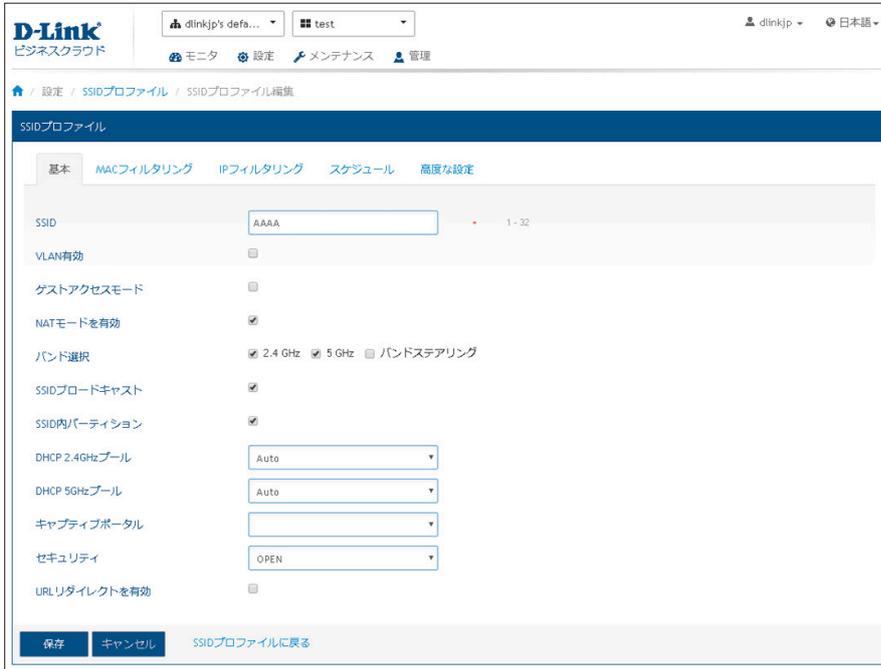


図 8-4 SSID プロファイル編集 (基本) 画面

本画面には以下の項目があります。

項目	説明						
SSID	<p>SSID を指定します。無線ネットワークを識別する 1-32 文字の固有の ID です。</p> <p>注意 ASCII 印字可能文字表 (https://en.wikipedia.org/wiki/ASCII) の『ASCII printable code chart』に記載されている文字であれば使用可能ですが、以下も特殊文字については、下記のような制限がございます。</p> <table border="1"> <thead> <tr> <th>特殊文字</th> <th>制限概要</th> </tr> </thead> <tbody> <tr> <td>「?」「"」「\$」「[」 「\」「]」「+」</td> <td>使用できません。</td> </tr> <tr> <td>「!」「#」「;」</td> <td>使用できますが、『!abcd...』『#abcd...』『;abcd...』のように、先頭で使用することはできません。</td> </tr> </tbody> </table>	特殊文字	制限概要	「?」「"」「\$」「[」 「\」「]」「+」	使用できません。	「!」「#」「;」	使用できますが、『!abcd...』『#abcd...』『;abcd...』のように、先頭で使用することはできません。
特殊文字	制限概要						
「?」「"」「\$」「[」 「\」「]」「+」	使用できません。						
「!」「#」「;」	使用できますが、『!abcd...』『#abcd...』『;abcd...』のように、先頭で使用することはできません。						
VLAN 有効	<p>ネットワークの VLAN を有効にし、「VLAN タイプ」と「VLAN タグ」を指定します。 (「VLAN タイプ」と「VLAN タグ」は VLAN 有効時のみ表示されます。)</p>						
ゲストアクセスモード	<p>VLAN などの設定を行わずにゲスト用の SSID を設定します。 本機能を有効にすると、下記の機能が自動的に有効になります。</p> <ul style="list-style-type: none"> プライベート IP アドレスフィルタリング: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 宛ての packets を破棄します。 DHCP サーバ機能: 10.229.x.x の IP アドレスが所属端末に割り当てられます。 DNS リレー機能: 所属端末からの DNS packets をリレーします。 NAT 機能: 所属端末からの packets を DBA-1510P の管理 IP/VLAN に変換します。 SSID 間パーティション: ゲストアクセスモードが設定されている SSID と他の SSID 間の通信を禁止します。 SSID 内パーティション: 所属端末同士の通信を遮断します。 <p>注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。</p>						

項目	説明
NAT モードを有効	<p>本機能を有効にすると、下記の機能が自動的に有効になります。ゲストアクセスモードを有効にすると、NAT 機能も自動的に有効になります。</p> <ul style="list-style-type: none"> ・ NAT 機能: 帰属端末からのパケットを DBA-1510P の管理 IP/VLAN に変換します。 ・ DHCP サーバ機能: DHCP2.4GHz プールで、SSID (2.4GHz 帯) に適用する DHCP プールを選択し、DHCP5GHz プールで、SSID (5GHz) に適用する DHCP プールを選択します。 ・ DNS リレー機能: 帰属端末からの DNS パケットをリレーします。 ・ SSID 間パーティション: ゲストアクセスモードが設定されている SSID と他の SSID 間の通信を禁止します。 <p>注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 DHCP プール機能はファームウェアバージョン 1.3 以上が DBA-1510P にインストールされている必要があります。</p>
バンド選択	SSID のバンド (帯域) を選択します。「2.4GHz」「5GHz」「バンドステアリング」から選択可能です。
SSID ブロードキャスト	当該の SSID をブロードキャストする場合、チェックを入れます。ブロードキャストされた SSID は無線クライアントから識別できます。追加のセキュリティ対応が必要な場合、SSID のブロードキャストは無効になります。本ネットワークに接続する無線クライアントが当該の SSID に確認される必要がある場合、有効です。
SSID 内パーティション	有効にすると SSID 内の無線クライアントは互いに通信ができなくなります。
DHCP 2.4GHz プール	2.4GHz 帯で使用する DHCP プールを選択します。DHCP プールは「設定 > DHCP プール設定」で設定することができます。また自動的に DHCP プールを割り当てたい場合には、DHCP プール「Auto」を選択することができます。「Auto」を選択すると、自動的に DHCP プールの割り当てが行われます。
DHCP 5GHz プール	5GHz 帯で使用する DHCP プールを選択します。DHCP プールは「設定 > DHCP プール設定」で設定することができます。また自動的に DHCP プールを割り当てたい場合には、DHCP プール「Auto」を選択することができます。「Auto」を選択すると、自動的に DHCP プールの割り当てが行われます。
キャプティブポータル	「キャプティブポータル」の設定には事前に「設定 > キャプティブポータル」でキャプティブポータルを設定しておく必要があります。キャプティブポータルは機器によって無線クライアントに対しカスタム設定のページを提示し、接続する前にクライアントの認証情報を取得します。
URL リダイレクトを有効	<p>「URL リダイレクトを有効」をチェックするとクライアントが無線 LAN に接続後、ブラウザを開くと指定された URL へ強制的にリダイレクトされます。キャプティブポータルを有効にしている場合、キャプティブポータルの処理の後に指定された URL に強制的にリダイレクトされます。</p> <ul style="list-style-type: none"> ・ 「リダイレクト先 URL」: リダイレクト先の任意の URL を入力します。 ・ 「リダイレクト間隔 (分)」: 強制再リダイレクトを実施する時間間隔 (分) を指定します。15 (分) に設定すると、15 分おきに指定された URL へ強制的にリダイレクトされます。強制再リダイレクトを無効にする場合には、0 を指定します。0 を指定した場合、一旦 URL リダイレクトが実施されたクライアントは、無線 LAN 接続が切断されるまで通信を行う事ができます。 <p>注意 URL リダイレクトが有効な場合、リダイレクト処理が終了するまでクライアントからの全ての通信は遮断されます。通信が許可されるには、ブラウザを開いてリダイレクト先 URL を閲覧する必要があります。</p> <p>注意 本機能はファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。</p>
セキュリティ	SSID のセキュリティモードを指定します。 選択するセキュリティモードによって指定する項目が異なります。表示される各項目に適切な設定を行います。
セキュリティモード「WEP」を選択時	
WEP 認証	WEP 認証方式を「Open System」または「Shared Key」から選択します。
WEP 暗号化	WEP 暗号化方式を「64bit WEP」(64 ビット) または「128bit WEP」(128 ビット) から選択します。
WEP キーのフォーマット	WEP キーのフォーマットを「ASCII」(ASCII 文字) または「Hexadecimal」(16 進数方式) から選択します。
WEP キー 0 ~ 3	WEP キーを指定します。キーは「WEP キー 0」から「WEP キー 3」まで設定することが可能です。 WEP キー文字数仕様は下記の通りとなります。 64bit/ASCII: 5, 64bit/HEX: 10, 128bit/ASCII: 13, 128bit/HEX: 26
セキュリティモード「WPA」 「WPA2」または「WPA+WPA2」を選択時	
認証方式	「セキュリティモード」で「WPA」「WPA2」または「WPA+WPA2」を選択時に表示されます。 「PSK」(Pre-shared Key) もしくは「RADIUS」(ネットワークに RADIUS サーバが構築されている場合) を選択します。 RADIUS サーバは「設定 > RADIUS 設定」で設定します。
暗号化方式	「セキュリティモード」で「WPA」「WPA2」または「WPA+WPA2」を選択時に表示されます。 暗号化方式を選択します。「AES」「TKIP」「AES+TKIP」から選択します。
事前共有鍵	「認証方式」で「PSK」を選択時に表示されます。「PSK」(Pre-Shared Key/事前共有鍵) を入力します。 「8」文字から「63」文字の間で指定できます。「文字列を表示」にチェックを入れると、文字列の入力時に入力した文字がそのまま表示されます。ASCII 印字可能文字表 (https://en.wikipedia.org/wiki/ASCII) の『ASCII printable code chart』に記載されている文字であれば使用可能です。
事前認証	「認証方式」で「RADIUS」を選択時に表示されます。RAIDUS サーバでの事前認証を有効にする場合指定します。
プライマリ RADIUS サーバ セカンダリ RADIUS サーバ プライマリ Accounting サーバ セカンダリ Accounting サーバ	「認証方式」で「RADIUS」を選択時に表示されます。 「プライマリ/セカンダリ」の RADIUS サーバと「プライマリ/セカンダリ」の Accounting サーバを指定します。 設定する RADIUS サーバは「設定 > RADIUS 設定」で事前に設定します。
グループキー更新間隔	グループキーの更新間隔を指定します。

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

注意 ブラウザ（Google Chrome）の設定により「サイトのパスワード保存」に関するダイアログが表示される場合がありますが、「使用しない」（保存しない）をクリックしてください。



図 8-5 パスワード保存の確認メッセージ

MAC フィルタリング（SSID プロファイル編集）

「SSID プロファイル編集」で「MAC フィルタリング」タブを選択します。
 「MAC フィルタリング」は接続要求のあった無線クライアントを、その MAC アドレスを基準に承認 / 拒否する機能です。
 本項目では事前に設定した MAC アドレスリストと、その無線クライアントへの動作の設定を行います。

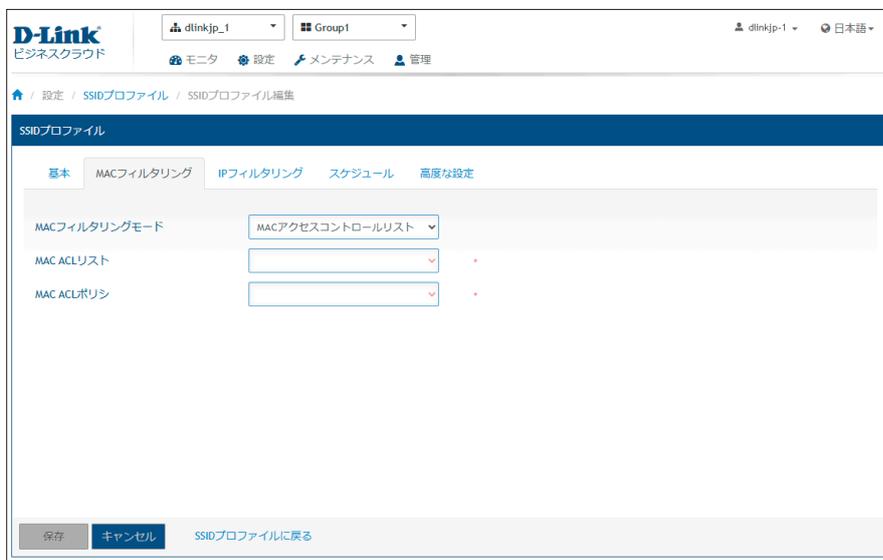


図 8-6 SSID プロファイル編集（MAC フィルタリング）画面

本画面には以下の項目があります。

項目	説明
MAC フィルタリングモード	<p>MAC フィルタリングモードを指定します。「無効化」「MAC アクセスコントロールリスト」「Radius サーバ」から選択します。初期値は「無効化」です。</p> <p>Radius サーバを選択した場合、クライアントの MAC アドレスを指定した外部 Radius サーバで認証します。外部 Radius サーバは下記のアトリビュートを利用します。</p> <ul style="list-style-type: none"> 「User」：認証するクライアントの MAC アドレス 「PWD」：DBA-1510P <p>「MAC アクセスコントロールリスト」を選択するには事前に MAC アクセスコントロールリストを作成する必要があります。</p> <p>注意 「Radius サーバ」を選択する場合、ファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 RADIUS サーバの変更を行う場合、「設定 > RADIUS 設定」で RADIUS サーバの設定変更を行い、本設定画面で「保存」ボタンをクリック、その後「設定 > プッシュ設定」で設定の更新を実施する必要があります。</p>
MAC ACL リスト	<p>「MAC フィルタリングモード」で「MAC アクセスコントロールリスト」を選択時に表示されます。事前設定した MAC ACL リストを選択します。MAC ACL リストは「メンテナンス > MAC データベース」で事前登録する必要があります。</p>
MAC ACL ポリシ	<p>「MAC フィルタリングモード」で「MAC アクセスコントロールリスト」を選択時に表示されます。</p> <ul style="list-style-type: none"> 「許可」を選択すると MAC ACL リストに登録された MAC アドレスの無線クライアントのみアクセスが許可され、それ以外の無線クライアントのアクセスは拒否されます。 「拒否」を選択すると MAC ACL リストに登録された MAC アドレスの無線クライアントのみアクセスを拒否され、それ以外の無線クライアントのアクセスが許可されます。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

IP フィルタリング (SSID プロファイル編集)

「SSID プロファイル編集」で「IP フィルタリング」タブを選択します。

「IP フィルタリング」は IP データベースに登録した特定の IP アドレス、ネットワーク宛での通信を、許可 / 拒否する機能です。

本項目では事前に設定した IP フィルタリングリストと、その IP アドレス宛での通信の動作設定を行います。

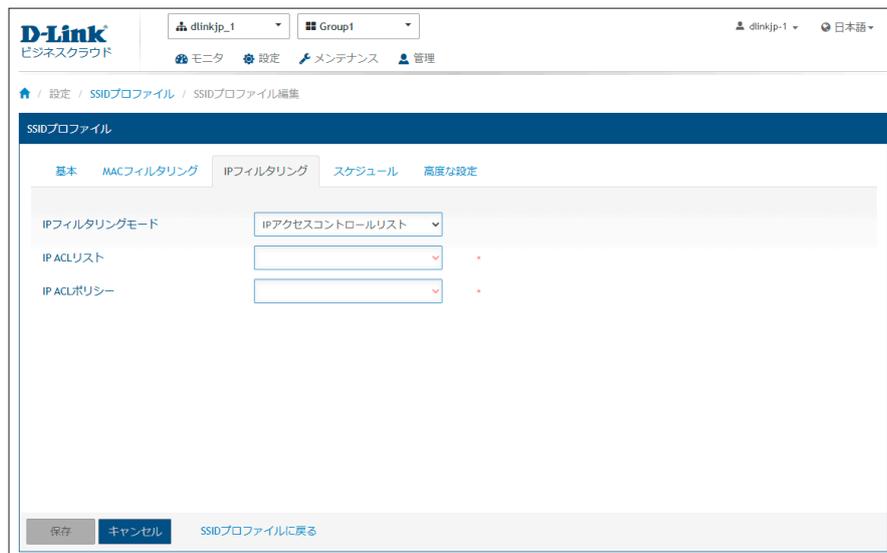


図 8-7 SSID プロファイル編集 (IP フィルタリング) 画面

本画面には以下の項目があります。

項目	説明
IP フィルタリングモード	<p>IP フィルタリングモードを指定します。「IP アクセスコントロールリスト」を選択すると、IP フィルタリングが有効になります。「無効化」を選択すると IP フィルタリングが無効になります。初期値は「無効化」です。</p> <p>注意 「基本 (SSID プロファイル編集)」で「ゲストアクセスモード」を有効にした場合、自動的に「プライベート IP アドレスフィルタリング」が有効になるので、「10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16」宛のパケットは破棄されます。「ゲストアクセスモード」有効時に本機能 (IP フィルタリングモード) を有効にした場合、「プライベート IP アドレスフィルタリング」は無効となりますので、「プライベート IP アドレスフィルタリング」でフィルタされる IP アドレス (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16) を本機能でフィルタする場合、当該アドレスを「IP ACL リスト」に手動で追加する必要があります。</p> <p>注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。</p>
IP ACL リスト	<p>IP フィルタリングに適用する「IP ACL リスト」を選択します。</p> <p>注意 「IP ACL リスト」は、「メンテナンス > IP データベース」で登録する必要があります。</p>
IP ACL ポリシー	<p>選択した「IP ACL リスト」に登録された IP アドレス宛の通信の許可 / 破棄を指定します。</p> <p>「許可」を選択すると許可され、「拒否」を選択すると破棄されます。</p>

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

スケジュール (SSID プロファイル編集)

「SSID プロファイル編集」で「スケジュール」タブを選択します。

SSID のスケジュール設定を行います。指定した日時に SSID が有効になります。「終日」を選択すると対応する曜日終日、「終日」チェックを外し対応する日の時間を設定することも可能です。

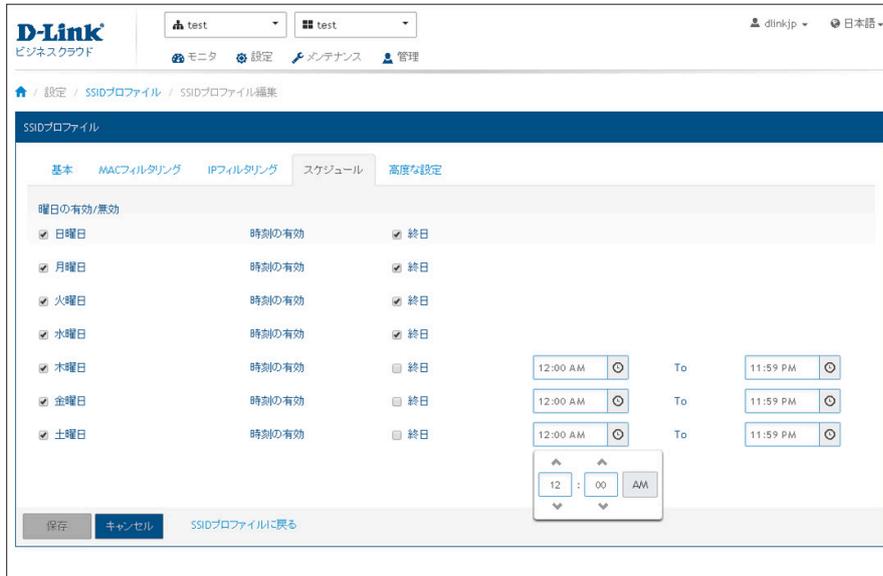


図 8-8 SSID プロファイル編集 (スケジュール) 画面

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

高度な設定 (SSID プロファイル編集)

「SSID プロファイル編集」で「高度な設定」タブを選択します。

「高度な設定」では SSID プロファイルの詳細設定を行います。

The screenshot shows the 'SSID プロファイル編集' (SSID Profile Edit) page in the '高度な設定' (Advanced Settings) tab. The page contains the following configuration items:

- 最大クライアント数: 64 (Range: 1 - 64)
- クライアントからの最大接続リトライ数: 5 (Range: 1 - 10)
- 最大上り帯域(Kbps): 0 (Range: 0 - 900000)
- 最大下り帯域(Kbps): 0 (Range: 0 - 900000)
- 最大クライアント上り帯域(Kbps): 0 (Range: 0 - 900000)
- 最大クライアント下り帯域(Kbps): 0 (Range: 0 - 900000)
- Bonjourパケットフォワーディング:
- IGMPスヌーピング有効:
- 最大マルチキャスト帯域(Kbps): 0 (Range: 0 - 900000)
- RTS閾値: 2347 (Range: 256 - 2347)
- フラグメント閾値: 2346 (Range: 257 - 2346)
- 強制ローミング:
- 電波強度閾値: (Range: -100 - 0)
- 低電波強度を許可:
- アソシエーションRSSI閾値: 5 (Range: 1 - 10)

Buttons at the bottom include '保存' (Save), 'キャンセル' (Cancel), and a link 'SSIDプロファイルに戻る' (Return to SSID Profile).

図 8-9 SSID プロファイル編集 (高度な設定) 画面

本画面には以下の項目があります。

項目	説明
最大クライアント数	接続するクライアントの最大数を指定します。1 - 64の間で指定できます。
クライアントからの最大接続リトライ数	最大クライアント数を越えた場合でも、クライアントからの接続を許容するクライアントの接続リトライ回数の条件を設定します。1-10の間で指定できます。
最大上り帯域 (Kbps) (SSID)	SSID のアップストリームの最大値を指定します。0 - 900000 (Kbps) で指定できます。
最大下り帯域 (Kbps) (SSID)	SSID のダウンストリームの最大値を指定します。0 - 900000 (Kbps) で指定できます。
最大クライアント上り帯域 (Kbps)	クライアントによるアップストリームの最大値を指定します。0 - 900000 (Kbps) で指定できます。クライアントの帯域設定が有効になった場合、機器の帯域設定より優先されます。SSID の帯域設定を有効にする場合、クライアントの帯域設定を 0 にする必要があります。
最大クライアント下り帯域 (Kbps)	クライアントによるダウンストリームの最大値を指定します。0 - 900000 (Kbps) で指定できます。クライアントの帯域設定が有効になった場合、機器の帯域設定より優先されます。SSID の帯域設定を有効にする場合、クライアントの帯域設定を 0 にする必要があります。
Bonjour パケットフォワーディング	クライアントからの Bonjour パケットフォワーディングを有効にします。
IGMP スヌーピング有効	マルチキャスト接続を構築する IGMP スヌーピングを有効にします。
最大マルチキャスト帯域 (Kbps)	マルチキャストトラフィックの最大値を指定します。0 - 900000 (Kbps) で指定できます。
RTS 閾値	送信者による RTS プロトコルを使用の際のフレームサイズ (RTS のしきい値) を指定します。主に隠れ端末問題などを解決します。256 - 2347 から指定できます。
フラグメント閾値	フラグメントの最大フレームサイズのしきい値を指定します。257 - 2346 から指定できます。それによりフレームを送信する時間を短縮し、データ破損の可能性を減少させます。
強制ローミング	有効にすると、クラウド AP によって認識されているクライアントの信号の強度が設定したしきい値を下回った場合、当該のクライアントはクラウド AP から切断されます。これによりクライアントにより信号強度の良い他の AP を検出するように促します。 注意 本設定は、クライアントがクラウド AP に接続する際に有効となります。クライアントがクラウド AP に接続後、電波強度が弱まった場合には適用されません。
電波強度閾値	「強制ローミング」が有効の場合、クライアントが設定されたしきい値を下回った場合に切断されるしきい値を指定します。-100-0 (dBm) から指定します。
低電波強度を許可	信号強度の弱いクライアントととの接続を許可します。クライアントが指定された時間、同じ AP への接続を試みている時などは、他に良いローミング対象がないと見なされるためです。
アソシエーション RSSI 閾値	接続には弱い信号強度のクライアントが AP への接続を試みる回数を指定します。1 - 10 で指定できます。

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

無線設定

「無線設定」ではチャンネルや無線出力の設定を当該のデバイスグループに対し行う事ができます。デバイスはデュアルバンド、つまり 2.4GHz と 5GHz の帯域から選択することが可能です。選択した操作帯域に基づいたモード選択によりレガシー接続、または 802.11n 接続のみ（または両方）を AP に設定することが可能です。

基本

無線設定の基本的な設定を行います。

設定 > 無線設定 > 基本 をクリックし、以下の画面を表示します。

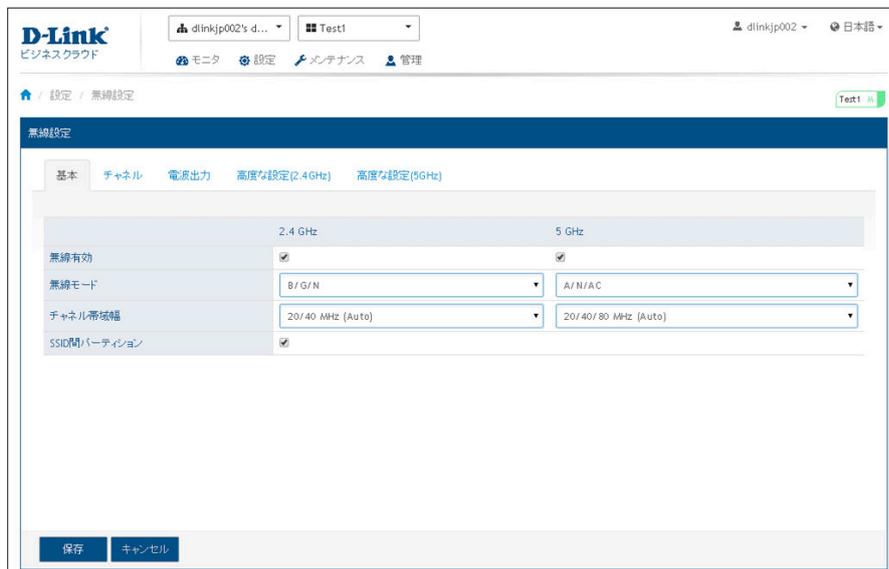


図 8-10 無線設定画面（基本）

本画面には以下の項目があります。

項目	説明
無線有効	デバイスグループに使用する無線帯域を「2.4GHz」「5GHz」から選択します。
無線モード	各帯域の無線モード（WiFi 操作モード）を「802.11」の「A」「B」「G」「N」「AC」とその組み合わせから選択します。
チャンネル帯域幅	各帯域のチャンネル帯域幅を「20」「40」「80」「20/40 (Auto)」「20/40/80 (Auto)」（MHz）から選択します。
SSID 間パーティション	有効にする事で、SSID 間での通信を禁止します。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

チャンネル

「チャンネル」では AP に対し自動的に環境内における最適なチャンネルを選択させます。「最適なチャンネル」とは最小限のノイズと送信ロスを実現する環境のことを意味します。クラウドの UI ではスキャンインターバルの設定も行うことが可能です。

設定 > 無線設定 > チャンネルをクリックし、以下の画面を表示します。

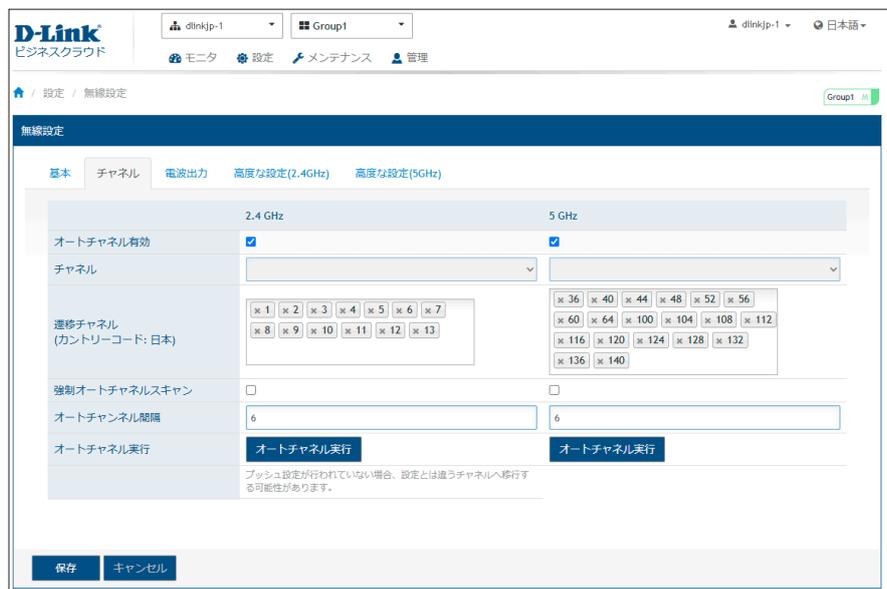


図 8-11 無線設定画面（チャンネル）

本画面には以下の項目があります。

項目	説明
オートチャンネル有効	チェックを入れるとオートチャンネルが有効になります。 「オートチャンネル有効」のチェックを外すと各帯域（2.4GHz と 5GHz）にチャンネルを選択する項目が表示されるので、それぞれの帯域でチャンネルを手動で選択します。
チャンネル	「オートチャンネル有効」でない場合に手動でチャンネルを選択します。
遷移チャンネル	オートチャンネル機能で利用するチャンネルを選択します。デフォルトでは、全てのチャンネルが選択された状態となっています。オートチャンネルで利用しないチャンネルは「×」ボタンをクリックすることで、オートチャンネル機能の対象チャンネルから除外する事ができます。また、対象チャンネル表示ボックスの空欄をクリックすることで、利用対象外に設定したチャンネルを表示することができます。利用対象外チャンネルをクリックすることで、利用対象チャンネルに戻す事ができます。 注意 レーダー検知や電波干渉による影響がある場合、設定した対象チャンネル以外のものが選択される場合があります。 注意 選択した遷移チャンネルに移行するには、オートチャンネルが動作する必要があります。オートチャンネルを手動で実行するか、定期オートチャンネル（最短 6 時間間隔）のいずれかが動作する必要があります。 注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。
強制オートチャンネルスキャン	オートチャンネルを強制的に実行する機能を有効にします。 有効にすると、クライアントが AP に接続している場合でも、オートチャンネルが実行されますが、通信に影響が出る場合がありますので、ご注意ください。
オートチャンネル間隔	オートチャンネルの実行間隔を指定します。一時間単位で 6-24 時間で設定することが可能です。
オートチャンネル実行	「オートチャンネル実行」をクリックすると、上記の設定とは関係なくクリックしたタイミングで、手動でオートチャンネルを開始します。 クリックすると「オートチャンネル実行中は Wi-Fi ネットワークが停止する可能性があります、本当に実行しますか」という確認画面が表示されるので、実行する場合のネットワークの停止を考慮してください。 注意 レーダー検知や電波干渉による影響がある場合、リアルタイムにオートチャンネルが実行されない場合もあります。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

電波出力

「電波出力」では AP の無線電波出力を増加（環境ノイズの解消目的）または減少（クライアント飽和とネットワーク環境への干渉の削減目的）を設定することが可能です。

設定 > 無線設定 > 電波出力をクリックし、以下の画面を表示します。

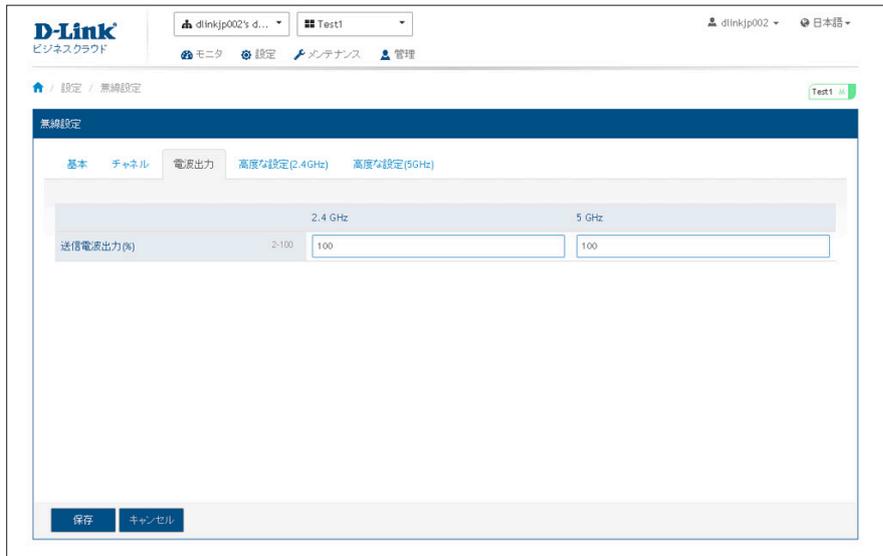


図 8-12 無線設定画面（電波出力）

本画面には以下の項目があります。

項目	説明
送信電波出力 (%)	各帯域（2.4GHz / 5GHz）の送信電波出力をそれぞれ「2-100」 (%) で指定します。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

高度な設定 (2.4GHz)

「高度な設定 (2.4GHz)」では 2.4GHz 帯での無線 AP をサポートする高度な設定を行います。スループットや出力に影響する使用環境の設定を行います。

設定 > 無線設定 > 高度な設定 (2.4GHz) をクリックし、以下の画面を表示します。

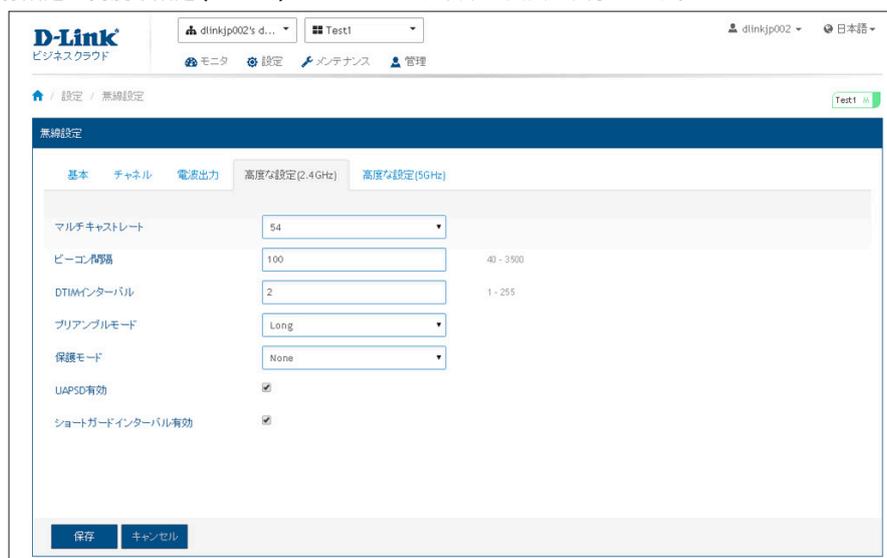


図 8-13 無線設定画面 (高度な設定 (2.4GHz))

本画面には以下の項目があります。

項目	説明
マルチキャストレート	クライアント接続のための最低限のクオリティを指定します。より少ない数値は接続されているクライアントからのより弱い信号強度を示しています。
ビーコン間隔	ビーコン間隔は無線レベル (ネットワーク情報を含む 802.11 の管理フレーム) におけるビーコン頻度を示します。40 - 3500 の間で指定します。
DTIM インターバル	DTIM インターバルは TIM (Traffic Indication Map) アクセスポイントのバッファされたマルチキャスト / ブロードキャストデータをクライアントに通知します。DTIM インターバルで設定したビーコン頻度にて情報は通知されます。1 - 255 の間で指定します。
プリアンブルモード	プリアンブル (前文) はネットワーク通信において二つ以上のシステム間の送信同期のタイミングのために使用する信号です。プリアンブルモードの信号の長さを「Long」「Short」から指定します。
保護モード	保護モードを指定します。「CTS-to-Self Protection」または「None」から指定します。保護モードに「CTS-to-Self Protection」を指定するとミックスモード (802.11n や g が混在するモード) などの環境で有効です。「802.11n」「802.11g」などの AP の信号がブロードキャストになります。ノイズの多い環境でのフレーム衝突を減少させます。
UAPSD 有効	「U-APSD」は「WMM パワーセーブ」としても知られる双方向出力保護のメカニズムです。音声無線 LAN 機器のショートガードインターバルを保護します。これらの技術は音声通話のような双方向トラフィックにも有効な技術です。
ショートガードインターバル有効	ショートガードインターバルを有効にします。

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

高度な設定 (5GHz)

「高度な設定 (5GHz)」では 5GHz 帯での無線 AP をサポートする高度な設定を行います。スループットや出力に影響する使用環境の設定を行います。

設定 > 無線設定 > 高度な設定 (5GHz) をクリックし、以下の画面を表示します。

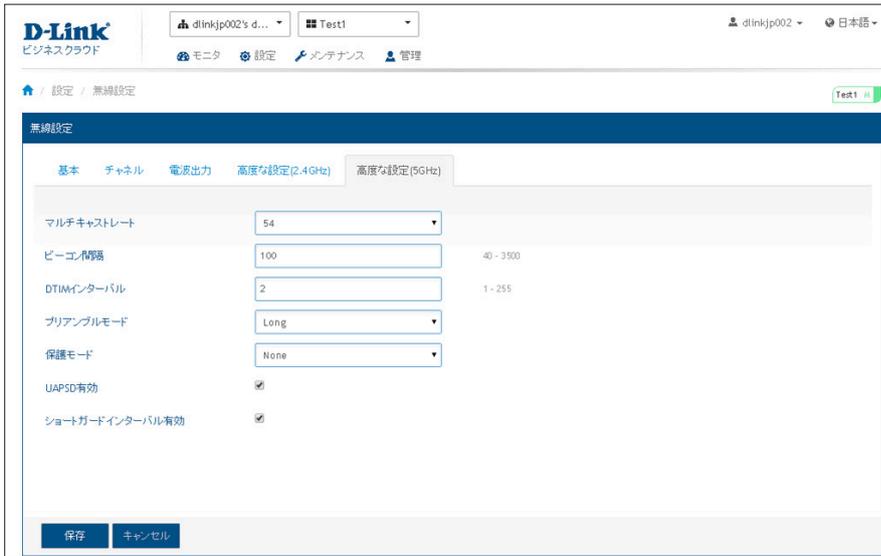


図 8-14 無線設定画面 (高度な設定 (5GHz))

本画面には以下の項目があります。

項目	説明
マルチキャストレート	クライアント接続のための最低限のクオリティを指定します。より少ない数値は接続されているクライアントからのより弱い信号強度を示しています。
ビーコン間隔	ビーコン間隔は無線レベル (ネットワーク情報を含む 802.11 の管理フレーム) におけるビーコン頻度を示します。40 - 3500 の間で指定します。
DTIM インターバル	DTIM インターバルは TIM (traffic indication map) アクセスポイントのバッファされたマルチキャスト/ブロードキャストデータをクライアントに通知します。DTIM インターバルで設定したビーコン頻度にて情報は通知されます。1 - 255 の間で指定します。
プリアンブルモード	プリアンブル (前文) はネットワーク通信において二つ以上のシステム間の送信同期のタイミングのために使用する信号です。プリアンブルモードの信号の長さを「Long」「Short」から指定します。
保護モード	保護モードを指定します。「CTS-to-Self Protection」または「None」から指定します。保護モードに「CTS-to-Self Protection」を指定するとミックスモード (802.11n や g が混在するモード) などの環境で有効です。「802.11n」「802.11g」などの AP の信号がブロードキャストになります。ノイズの多い環境でのフレーム衝突を減少させます。
UAPSD 有効	「U-APSD」は「WMM パワーセーブ」としても知られる双方向出力保護のメカニズムです。音声無線 LAN 機器のショートガードインターバルを保護します。これらの技術は音声通話のような双方向トラフィックにも有効な技術です。
ショートガードインターバル有効	ショートガードインターバルを有効にします。

「保存」をクリックして設定を保存します。デバイス (クラウド AP) への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

RADIUS 設定

RADIUS 認証を有効にした場合、RADIUS サーバがユーザを認証する場合のみ無線クライアントはアクセスを許可されます。

「RADIUS 設定」では新規 RADIUS サーバの追加、既存 / 新規 RADIUS サーバの設定、そしてサーバの稼働状況や設定情報の表示などを行います。SSID の無線クライアント認証は外部 RADIUS 認証サーバによって管理することが可能です。「WPA」「WPA2」セキュリティは認証方式を「事前共有鍵」(Pre-Shared Key/PSK) または「RADIUS サーバ」から選択することができます。

設定 > RADIUS 設定をクリックし、以下の画面を表示します。



図 8-15 RADIUS 設定画面（初期画面）

本画面には以下の項目があります。

項目	説明
Radius サーバリスト	「サーバ」は既存の RADIUS サーバ、「ポート」は当該サーバのポート番号を示します。 「アクション」をクリックすると、「編集」「削除」が表示され、「編集」をクリックすると当該 RADIUS サーバの「サーバ IP アドレス」「ポート番号」「シークレット (パスワード)」「キープアライブ有効」を設定することができます。 「削除」をクリックすると当該サーバを削除します。
新しい RADIUS サーバ	クリックすると追加する RADIUS サーバの設定項目が表示されます。既存 RADIUS サーバ編集時と項目内容は同じです。

RADIUS サーバの編集や新しい RADIUS サーバの設定詳細については「[RADIUS サーバの編集 / 新しい RADIUS サーバ](#)」を参照ください。

RADIUS サーバの編集 / 新しい RADIUS サーバ

新規、既存の RADIUS サーバの設定を行います。

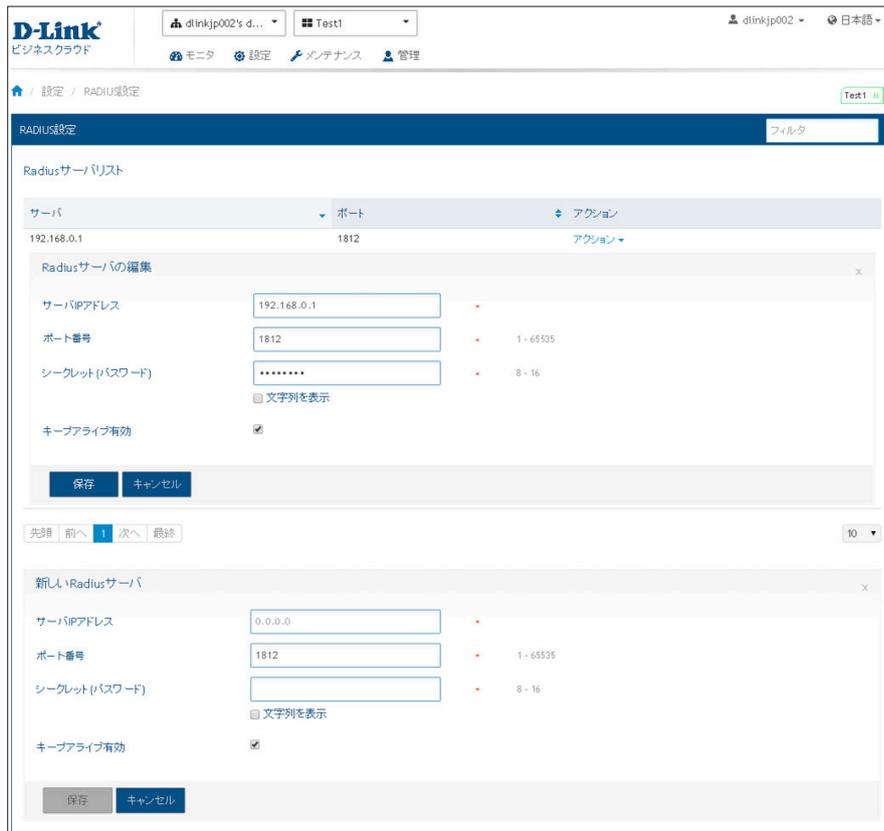


図 8-16 RADIUS 設定画面 (RADIUS サーバ編集時 / 新しい RADIUS サーバ設定時)

本画面には以下の項目があります。

項目	説明
サーバ IP アドレス	RADIUS サーバの IP アドレスです。
ポート番号	RADIUS サーバが実行しているポート番号です。初期値は「1645」が認証用、「1646」がアカウントリング用です。1 - 65535 から指定します。
シークレット (パスワード)	RADIUS サーバにログインするためのシークレット (パスワード) です。8 - 16 文字で指定します。「文字列を表示」にチェックを入れると入力する文字列が表示されます。
キープアライブ有効	無線クライアントサイドの「キープアライブ」メッセージを有効にします。

「保存」をクリックして設定を保存します。

注意 ブラウザ (Google Chrome) の設定により「サイトのパスワード保存」に関するダイアログが表示される場合がありますが、「使用しない」(保存しない) をクリックしてください。



図 8-17 パスワード保存の確認メッセージ

LDAP 設定

LDAP 設定を有効にすることで、LDAP サーバを利用したキャプティブポータルでのユーザ認証を実行することができます。

設定 > LDAP 設定をクリックし、以下の画面を表示します。



図 8-18 LDAP 設定 画面（初期画面）

本画面には以下の項目があります。

項目	説明
LDAP サーバリスト	「サーバ」は既存の LDAP サーバ、「ポート」は当該サーバのポート番号を示します。「アクション」をクリックすると、「編集」「削除」が表示され、「編集」をクリックすると当該 RADIUS サーバの「サーバ IP アドレス」「ポート番号」「バインド DN」を設定することができます。「削除」をクリックすると当該サーバを削除します。
新しい LDAP サーバ	クリックすると追加する LDAP サーバの設定項目が表示されます。既存 LDAP サーバ編集時と項目内容は同じです。

LDAP サーバの編集や新しい LDAP サーバの設定詳細については「LDAP サーバの編集 / 新しい LDAP サーバ」を参照ください。

LDAP サーバの編集 / 新しい LDAP サーバ

新規、既存の LDAP サーバの設定を行います。

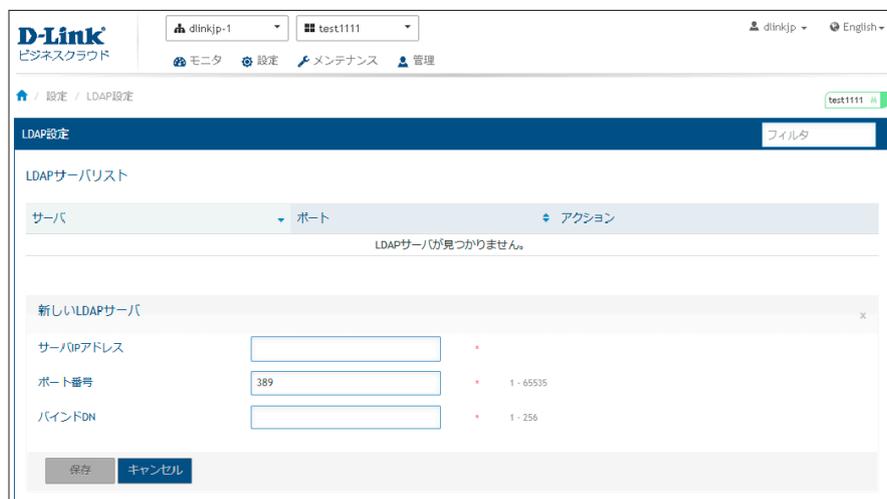


図 8-19 LDAP 設定 画面（LDAP サーバ編集時 / 新しい LDAP サーバ設定時）

本画面には以下の項目があります。

項目	説明
サーバ IP アドレス	LDAP サーバの IP アドレスです。
ポート番号	LDAP サーバが利用するポート番号です。初期値は「389」です。1 - 65535 から指定します。
バインド DN	LDAP サーバのバインド DN を指定します。

「保存」をクリックして設定を保存します。

キャプティブポータル

「キャプティブポータル」では無線クライアントのユーザによるクラウド AP へアクセスする際に、Web ページ（スプラッシュページ）を経由させ、アクセスの前に指定の情報をユーザに表示し対応させる機能です。このページは通常、追加の認証方法、またはネットワークからのサービス情報を表示し、クライアントのトラフィックはスプラッシュページでリクエストされた情報をユーザが提供した場合にのみに許可されます。キャプティブポータルの設定、追加により、ユーザにはスプラッシュページを経由させることでクラウドの認証メカニズムを追加させます。「新しいキャプティブポータル」をクリックすると新しくキャプティブポータル作成画面が表示されます。

Wi-Fi クライアントがキャプティブポータルを有効にした SSID に接続し、" 任意の Web サイト " にアクセスすると、スプラッシュページに自動的にリダイレクトされます。但し利用ブラウザによっては、" 任意の Web サイト " が SSL サイト (https サイト) の場合、スプラッシュページに正常にリダイレクトされないものもありますので、非 SSL サイト (http サイト) へアクセスする事を推奨します。

キャプティブポータルを SSID に適用するには、下記の設定が必要となります。

1. **メンテナンス > スプラッシュページの編集**で、キャプティブポータルで利用する Web ページを編集
2. **設定 > RADIUS 設定**で、ユーザ認証に使用する Radius サーバを指定 (Radius サーバを利用しない場合は不要)
3. **設定 > キャプティブポータル**で、キャプティブポータルのポリシーを定義
4. **設定 > SSID プロファイル**で、3 で設定したキャプティブポータルのポリシーを指定

設定 > キャプティブポータルをクリックし、以下の画面を表示します。



図 8-20 キャプティブポータル画面（初期画面）

本画面には以下の項目があります。

項目	説明
キャプティブポータル初期画面	
キャプティブポータル	既存のキャプティブポータル名が表示されます。
有効	当該キャプティブポータルの有効 / 無効ステータスが表示されます。
認証タイプ	当該キャプティブポータルの認証タイプを表示します。
アクション	「アクション」をクリックすると、「編集」「削除」が表示され、「編集」をクリックすると当該キャプティブポータルの設定内容を編集することができます。 「削除」をクリックすると当該キャプティブポータルを削除します。
新しいキャプティブポータル	クリックすると追加するキャプティブポータルの設定項目が表示されます。 既存のキャプティブポータル編集時と項目内容は同じです。

注意 タグ VLAN を設定している SSID では、キャプティブポータルはご利用頂けません。

キャプティブポータル編集 / 新しいキャプティブポータル

新規、既存のキャプティブポータルの設定を行います。

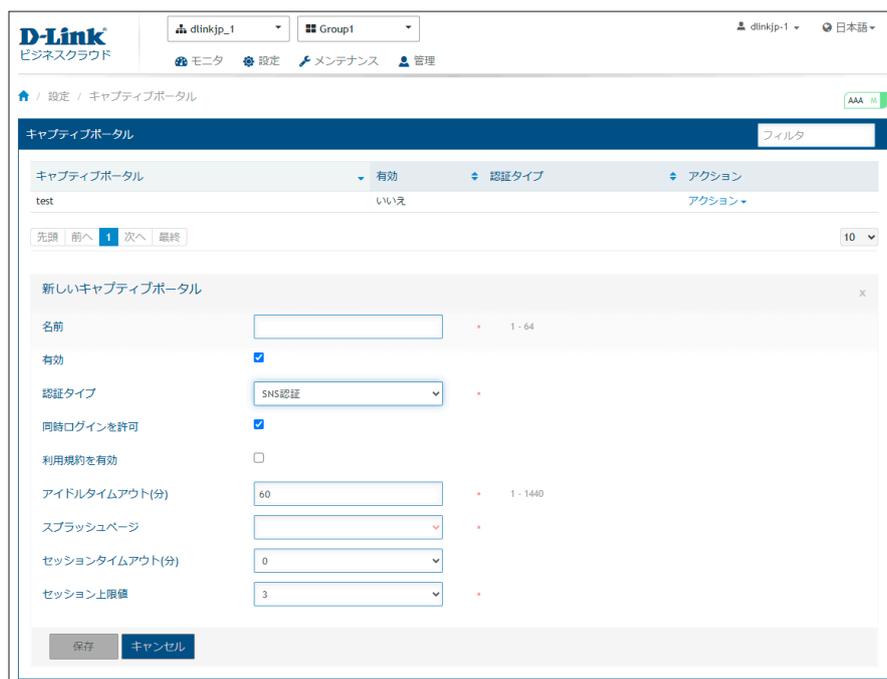


図 8-21 キャプティブポータル画面 (新しいキャプティブポータル / キャプティブポータル編集)

本画面には以下の項目があります。

項目	説明
新しいキャプティブポータル / キャプティブポータル編集画面	
名前	キャプティブポータルの名前を設定します。
有効	チェックを入れると当該のキャプティブポータルを有効にします。 Wi-Fi クライアントがキャプティブポータルを有効にした SSID に接続し、" 任意の Web サイト " にアクセスすると、splash ページに自動的にリダイレクトされます。但し利用ブラウザによっては、" 任意の Web サイト " が SSL サイト (https サイト) の場合、splash ページに正常にリダイレクトされないものもありますので、非 SSL サイト (http サイト) へアクセスする事を推奨します。 以下の設定項目はキャプティブポータルを「有効」にした時点で表示されます。
認証タイプ	キャプティブポータルがクライアントと接続するために使用する認証の種類を指定します。 認証タイプには以下の種類があります。 <ul style="list-style-type: none"> • RADIUS：お客様でご用意頂く外部 RADIUS サーバでユーザ認証を行います。 • ローカル DB：クラウド上 (メンテナンス / ローカル DB) で設定する ID・パスワードでユーザ認証を行います。 • クリックスルー：クラウド上 (メンテナンス > splash ページの編集) で設定するクリックスルーページのボタンを押すことで、上位ネットワークとの通信が許可されます。 • SNS 認証：SNS 認証機能、または E メール認証にて上位ネットワークとの通信が許可されます。SNS 認証は、Google、Facebook、LINE または Weibo アカウントを入力します。E メール認証ではメールアドレスを入力すると、一時的に上位ネットワークとの通信が可能になりますので、その間に認証用メールを受信し、認証を実施します。 • LDAP：お客様でご用意頂く外部 LDAP サーバでユーザ認証を行います。 <p>注意 「ローカル DB」「クリックスルー」は、ファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 「SNS 認証」「LDAP」は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 Weibo、E メール認証はファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
プライマリ認証クライアント名 セカンダリ認証クライアント名 プライマリ Accounting クライアント名 セカンダリ Accounting クライアント名	「認証タイプ」で「RADIUS」を選択時に表示されます。 「プライマリ / セカンダリ」のクライアント名と「プライマリ / セカンダリ」の Accounting クライアント名を指定します。設定する RADIUS クライアントは「設定 > RADIUS 設定」で事前に設定します。
プライマリ LDAP セカンダリ LDAP	「認証タイプ」で「LDAP」を選択時に表示されます。 「プライマリ / セカンダリ」の LDAP サーバを選択します。設定する LDAP サーバは「設定 > LDAP 設定」で事前に設定します。

「設定」メニュー

項目	説明
同時ログインを許可	<p>キャプティブポータルローカル DB 認証または E メール認証で、同一 ID または同一メールアドレスでのログイン申請が複数の無線 LAN クライアントからあった場合、ログインを許可するかどうかを指定します。</p> <p>注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 SNS 認証機能 (Facebook、Google、Line、Weibo) の場合、本項目の指定に関わらず同時ログインが許可された状態となります。</p>
利用規約を有効	利用規約を有効にします。
アイドルタイムアウト	認証クライアントが SSID を通じてトラフィックがない状態を続けて、認証セッションから切断されるまでの時間 (分) を指定します。「1 - 1440」まで指定できます。
スプラッシュページ	当該のキャプティブポータルに接続しようとした無線 LAN クライアントに表示する情報 / 警告メッセージを含むフロントページです。スプラッシュページは「メンテナンス > スプラッシュページ編集」で事前に設定します。
Facebook アカウントでのログイン	<p>有効にする事で、Facebook アカウントでの認証を実施することができます。</p> <p>注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 Facebook アカウントでの認証の場合、ユーザ情報が正しくイベントログ上に表示されない場合があります。</p>
Google アカウントでのログイン	<p>有効にする事で、Google アカウントでの認証を実施することができます。</p> <p>注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p>
LINE アカウントでのログイン	<p>有効にする事で、LINE アカウントでの認証を実施することができます。</p> <p>注意 本機能は、ファームウェアバージョン 1.50 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 iPhone 等の端末で LINE アカウントでの認証を実施する際、自動で LINE アプリに切り替わる場合があります。その場合は Safari 等のブラウザに手動で切り替え、表示される「ログイン画面」からログインを実施してください。</p> <p>注意 LINE アカウントでの認証の場合、ユーザ情報が正しくイベントログ上に表示されない場合があります。</p>
Weibo アカウントでのログイン	<p>有効にする事で、Weibo アカウントでの認証を実施することができます。</p> <p>注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
E メール認証の有効化	<p>有効にする事で、E メール認証を実施することができます。</p> <p>注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
E メール認証許容時間 (分)	<p>E メール認証で、無線利用者が認証メールを要求後、メール受信や認証を行うために一時的にインターネットに接続できる時間を設定します。</p> <p>注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
E メール認証許容回数	<p>E メール認証で、1 日の中で何回認証メールを要求できるかを指定します。</p> <p>注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
E メール認証拒否時間 (分)	<p>無線利用者が認証用メールを要求後、「E メール認証許容時間 (分)」で設定した時間内に認証が行われなかった場合、認証用メールの再要求を本項目で指定した時間拒否します。</p> <p>注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。</p>
セッションタイムアウト	<p>1 回の接続で、何分間接続が許容されるかを選択します。0 を選択すると無制限になります。</p> <p>注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p>
セッション上限値	<p>1 日の中で、何回接続を許容するかを選択します。0 を選択すると無制限になります。</p> <p>注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p>

「保存」をクリックして設定を保存します。

DHCP プール設定

「DHCP プール設定」では、NAT モードで利用するための DHCP アドレスプールの設定を行います。

注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。

設定 > DHCP プール設定をクリックし、以下の画面を表示します。

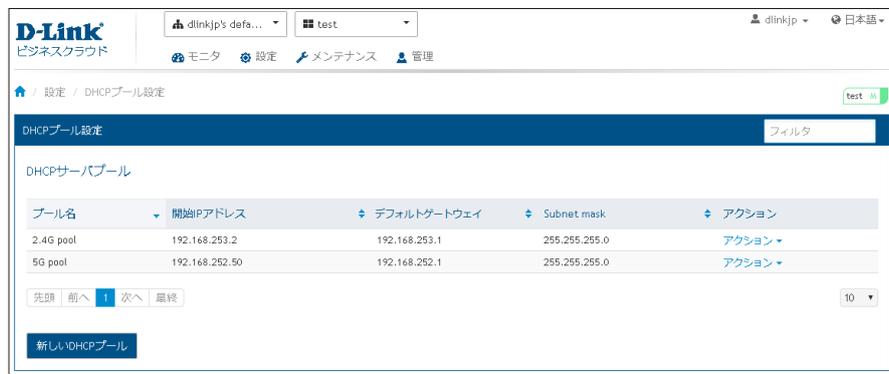


図 8-22 DHCP プール設定 画面

既存の DHCP プールの **アクション** > **編集** をクリックするか「新しい DHCP プール」をクリックし、新規、既存の DHCP プールの設定を行います。

DHCP プール編集 / 新しい DHCP プール

新規、既存の DHCP プールの設定を行います。

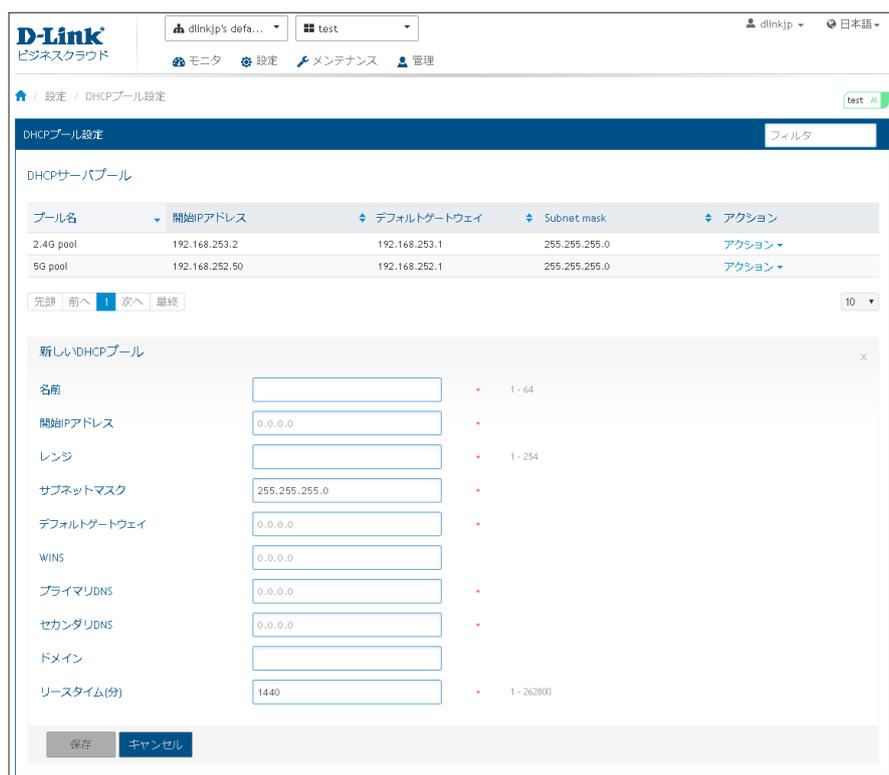


図 8-23 DHCP プール設定 (DHCP プール編集 / 新しい DHCP プール) 画面

本画面には以下の項目があります。

項目	説明
名前	任意の DHCP プールポリシー名を指定します。1~64 文字の間で指定します。
開始 IP アドレス	IP アドレスプールの一番最初の IP アドレスを指定します。
レンジ	IP アドレスプールのアドレス数を指定します。1~254 の間で指定します。
サブネットマスク	IP アドレスプールのサブネットを指定します。
デフォルトゲートウェイ	DHCP で配布するゲートウェイアドレスを指定します。
WINS	DHCP で配布する WINS サーバのアドレスを指定します。
DNS1	DHCP で配布するプライマリ DNS サーバのアドレスを指定します。

「設定」メニュー

項目	説明
DNS2	DHCP で配布するセカンダリ DNS サーバのアドレスを指定します。
ドメイン	DHCP で配布するドメイン名を指定します。
リースタイム (分)	DHCP で配布するリースタイムを指定します。1~262800 分の間で指定をします。

「保存」をクリックして設定を保存します。

一般設定

「一般設定」ではデバイスの Web GUI / CLI ユーザ名とパスワードの設定を行います。

設定 > 一般設定をクリックし、以下の画面を表示します。

図 8-24 一般設定画面

本画面には以下の項目があります。

項目	説明
ユーザ名	デバイスのユーザ名を表示します。
パスワード	パスワードを指定します。8-31 文字で指定できます。 「文字列を表示」にチェックを入れると入力する文字列が表示されます。
VLAN 有効	当該 SSID の VLAN を有効にします。
VLAN タイプ	VLAN の「タグ付き」「タグなし」を指定します。
VLAN タグ	VLAN タグの ID を指定します。
プロキシ経由で接続	DBA-1510P をプロキシサーバ経由でクラウドに接続するかどうかを指定します。 注意 無線 LAN クライアントをプロキシ経由でインターネットに接続する場合は、無線 LAN クライアントへのプロキシ設定が別途必要となります。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
プロキシサーバ	DBA-1510P が接続するプロキシサーバを指定します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
プロキシ ポート番号	DBA-1510P が接続するプロキシサーバのポート番号を指定します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTP サーバ 1	DBA-1510P の参照する、NTP サーバ 1 を指定します。 注意 デフォルト値は弊社 NTP サーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTP サーバ 2	DBA-1510P の参照する、NTP サーバ 2 を指定します。 注意 デフォルト値は弊社 NTP サーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTP サーバ 3	DBA-1510P の参照する、NTP サーバ 3 を指定します。 注意 デフォルト値は弊社 NTP サーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
IPv6 有効	DBA-1510P で IPv6 によるローカル設定を有効にするかどうかを指定します。

項目	説明
ローカル設定を優先	ローカル GUI や CLI から設定*された内容を、クラウド側の設定に関わらず優先適用するかどうかの指定をします。本機能を有効にする事で、IP アドレスや VLAN の変更をローカル設定だけの変更で実施することができます。ローカル設定の優先が有効になっている場合、クラウド側の設定*を変更・保存してプッシュ設定を行っても、クラウド側の設定は DBA-1510P に反映されません。デフォルト値は「ローカル設定を優先する」となっています。 ※本機能の対象となる設定項目は、DBA-1510P の「IP アドレス設定」「サブネットマスク設」「デフォルトゲートウェイ設定」「DNS 設定」「VLAN 設定」「IPv6 設定」「プロキシ設定」「NTP 設定」です。
タイムゾーン	ローカル設定を優先を無効にすると、デバイスのタイムゾーンを変更するための設定が表示されます。デフォルト値は日本時間 (GMT+9) です。デバイスのタイムゾーンを変更すると、SSID スケジュールの設定が、変更したタイムゾーンの時間で稼働するようになります。 注意 タイムゾーン設定は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。
LLMNR 有効	LLMNR の機能を無効にする場合、チェックを外してください。 注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。
Telnet 有効	Telnet での AP への接続を無効にする場合、チェックを外してください。 注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

注意 プロキシ設定が正しく設定されていないと、クラウドに接続する事ができませんのでご注意ください。

注意 NTP サーバが正しく設定されていないと、スケジュール機能が正常に動作しませんのでご注意ください。

注意 ローカル設定を優先する機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。DBA-1510P でファームウェアバージョン 1.00 を利用している場合、クラウド側の設定が常に優先されますのでご注意ください。

プッシュ設定

ビジネスクラウドに保存されたデバイスの設定を、デバイスグループ内のすべてのデバイスに適用します。

本機能はユーザに設定上の複数の変更を一回の設定動作で、デバイスグループ内の全デバイスに配信することができます。

設定 > プッシュ設定をクリックし、以下の画面を表示します。

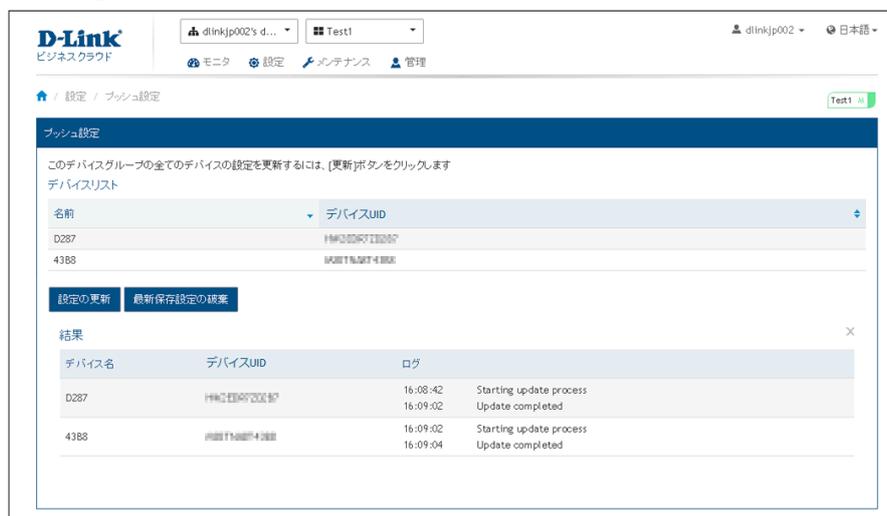


図 8-25 プッシュ画面

本画面には以下の項目があります。

項目	説明
名前	デバイスグループ内のデバイス名です。
デバイス UID	当該デバイスの識別番号（デバイス UID）です。
設定の更新	クリックするとデバイスに設定を適用します。クリックした後、画面下部に設定更新の「結果」が表示されます。
最新保存設定の破棄	クリックすると、クラウド上の最新保存設定を破棄し直近の「設定の更新」クリック済みの設定情報に戻ります。但しメンテナンスメニュー配下の設定は、最新の状態を保持し続けます。本操作で、DBA-1510P の設定情報は変更されません。
ログ	設定の更新ログです。更新結果、更新時間が表示されます。

注意 デバイスグループ内のデバイスの設定更新には「設定の更新」は必須です。クリックしない場合は機器の設定は更新されません。

注意 初期化された工場出荷状態の機器がクラウドに初めて接続した場合、「設定の更新」ボタンが押されていなくても、保存済みの最新の設定

が配信されます。

注意

設定変更を実施し設定を保存した後、「設定の更新」をクリックしない場合、GUIに「設定変更を既登録デバイスに適用するためには、プッシュ設定が必要です。新規登録デバイスには、保存された最新の設定が自動適用されますのでプッシュ設定は不要です。」というメッセージが表示されます。但し「メンテナンス>MAC データベース /IP データベース / ローカル DB/ スブラッシュページの編集」の設定を変更しても、本メッセージは表示されませんが、DBA-1510P に設定の変更を適用する場合には、「設定の更新」のクリックが必要となりますので、ご注意ください。

デバイスの設定

デバイスグループ内のデバイスの状態や使用率などを確認、さらに各デバイスの設定も個別に行う事が可能です。

注意

「デバイスの設定」で、個別のデバイスの設定を変更する場合、当該のデバイスのみデバイスグループの設定（Wi-Fi ポリシー）から変更され違う設定内容を保持するデバイスとなります。デバイスグループ内の設定を統一している場合はご注意ください。

「デバイスの設定」は「**モニタ > デバイス**」で表示されたデバイスリストにある各デバイスの「**詳細**」をクリックしても表示することができます。

デバイスの選択について



図 8-26 デバイスの選択

画面上部に表示されている「デバイス名」の右横の「▼」をクリックし、表示されたデバイス名から設定するデバイスを指定できます。

ステータス

デバイスのステータスについて表示します。

設定 > デバイスの設定 > ステータスをクリックし、以下の画面を表示します。

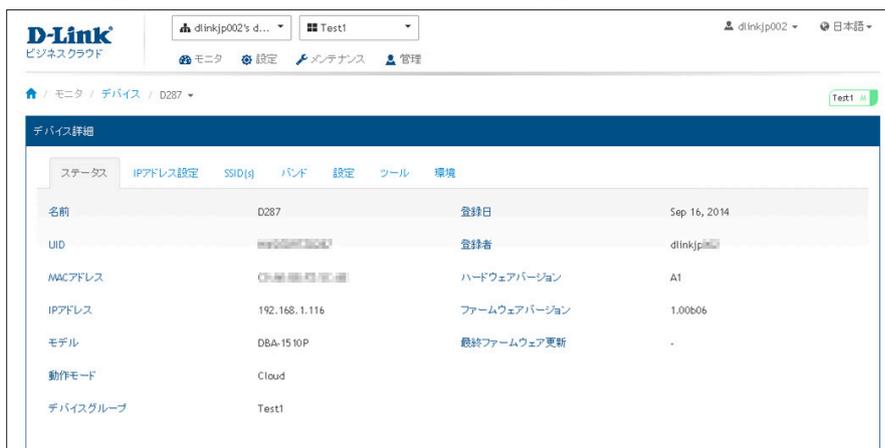


図 8-27 デバイスの設定画面（ステータス）

本画面には以下の項目があります。

項目	説明
名前	デバイスグループ内のデバイス名です。
UID	当該デバイスの UID（デバイス UID）です。
MAC アドレス	当該デバイスの MAC アドレスです。
IP アドレス	当該デバイスの IP アドレスです。
モデル	当該デバイスのモデル名です。
動作モード	当該デバイスの動作モードです。

項目	説明
デバイスグループ	当該デバイスが所属するデバイスグループです。
登録日	当該デバイスの登録日です。
登録者	当該デバイスの登録者（管理者）です。
ハードウェアバージョン	当該デバイスのハードウェアバージョンです。
ファームウェアバージョン	当該デバイスのファームウェアバージョンです。
最終ファームウェア更新	当該デバイスの最後にファームウェアを更新した日です。

IP アドレス設定

デバイスの IP アドレスについて表示、設定します。

設定 > デバイスの設定 > IP アドレス設定をクリックし、以下の画面を表示します。

図 8-28 デバイスの設定画面 (IP アドレス設定)

本画面には以下の項目があります。

項目	説明
アドレスタイプ	当該デバイスのアドレスの種類です。「DHCP」「Static」から指定します。「Static」を指定すると「VLAN 有効」以外の以下の項目が表示されます。
IP アドレス	当該デバイスの IP アドレスを指定します。
サブネットマスク	当該デバイスのサブネットマスクを指定します。
プライマリ DNS アドレス	当該デバイスのプライマリ DNS アドレスを指定します。
セカンダリ DNS アドレス	当該デバイスのセカンダリ DNS アドレスを指定します。
サード DNS アドレス	当該デバイスのサード DNS アドレスを指定します。
デフォルトゲートウェイ	当該デバイスのデフォルトゲートウェイを指定します。
VLAN 有効	当該デバイスの VLAN を有効にします。
VLAN タイプ	有効にした VLAN の種類を指定します。「Tagged」(タグ付き)「Untagged」(タグなし)から指定します。
VLAN タグ	有効にした VLAN のタグ番号を指定します。1 - 4097 の間で指定できます。
プロキシ経由で接続	DBA-1510P をプロキシサーバ経由でクラウドに接続するかどうかを指定します。 注意 無線 LAN クライアントをプロキシ経由でインターネットに接続する場合は、無線 LAN クライアントへのプロキシ設定が別途必要となります。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。

「設定」メニュー

項目	説明
プロキシサーバ	DBA-1510P が接続するプロキシサーバを指定します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
プロキシポート番号	DBA-1510P が接続するプロキシサーバのポート番号を指定します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTPサーバ1	DBA-1510P の参照する、NTPサーバ1を指定します。 注意 デフォルト値は弊社 NTPサーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTPサーバ2	DBA-1510P の参照する、NTPサーバ2を指定します。 注意 デフォルト値は弊社 NTPサーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
NTPサーバ3	DBA-1510P の参照する、NTPサーバ3を指定します。 注意 デフォルト値は弊社 NTPサーバになっていますので、そのままご利用頂く事を推奨します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
グループ設定を使用	「グループ設定」にチェックがある場合、当該デバイスにおいて、デバイスグループでの設定が有効になります。当該デバイス独自に設定変更を行う場合には、本設定を無効化する必要があります。初期値は有効になっています。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

注意 プロキシ設定が正しく設定されていないと、クラウドに接続する事ができませんのでご注意ください。

注意 NTPサーバが正しく設定されていないと、スケジュール機能が正常に動作しませんのでご注意ください。

SSID(s)

デバイスの SSID について表示、設定します。

設定 > デバイスの設定 > SSID(s) をクリックし、以下の画面を表示します。

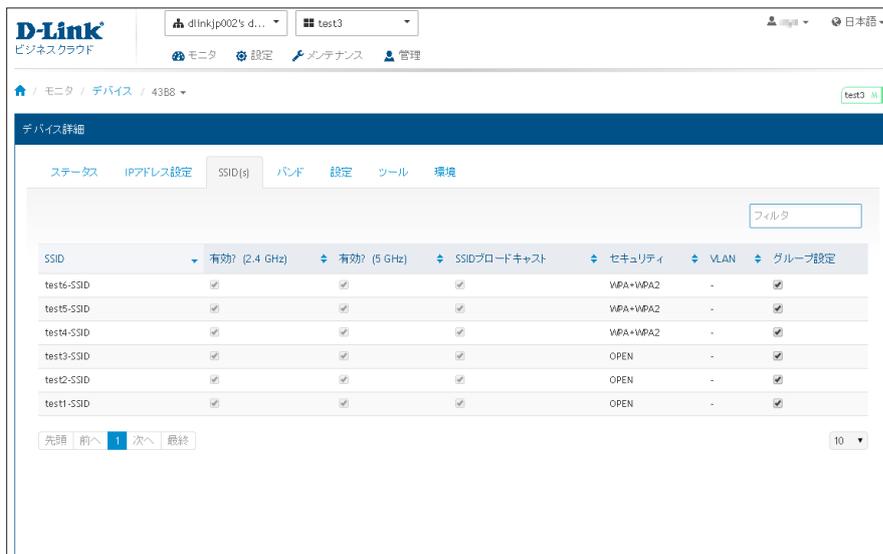


図 8-29 デバイスの設定画面 (SSID(s))

本画面には以下の項目があります。

項目	説明
フィルタ	SSID のリストにフィルタをかけて SSID を絞り込みます。 SSID 名の他にセキュリティの種類など（WPA 等）でも絞り込むことが可能です。
SSID	SSID 名です。
有効 (2.4 GHz)	当該 SSID が 2.4GHz 帯で有効な場合チェックがあります。チェックを外すとその時点で無効になります。
有効 (5 GHz)	当該 SSID が 5GHz 帯で有効な場合チェックがあります。チェックを外すとその時点で無効になります。
SSID ブロードキャスト	当該 SSID の SSID ブロードキャストが有効な場合チェックがあります。チェックを外すとその時点で無効になります。
セキュリティ	当該デバイスの設定セキュリティを表示します。
VLAN	当該デバイスの設定 VLAN を指定します。

項目	説明
グループ設定	「グループ設定」にチェックがある場合、当該 SSID に対して所属するデバイスグループでの設定が有効になります。これは初期値で設定されており、すべてのデバイスグループ内の SSID に対しチェックがあります。このチェックを外すことにより、特定の SSID に対してデバイスグループでの設定を無効にし、デバイス個別の設定を行うことができます。

バンド

デバイスのバンド（帯域）について表示、設定します。

設定 > デバイスの設定 > バンドをクリックし、以下の画面を表示します。

図 8-30 デバイスの設定画面（バンド）

本画面には以下の項目があります。

項目	説明
無線有効	各帯域の無線機能を有効/無効にします。
送信電波出力 (%)	各帯域の送信電波出力を「2-100」(%) で指定します。
無線モード	各帯域の無線モード (WiFi 操作モード) を「802.11」の「A」「B」「G」「N」「AC」とその組み合わせから選択します。
チャンネル帯域幅	各帯域のチャンネル帯域幅を「20」「40」「80」「20/40 (Auto)」「20/40/80 (Auto)」(MHz) から選択します。
オートチャンネル有効	チェックを入れるとオートチャンネルが有効になります。「オートチャンネル有効」のチェックを外すと各帯域(2.4GHzと5Ghz)にチャンネルを選択する項目が表示されるので、それぞれの帯域でチャンネルを手動で選択します。
チャンネル	「オートチャンネル有効」でない場合に手動でチャンネルを選択します。
遷移チャンネル	<p>オートチャンネル機能で利用するチャンネルを選択します。デフォルトでは、全てのチャンネルが選択された状態となっています。オートチャンネルで利用しないチャンネルは「×」ボタンをクリックすることで、オートチャンネル機能の対象チャンネルから除外する事ができます。また、対象チャンネル表示ボックスの空欄をクリックすることで、利用対象外に設定したチャンネルを表示することができます。利用対象外チャンネルをクリックすることで、利用対象チャンネルに戻す事ができます。</p> <p>注意 レーダー検知や電波干渉による影響がある場合、設定した対象チャンネル以外のものが選択される場合があります。</p> <p>注意 選択した遷移チャンネルに移行するには、オートチャンネルが動作する必要があります。オートチャンネルを手動で実行するか、定期オートチャンネル（最短6時間間隔）のいずれかが動作する必要があります。</p> <p>注意 本機能は、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p>

「設定」メニュー

項目	説明
強制オートチャネルスキャン	<p>オートチャネルを強制的に実行する機能を有効にします。</p> <p>注意 有効にするとクライアントが AP に接続している場合でもオートチャネルが実行されますが、通信に影響が出る場合がありますのでご注意ください。</p> <p>注意 クリックすると「オートチャネル実行中は Wi-Fi ネットワークが停止する可能性があります、本当に実行しますか」という確認画面が表示されます。実行する場合のネットワーク停止を考慮し、実行する必要があります。</p>
オートチャネル間隔	<p>オートチャネルの実行間隔を指定します。一時間単位で 6-24 時間で設定することが可能です。</p>
オートチャネル実行	<p>「オートチャネル実行」をクリックすると、上記の設定とは関係なくクリックしたタイミングで、手動でオートチャネルを開始します。</p> <p>注意 クリックすると「オートチャネル実行中は Wi-Fi ネットワークが停止する可能性があります、本当に実行しますか」という確認画面が表示されます。実行する場合のネットワーク停止を考慮し、実行する必要があります。</p>
グループ設定を使用	<p>「グループ設定」にチェックがある場合、当該デバイスにおいて、デバイスグループでの設定が有効になります。当該デバイス独自に設定変更を行う場合には、本設定を無効化する必要があります。初期値は有効になっています。</p>

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「**設定 > プッシュ設定**」での「設定の更新」が必要です。

設定

デバイスの一般設定について表示、設定します。

設定 > デバイスの設定 > 設定をクリックし、以下の画面を表示します。

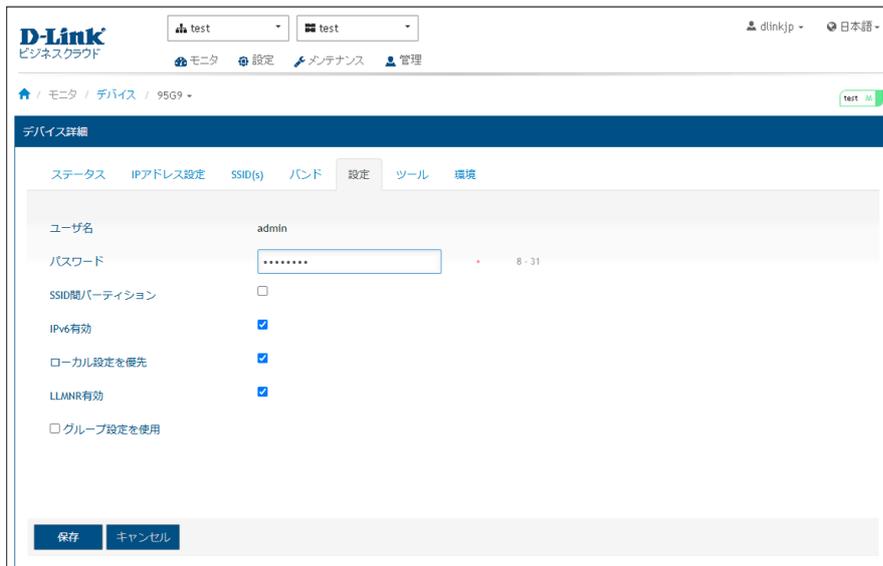


図 8-31 デバイスの設定画面（設定）

本画面には以下の項目があります。

項目	説明
ユーザ名	ユーザ名です。「admin」から変更することはできません。
パスワード	パスワードを指定します。8-31 文字で指定できます。「文字列を表示」にチェックを入れると入力する文字列が表示されます。
SSID 間パーティション	有効にする事で、SSID 間の通信を禁止します。
IPv6 有効	DBA-1510P で IPv6 によるローカル設定を有効にするかどうかを指定します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
LLMNR 有効	LLMNR を有効にするかどうかを指定します。 注意 本機能はファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。

項目	説明
ローカル設定を優先	ローカル GUI や CLI から設定*された内容を、クラウド側の設定に関わらず優先適用するかどうかの指定をします。本機能を有効にする事で、IP アドレスや VLAN の変更をローカル設定だけの変更で実施することができます。ローカル設定の優先が有効になっている場合、クラウド側の設定*を変更・保存してプッシュ設定を行っても、クラウド側の設定は DBA-1510P に反映されません。デフォルト値は優先する設定となっています。 ※本機能の対象となる設定項目は、DBA-1510P の「IP アドレス設定」「サブネットマスク設」「デフォルトゲートウェイ設定」「DNS 設定」「VLAN 設定」「IPv6 設定」「プロキシ設定」「NTP 設定」です。 注意 ローカル設定を優先する機能は、ファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。DBA-1510P でファームウェアバージョン 1.00 を利用している場合、クラウド側の設定が常に優先されますので、ご注意ください。
グループ設定を使用	「グループ設定」にチェックがある場合、当該デバイスにおいて、デバイスグループでの設定が有効になります。当該デバイス独自に設定変更を行う場合には、本設定を無効化する必要があります。初期値は有効になっています。

「保存」をクリックして設定を保存します。デバイス（クラウド AP）への設定の適用には「設定 > プッシュ設定」での「設定の更新」が必要です。

ツール

デバイスのツールについて表示、設定します。

本項目ではデバイスに対し「Ping」や「Traceroute」などの診断ツールを使用して接続性を確認することが可能です。それ以外にも LED の点滅などデバイスがビジネスクラウドからの操作に対応しているか確認するための便利なツールを使用することが可能です。

設定 > デバイスの設定 > ツールをクリックし、以下の画面を表示します。

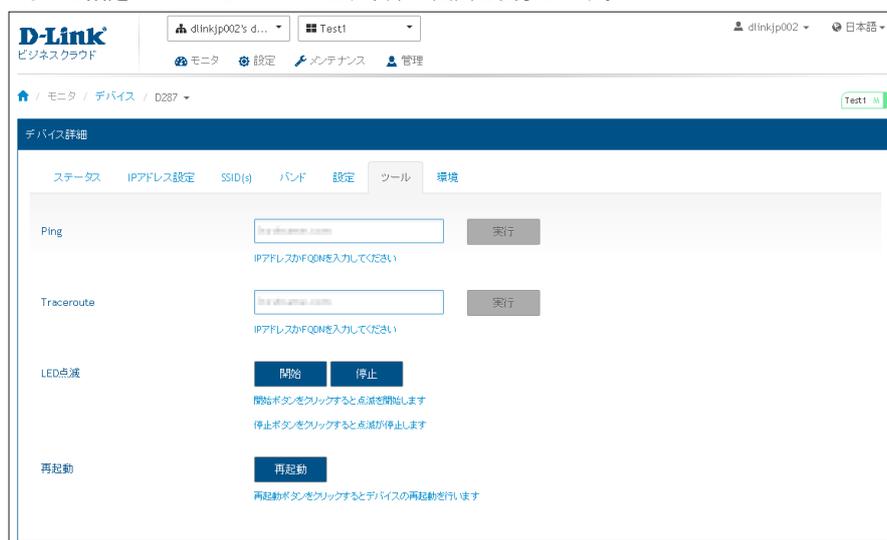


図 8-32 デバイスの設定画面（ツール）

本画面には以下の項目があります。

項目	説明
Ping	Ping を実行します。IP アドレスかドメイン名を入力し実行をクリックします。指定のデバイスに対する接続性を確認することが可能です。
Traceroute	Traceroute を実行します。経路を確認する宛先デバイスの IP アドレスかドメイン名を入力し実行をクリックします。宛先デバイスに対し Traceroute は実行され、デバイスも応答します。Traceroute の出力は宛先ピアにコンタクトするデバイスのネットワーク経路を表示します。
LED 点滅	「開始」をクリックすると当該デバイスの LED が点滅を開始します。 「停止」をクリックすると当該デバイスの LED が点滅が停止します。
Telnet	設定 > 一般設定 にて「TELNET」項目にチェックが入っていない場合に表示されます。 「有効」をクリックすることで、60 分間 TELNET 接続が有効になります。60 分経過すると自動的に TELNET 接続は無効となります。60 分経過前でも「無効」をクリックすることで、即時に無効化されます。 注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。
Wi-Fi 設定取得	CLI 上で Wi-Fi の設定を取得できる状態にします。 注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。
再起動	「再起動」をクリックするとデバイスの再起動を行います。

注意 本機能の使用にはデバイスと接続するルータや Firewall で「ICMP プロトコル」が許可されている必要があります。

環境

デバイスの環境について表示、設定します。

本項目では必要に応じたデバイスの無線スキャンの結果を表示します。「スキャン」をクリックするとデバイスの周囲環境が表示されます。スキャンはクライアント通信に影響が出る場合がありますので、充分ご注意ください。

設定 > デバイスの設定 > 環境をクリックし、以下の画面を表示します。

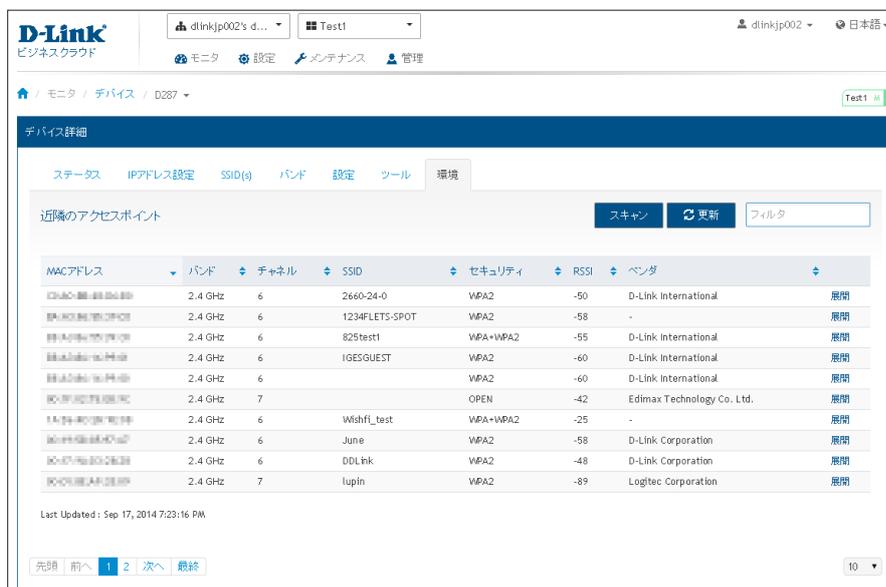


図 8-33 デバイスの設定画面（環境）

本画面には以下の項目があります。

項目	説明
スキャン	スキャンをクリックすると近隣のデバイスを検出します。
更新	更新をクリックすると検出したデバイスのリストを更新します。
フィルタ	デバイスのリストにフィルタをかけてデバイスを絞り込みます。 デバイス名の他にセキュリティの種類など（WPA 等）でも絞り込むことが可能です。
MAC アドレス	デバイスの MAC アドレスです。
バンド	デバイスの使用しているバンド（帯域）です。
チャンネル	デバイスの使用しているチャンネルです。
SSID	デバイスの使用している SSID です。
セキュリティ	デバイスの使用しているセキュリティ方式です。
RSSI	デバイスの RSSI の値です。
ベンダ	デバイスの製造ベンダです。
展開をクリックすると以下の項目も表示されます。	
無線 LAN 方式	デバイスの使用している無線 LAN 方式です。
有線ネットワークでの検出	デバイスが有線ネットワークで検出されたかどうかの状況です。
BSSID	デバイスの BSSID です。

第9章 「メンテナンス」メニュー（D-Link Business Cloud）

本章では「D-Link Business Cloud」の「メンテナンス」メニューの説明を行います。

以下は本章「メンテナンス」メニューのサブメニューの説明です。必要に応じて、設定/変更/修正を行ってください。

サブメニュー	説明
MAC データベース	特定のデバイスグループのSSID プロファイルに MAC アドレスのリストを設定し、MAC アドレスでのアクセス認証を SSID に適用します。
IP データベース	IP フィルタリング機能で使用する IP アドレス・サブネットデータベースを作成・管理します。 注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。
ローカル DB	キャプティブポータルでローカル DB 認証で使用するユーザ ID・パスワードを設定します。 注意 本機能はファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。
スプラッシュページ編集	キャプティブポータルなどで使用するスプラッシュページの作成、編集または削除を行います。
ファームウェア	デバイスの新しいファームウェアをアップグレードできます。「ファームウェア管理」ではファームウェアのアップグレードとともに、対応可能なファームウェアバージョンの選択などを行います。
設定の複製	デバイスグループで設定した設定内容（グループコンフィグ）を他のデバイスグループ（新規/既存）にも適用します。

「メンテナンス」メニューからサブメニューを選択します。



図 9-1 「メンテナンス」メニュー

MAC データベース

MAC データベースでは特定のデバイスグループに属する SSID プロファイルに適用する MAC アドレスのリストを設定します。

デバイスグループ内のデバイスに使用されるリストは無線クライアントの MAC アドレスを元に接続を許可 / 拒否されます。クライアント認証は二つのプロセスを経ることになり、まず SSID プロファイルによる認証、そして MAC アドレスリストによる認証という二つのセキュリティになります。

MAC データベースは以下の図の左側ボックスに表示されます。MAC データベース内のデバイスリストはデータベースリストの右側に表示されます。

メンテナンス > MAC データベースをクリックし、以下の画面を表示します。

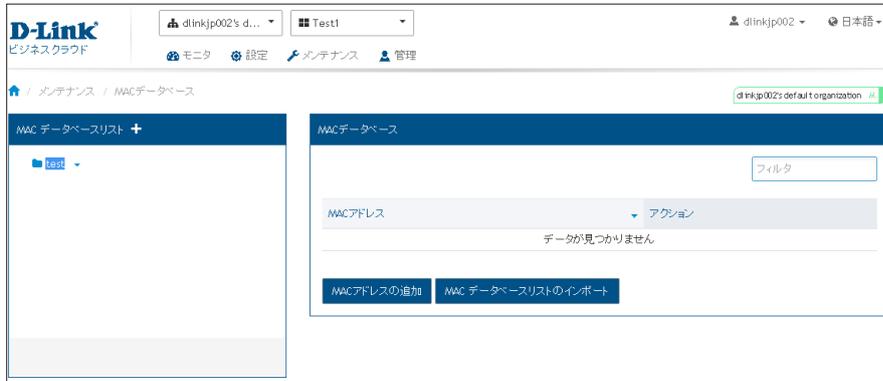


図 9-2 MAC データベース画面

本画面には以下の項目があります。

項目	説明
MAC データベースリスト+	
MAC データベースリスト名	リスト名の右端の「▼」をクリックすると当該リストの「リストの編集」「リストの削除」「リストの複製」が表示され、それぞれでリストに対する動作を実行します。一つの MAC リストも作成していない場合「+」クリックしてリストを追加します。その際に「名前」「説明」を入力します。 <ul style="list-style-type: none"> リストの編集 - MAC データベースリストを編集します。「名前」「説明」を入力します。 リストの削除 - MAC データベースリストを削除します。確認画面は出ないのでご注意ください。 リストの複製 - MAC データベースリストを複製します。「名前」「説明」を入力します。
MAC データベース	
フィルタ	MAC アドレスのリストにフィルタをかけて MAC アドレスを絞り込みます。
MAC アドレス	左側の MAC データベースリストで選択している MAC データベースリストの MAC アドレスを表示します。
アクション	当該の MAC アドレスに対する動作を実行します。🗑️(ごみ箱アイコン)をクリックすると MAC アドレスの削除を行います。
MAC アドレスの追加	選択中の MAC データベースリストに MAC アドレスを追加します。クリックすると MAC アドレスの入力欄が表示されます。MAC アドレスは、大文字とコロンで入力してください。
MAC データベースリストのインポート	MAC データベースリストファイルのインポートを行います。クリックすると「CSV ファイルのインポート」項目が表示され、「参照 / ファイルを選択」をクリックし CSV ファイル形式の MAC データベースリストファイルを参照します。CSV ファイルの文字コードは UTF-8 を利用してください。

MAC データベースの CSV ファイルについて

インポートする MAC データベースの CSV ファイルは以下のような形式で作成します。

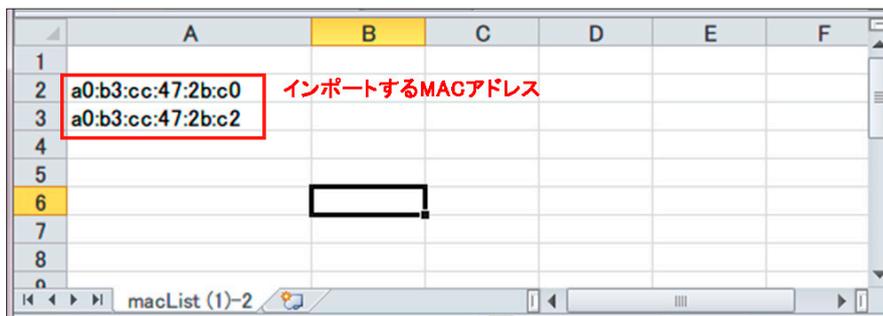


図 9-3 MAC データベースの CSV ファイル画面

IP データベース

本項目は、IP フィルタリング機能で使用する IP アドレス・ネットワークの作成・管理のために使用します。

IP フィルタリング機能 (SSID 設定) を有効にすることで、IP データベースに登録した IP アドレス、ネットワーク宛ての通信を、許可・拒否する事が可能になります。

注意 本機能はファームウェアバージョン 1.01 以上が DBA-1510P にインストールされている必要があります。

メンテナンス > IP データベース をクリックし、以下の画面を表示します。

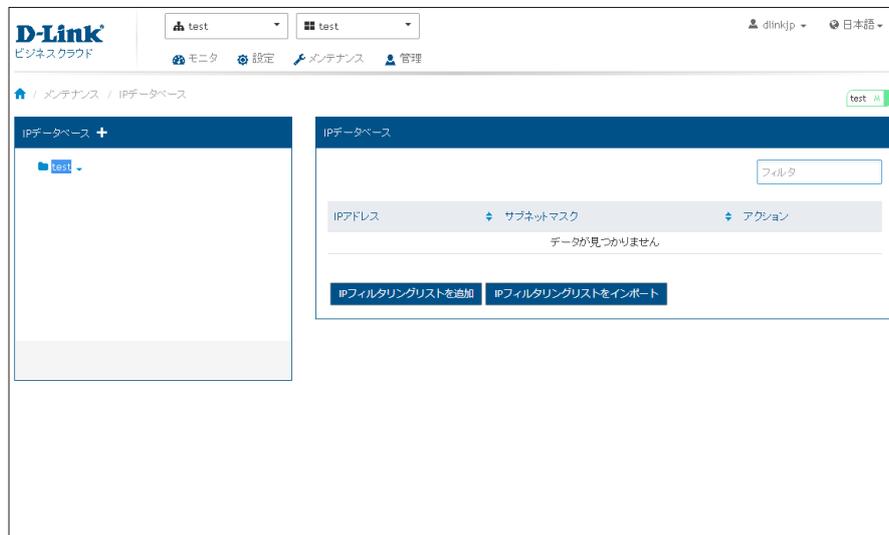


図 9-4 IP データベース編集画面

本画面には以下の項目があります。

項目	説明
IP データベース+	IP データベースの作成、編集、削除を行います。
IP データベース	IP フィルタリング機能で対象とする、IP アドレス、ネットワークを登録します。 IP フィルタリング機能 (SSID 設定) を有効にすることで、IP データベースに登録した IP アドレス、ネットワーク宛ての通信を、許可・拒否する事が可能になります。
IP フィルタリングリストを追加	クリックして「IP データベース+」で選択した IP データベースに IP アドレスを追加します。 IP アドレスとサブネットマスクをダイアログに入力後、保存をクリックします。
IP フィルタリングリストをインポート	クリックして「IP データベース+」で選択した IP データベースに CSV ファイルの IP アドレスリストを追加します。 ファイルを選択し「保存」をクリックします。

ローカル DB

本項目は、キャプティブポータル ローカル DB 認証のために使用します。

キャプティブポータル ローカル DB 認証を有効にすると、本項目で設定した「ユーザ ID」「パスワード」で、キャプティブポータルでのユーザ認証を行う事ができます。外部 Radius サーバの設置をしなくてもキャプティブポータルのユーザ認証を行う事ができます。

本項目で設定された「ユーザ ID」「パスワード」は、DBA-1510P に転送され、DBA-1510P がローカルでユーザ認証を行うためクラウドと通信ができない状態でも、キャプティブポータルを利用する事ができます。

注意 本機能はファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。

メンテナンス > ローカル DB をクリックし、以下の画面を表示します。



図 9-5 ローカル DB 画面

本画面には以下の項目があります。

項目	説明
ローカル DB +	ローカル DB の作成、編集、削除を行います。
ローカル DB	キャプティブポータルローカル DB 認証で利用する「ユーザ ID」「パスワード」を登録します。
ローカル DB エントリを追加	クリックすることで、GUI から「ユーザ ID」「パスワード」を登録できます。
ローカル DB エントリをインポート	ユーザ ID・パスワードを含む CSV ファイルをアップロードする事で「ユーザ ID」「パスワード」を一括登録する事ができます。

注意 ブラウザ (Google Chrome) の設定により「サイトのパスワード保存」に関するダイアログが表示される場合がありますが、「使用しない」(保存しない) をクリックしてください。



図 9-6 パスワード保存の確認メッセージ

スプラッシュページ編集

本項目ではスプラッシュページを作成、編集または削除するか、事前に定義済みのスプラッシュページのテンプレートを使用します。ユーザはテンプレートの以下の項目をカスタマイズすることが可能です。

- ・ ロゴ
- ・ バックグラウンドの色と画像
- ・ タイトルとサブタイトル
- ・ メッセージ

スプラッシュページ編集画面では以下をサポートしています。

- ・ キャプティブ Web ポータルとその ID/パスワード
- ・ 警告のみのクリックスルースプラッシュページ / 情報

メンテナンス > スプラッシュページ編集をクリックし、以下の画面を表示します。

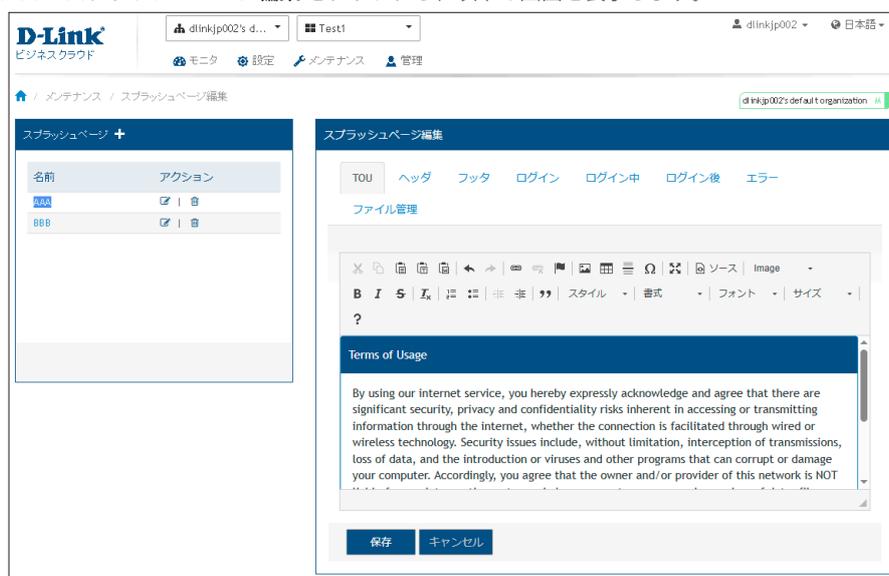


図 9-7 スプラッシュページ編集画面

本画面には以下の項目があります。

項目	説明
スプラッシュページ+	
スプラッシュページ名	編集するスプラッシュページを選択し、右側の「スプラッシュページ編集」ボックスでスプラッシュページの編集を行います。スプラッシュページ名の右端の「  」（ごみ箱アイコン）をクリックすると当該スプラッシュページを削除します。スプラッシュページを一つも作成していない場合「+」をクリックしてスプラッシュページを追加します。その際に「名前」「タイプ」「説明」を入力します。「タイプ」には、「Sign-On」「クリックスルー」「Sign-On-Third-Party」「SNS 認証」の 4 種類があり、ユーザ認証を行うためのスプラッシュページ作成の場合「Sign-On」を選択し、クリックスルーを行うためのスプラッシュページ作成の場合は、「クリックスルー」を選択します。またユーザ認証と SNS 認証、E メール認証を行うためのスプラッシュページ作成の場合は、「Sign-On-Third-Party」、SNS 認証や E メール認証を行うためのスプラッシュページ作成の場合には、「SNS 認証」を選択します。 注意 「Sign-On-Third-Party」、「SNS 認証」を利用するには、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。 注意 E メール認証を利用するには、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。
スプラッシュページ編集	
TOU	スプラッシュページの Terms of Usage ページを作成 / 編集します。
ヘッダ	スプラッシュページのヘッダについて作成 / 編集します。
フッタ	スプラッシュページのフッタについて作成 / 編集します。
ログイン	ログイン画面のスプラッシュページを作成 / 編集します。 (「スプラッシュページ+」の「タイプ」選択時に「Sign-On」を選択した場合にのみ表示されます。)
クリックスルー	スプラッシュページのクリックスルーページを作成、編集します。 (「スプラッシュページ+」の「タイプ」選択時に「クリックスルー」を選択した場合にのみ表示されます。)
ログイン中	ログイン中のスプラッシュページを作成 / 編集します。
ログイン後	ログイン後のスプラッシュページを作成 / 編集します。

項目	説明
エラー	エラー発生時のスプラッシュページを作成 / 編集します。
ファイル管理	スプラッシュページに使用する画像ファイルを管理します。 <ul style="list-style-type: none"> ファイル名 - スプラッシュページに使用しているファイルを表示しています。 ファイルのアップロード - スプラッシュページに使用するファイルをアップロードします。「参照 / ファイルを選択」をクリックしアップロードするファイルを参照します。 アップロード - クリックしファイルをアップロードします。

スプラッシュページ編集ボックス

スプラッシュページ編集ボックスではビジネスクラウド独自の HTML エディタとなっており、スプラッシュページの作成、編集を行います。「TOU」「ヘッダ」「フッタ」「クリックスルー」「ログイン」「ログイン中」「ログイン後」「エラー」の各項目タブに同様の HTML 編集ツールが設定されています。

メンテナンス > スプラッシュページ編集 をクリックし、「TOU」「ヘッダ」「フッタ」「クリックスルー」「ログイン」「ログイン中」「ログイン後」「エラー」の各タブから編集する項目を選択、以下の画面を表示します。



図 9-8 スプラッシュページ編集ボックス画面

本画面には以下の項目があります。

項目	説明
各タブについて（ファイル管理以外）	<p>「スプラッシュページ編集ボックス」に表示される各タブの対象ページについて説明します。</p> <ul style="list-style-type: none"> 「TOU」- スプラッシュページの Terms of Usage ページを作成、編集します。 「ヘッダ」- スプラッシュページのヘッダ部分を作成、編集します。 「フッタ」- スプラッシュページのフッタ部分を作成、編集します。 「ログイン」- スプラッシュページのログインページを作成、編集します。 「クリックスルー」- スプラッシュページのクリックスルーページを作成、編集します。 「ログイン中」- スプラッシュページのログイン中のページを作成、編集します。 「ログイン後」- スプラッシュページのログイン後に表示されるページを作成、編集します。 「エラー」- スプラッシュページのエラー画面を作成、編集します。 <p>注意 クリックスルーを利用するには、ファームウェアバージョン 1.20 以上が DBA-1510P にインストールされている必要があります。</p> <p>注意 各タブの設定において「スプラッシュページ+」の「タイプ」で「Sign-On」選択時は「ログイン」、「クリックスルー」選択時は「クリックスルー」が表示されます。</p> <p>注意 「Sign-On-Third-Party」、「SNS 認証」を利用するには、ファームウェアバージョン 1.30 以上が DBA-1510P にインストールされている必要があります。</p>
	スプラッシュページ編集時に「切り取り」「コピー」「貼り付け」「プレーンテキストとして貼り付け」「ワード文章から貼り付け」「元に戻す」「やり直す」などの設定を行うツールボックスです。
	スプラッシュページ編集時に「リンク挿入 / 編集」「リンク削除」「アンカー挿入 / 編集」などの設定を行うツールボックスです。
	スプラッシュページ編集時に「イメージ」「表」「水平線」「特殊文字を挿入」などの設定を行うツールボックスです。
	スプラッシュページ編集時に「最大化」の設定を行うツールボックスです。
	スプラッシュページ編集画面の「ソース」化を行うツールボックスです。HTML タグでスプラッシュページを編集・作成します。スプラッシュページの編集の際には、ソースを直接編集する事を推奨しています。
	スプラッシュページ編集時に「イメージ」の追加を行うツールボックスです。
	スプラッシュページ編集時に「太字」「斜体」「打消し線」「書式を解除」などの設定を行うツールボックスです。

項目	説明
	スプラッシュページ編集時に「番号付きリスト」「番号なしリスト」「インデント解除」「インデント」「ブロック引用文」などの設定を行うツールボックスです。
	スプラッシュページ編集時に「スタイル」「段落の書式」「フォント」「フォントサイズ」などの設定を行うツールボックスです。
	使用している HTML エディターについての情報を表示します。 エディターのユーザガイドや使用方法についての詳細情報を参照できます。

「保存」をクリックして編集した内容を保存します。

ファイル管理

本項目ではキャプティブポータルに対応しているサーバに新しいスプラッシュページ用のファイルをアップロードすることが可能です。

メンテナンス > スプラッシュページ編集 をクリックし、「ファイル管理」タブを選択、以下の画面を表示します。

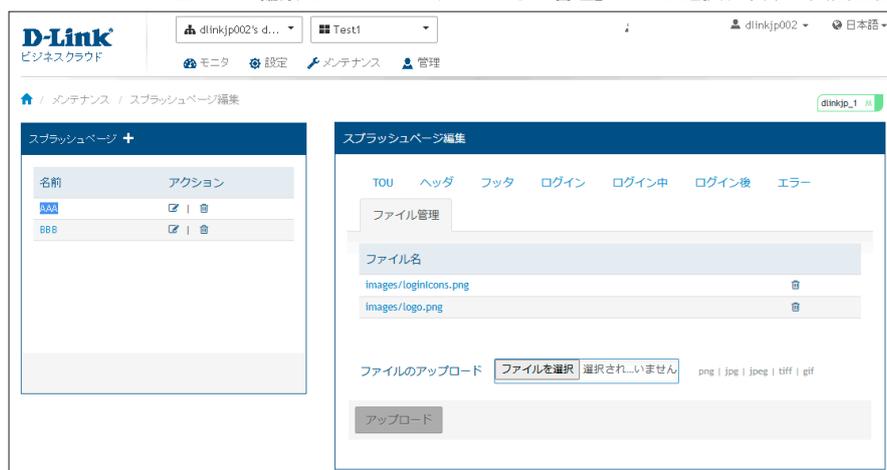


図 9-9 スプラッシュページ画面（ファイル管理）

本画面には以下の項目があります。

項目	説明
ファイル管理	スプラッシュページに使用する画像ファイルを管理します。 <ul style="list-style-type: none"> ファイル名 - スプラッシュページに使用しているファイルを表示しています。ファイル名の右端の「」をクリックすると当該ファイルを削除します。 ファイルのアップロード - スプラッシュページに使用するファイルをアップロードします。参照 / ファイルを選択」をクリックしアップロードするファイルを参照します。 アップロード - クリックしファイルをアップロードします。

注意 スプラッシュページがキャプティブポータルに対応し、デバイスグループに適用されると削除する事はできません。

ファームウェア

本項目を利用してデバイスの新しいファームウェアをアップグレードできます。「ファームウェア管理」ではファームウェアのアップグレードとともに、新しいファームウェアバージョンの選択、リストにて対応可能なファームウェアバージョンの選択などを行うことが可能です。

組織スケジュール

「組織スケジュール」ではスケジュールを設定することで、組織内の全てのデバイスグループでファームウェアのアップグレードスケジュールを設定する事ができます。

メンテナンス > ファームウェア > 組織スケジュールをクリックし、以下の画面を表示します。

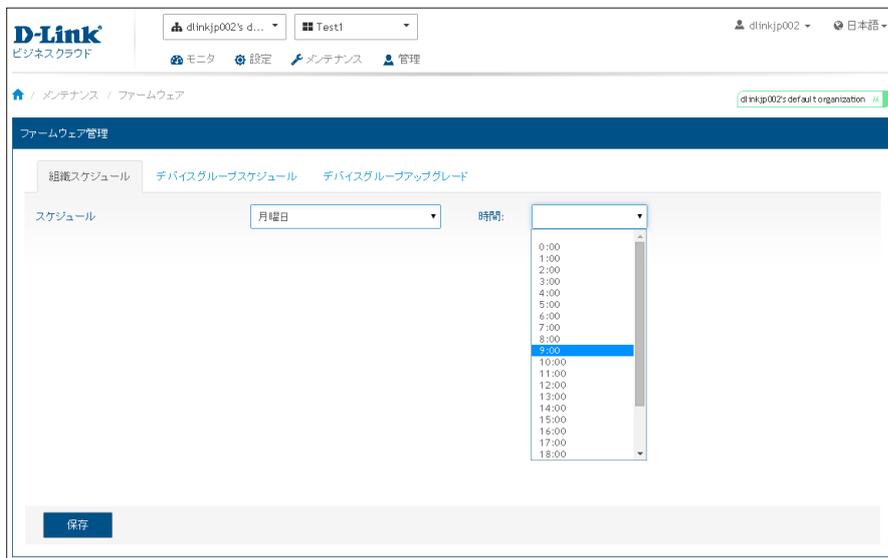


図 9-10 組織スケジュール画面（ファームウェア）

本画面には以下の項目があります。

項目	説明
スケジュール	ファームウェアアップグレードするスケジュールを指定します。 「日曜日」から「土曜日」までの各曜日を指定することができます。曜日を指定すると時間を指定する項目が表示されるのでアップグレードを開始する時間を指定します。

「保存」をクリックして編集した内容を保存します。

デバイスグループスケジュール

「デバイスグループスケジュール」ではスケジュールを設定することで、指定したデバイスグループのすべてのデバイスのファームウェアのアップグレードスケジュールを設定することができます。

メンテナンス > ファームウェア > デバイスグループスケジュールをクリックし、以下の画面を表示します。

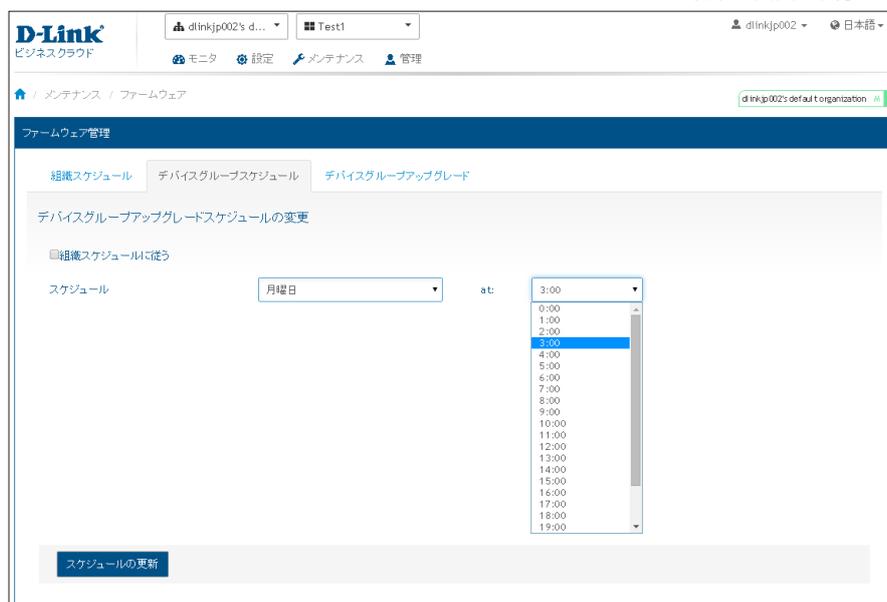


図 9-11 デバイスグループスケジュール画面（ファームウェア）

本画面には以下の項目があります。

項目	説明
組織スケジュールに従う	「組織スケジュールに従う」にチェックを入れると「組織スケジュール」でのアップグレードにのみ準じてアップグレードを行います。チェックを外すとデバイスグループ独自の設定が可能になります。
スケジュール	デバイスグループのファームウェアアップグレードするスケジュールを指定します。「日曜日」から「土曜日」までの各曜日を指定することができます。曜日を指定すると時間を指定する項目が表示されるので、アップグレードを開始する時間を指定します。

「スケジュールの更新」をクリックして設定したスケジュールを更新します。

デバイスグループアップグレード

「デバイスグループアップグレード」ではクラウド上の更新可能なファームウェアを選択、「バージョンの更新」をクリックしてバージョンの更新を行い「アップグレード開始」をクリックすることで、指定したデバイスグループのすべてのデバイスのファームウェアをすぐにアップグレードできます。

メンテナンス > ファームウェア > デバイスグループスケジュールをクリックし、以下の画面を表示します。

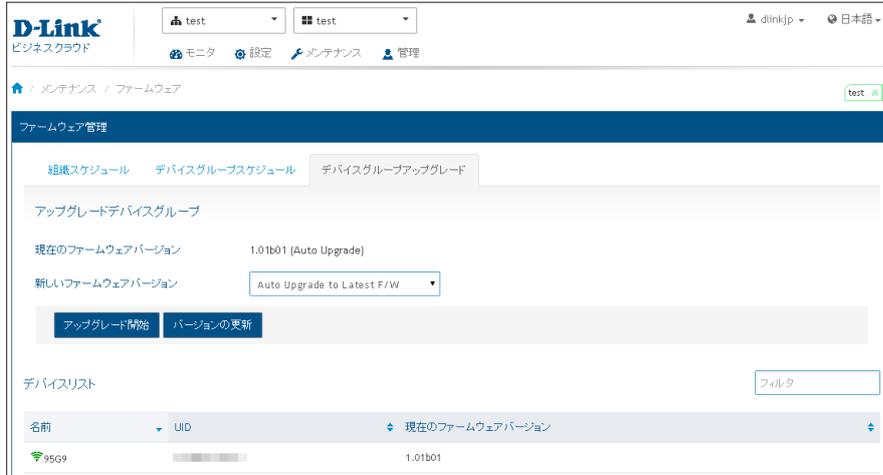


図 9-12 デバイスグループアップグレード画面（ファームウェア）

本画面には以下の項目があります。

項目	説明
アップグレードデバイスグループ	
現在のファームウェアバージョン	現在、当該デバイスグループに適用されているファームウェアバージョンを表示します。
新しいファームウェアバージョン	当該デバイスグループに適用可能なファームウェアバージョンを表示します。 最新の F/W を自動適用を選択すると最新の F/W が利用可能になった時点で、最新の F/W が当該デバイスグループに自動的に適用されます（ファームウェアアップグレードのスケジュール設定をしている場合）。
アップグレード開始	クリックするとファームウェアアップグレードが開始されます。本ボタンをクリックし、ファームウェアをアップグレードする場合には「最新の F/W を適用」ではなく、手動でファームウェアバージョンを指定する必要があります。
バージョンの更新	「新しいファームウェアバージョン」で選んだバージョンに「現在のファームウェアバージョン」を更新します。当該デバイスグループに選択した新しいファームウェアバージョンが適用されます。 バージョンの更新を行っても、デバイスへのファームウェアの更新は直ちに行われません。アップグレード開始をクリックするか、デバイスを再起動するか、またはスケジュールを設定している場合には、スケジュールが来るまで待つ必要があります。
デバイスリスト	
フィルタ	フィルタを通してデバイスを絞り込みます。
名前	デバイス名です。
UID	デバイス UID（識別番号）です。
現在のファームウェアバージョン	現在のファームウェアバージョンを表示します。

設定の複製

「設定の複製」を利用してデバイスグループで設定した設定内容 (Wi-Fi ポリシー) を他のデバイスグループ (新規 / 既存) にも適用することができます。デバイスグループの設定は他のデバイスグループの構成が同じであれば設定内容をそのままコピー (クローン) することができます。

「設定の複製」機能は無線やセキュリティを含めた設定を、選択したデバイスグループから適用するデバイスグループへそのまま同期します。複製を行うと適用されたデバイスグループの元々の設定は失われ、適用デバイスグループのデバイスはすべて新しい設定にてアップデートされます。

メンテナンス > 設定の複製 をクリックし、以下の画面を表示します。

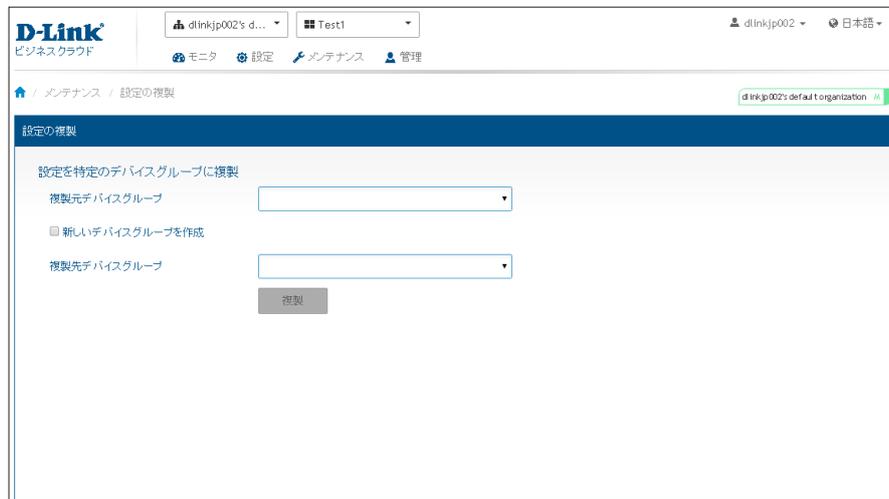


図 9-13 設定の複製画面

本画面には以下の項目があります。

項目	説明
複製元デバイスグループ	設定の複製元のデバイスグループを選択します。
新しいデバイスグループを作成	チェックを入れると新しくデバイスグループを作成し、そのデバイスグループに設定内容を複製させます。
既存のデバイスグループへの設定の複製	
複製先デバイスグループ	複製先のデバイスグループを選択し「複製」をクリックして、設定を複製します。
新しいデバイスグループへの設定の複製	
新しいデバイスグループ名	新しいデバイスグループ名を指定し「新しいデバイスグループを作成」をクリックして、設定を複製します。

項目を設定した後「複製」をクリックして複製を実行します。

第 10 章 「管理」メニュー (D-Link Business Cloud)

本章では「D-Link Business Cloud」の「管理」メニューの説明を行います。

以下は本章「管理」メニューのサブメニューの説明です。必要に応じて、設定 / 変更 / 修正を行ってください。

サブメニュー	説明
ダッシュボード	組織の重要な情報などをサマリ形式で確認することができ、更にデバイスグループの作成やデバイスの登録など管理上のタスクなどを実行することも可能です。(D-Link Business Cloud の初期画面になります。)
概要	デバイス数、デバイスのファームウェアバージョン、グループのパラメータを含むデバイスグループの主要な情報を表示します。
インベントリ	登録済のデバイスの一覧とその情報を表示します。デバイスの事前登録、読み込み、削除なども可能です。
一括インポート	100 組織までの設定情報を、エクセルファイル (.xls または .xlsx ファイル形式) で一括インポートすることができます。
タグ	様々な方法や形式でデバイスグループにタグを付与することができます。
Admin 管理	クラウドの管理者とその権限内容について管理します。 デバイスグループやタグにも関連した権限を付与することが可能です。
ライセンス	組織に紐づいているライセンス状態の確認、ライセンス履歴、ライセンス追加などを行います。
システムログ	ビジネスクラウドのデバイスグループ内で発生したイベント (システムログ) の詳細について表示、CSV ファイル形式でのダウンロードを行います。
組織設定	組織についての管理項目です。組織の状態を確認、組織の削除なども行います。

「管理」メニューからサブメニューを選択します。



図 10-1 「管理」メニュー

ダッシュボード

ダッシュボードでは組織の重要な情報などをサマリで確認でき、デバイスグループの作成やデバイスの登録など管理上のタスクなどを実行することも可能です。組織に所属するデバイスをライセンス項目などと一緒にグループ単位やタグの有無などで分類して表示することも可能です。

左側の項目ではライセンスの概要やデバイスの警告などの情報が確認でき、右側の項目ではデバイスの状態やタグなどで表示を絞り込むことができます。またデバイスをデバイスグループ間のドラッグ＆ドロップで移動させることができ、定義済みのフィルタやグループ内の事前登録済みのデバイスへのリンクなども表示されています。ビジネスクラウドログイン時の初期画面はこの「ダッシュボード」になります。

管理 > ダッシュボードをクリックし、以下の画面を表示します。

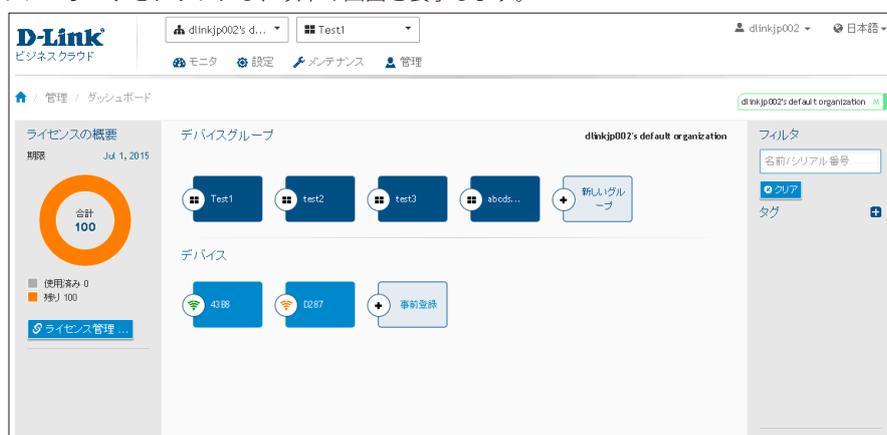


図 10-2 ダッシュボード画面

本画面には以下の項目があります。

項目	説明
ライセンスの概要	現在の組織のライセンスに関するステータスです。使用したポイントの数、ライセンス使用期限などが表示されます。
ライセンス管理	クリックするとライセンス管理画面へ移動します。 ライセンス管理画面へは「管理 > ライセンス」からも移動可能です。「ライセンス管理」に関する設定情報は「ライセンス」を参照ください。「ライセンスは1組織に1ライセンス」となっており、「組織」単位で表示されます。
デバイスグループ	組織内のデバイスグループ一覧です。「新しいグループ」をクリックすると「デバイスグループ名」と「モデル名」(機器モデル。通常は DBA-1510P) を入力するダイアログが表示されるので、入力し「保存」をクリックすると新しいデバイスグループが作成されます。
デバイス	組織内のデバイス (クラウド AP/DBA-1510P) の一覧です。「事前登録」をクリックすると「デバイス名」「デバイスUID」「デバイスグループを選択」「デバイスグループ名」を指定するダイアログが表示されるので、各項目を指定をして「事前登録」をクリックするとデバイスが登録されます。「デバイスグループを選択」で「新しいグループ」を選択し「デバイスグループ名」を入力するところでも新しいデバイスグループを作成することができます。 デバイスアイコンをデバイスグループ上にドラッグアンドドロップする事で、デバイスの所属するデバイスグループを変更する事ができます。
フィルタ	表示されている既存の「デバイスグループ」「デバイス」を検索条件 (グループ名/デバイス名) を設定して表示を絞り込みます。「クリア」をクリックすると検索条件がクリアされます。
タグ	タグを設定します。「+」をクリックして表示されたダイアログにタグ名を入力、保存をクリックすると新しいタグを使えます。

新しいグループの作成

デバイスグループは同じ設定を共有する組織内のデバイスの集合体です。管理者によって複数のデバイスの状態の確認や設定の適用などをまとめて行うことができます。デバイスグループの「新しいグループ」をクリックすることで新しいグループを作成することが可能です。

管理 > ダッシュボード > 新しいグループをクリックし、以下の画面を表示します。

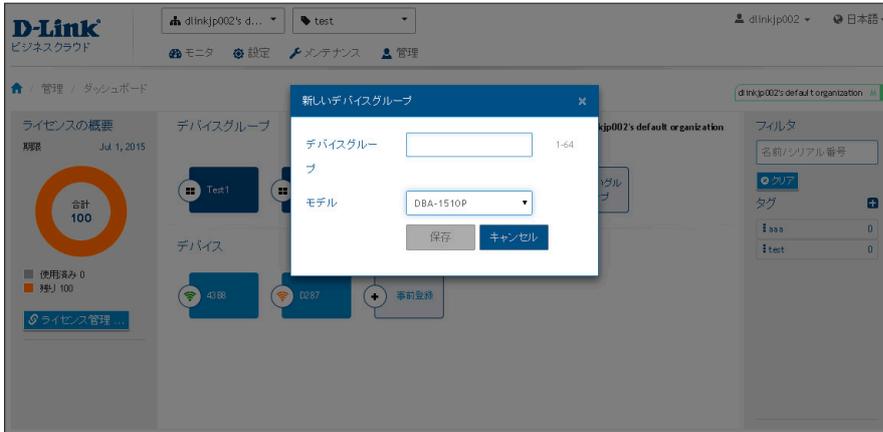


図 10-3 ダッシュボード画面（新しいデバイスグループ）

本画面には以下の項目があります。

項目	説明
デバイスグループ	「デバイスグループ」を入力します。
モデル	「モデル名」（機器モデル。通常は DBA-1510P）を入力します。

「保存」をクリックすると新しいデバイスグループが作成されます。

デバイスの事前登録

管理者はビジネスクラウドで管理するデバイスを登録する必要があります。デバイスを事前登録することでデバイスはクラウドとつながり、オンラインになるとデバイスは自動的にクラウドへと接続します。

管理 > ダッシュボード > 事前登録をクリックし、以下の画面を表示します。

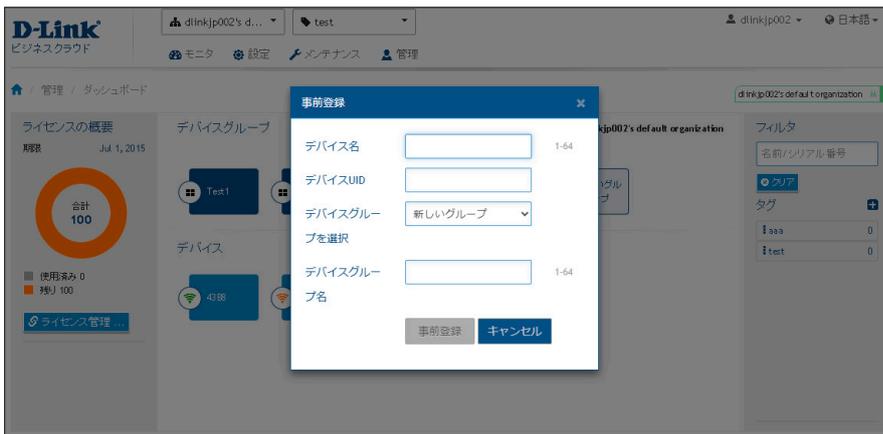


図 10-4 ダッシュボード画面（事前登録）

本画面には以下の項目があります。

項目	説明
デバイス名	事前登録する「デバイス名」を入力します
デバイス UID	デバイスの識別番号（デバイス UID）を入力します。
デバイスグループを選択	デバイスが所属する既存 / 新規「デバイスグループ」を選択します。 「新しいグループ」を選択すると新しいデバイスグループが作成され、「デバイスグループ名」でグループ名を指定します。
デバイスグループ名	新しいデバイスグループのグループ名を指定します。

「事前登録」をクリックすると新しいデバイスがクラウドに登録されます。

概要（管理）

「概要」ではデバイス数、デバイスのファームウェアバージョン、そしてグループのパラメータを含む主要なデバイスグループ情報を表示します。これらの情報は「ダッシュボード」や「インベントリ」でも別のフォーマットで表示されますが、「概要」では各グループの設定の比較などを含めて表示されます。例えば、大量のアクティブなデバイスを抱えるグループとほとんどのデバイスがオフラインのグループを比較して、ネットワークの状況などを把握することが可能です。

管理 > 概要をクリックし、以下の画面を表示します。

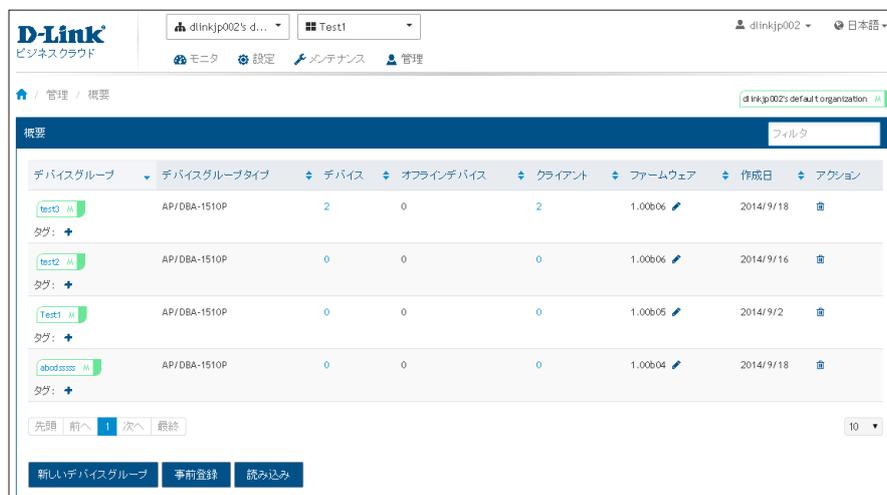


図 10-5 概要（管理）画面

本画面には以下の項目があります。

項目	説明
フィルタ	表示されている既存の「デバイスグループ」「デバイス」を検索条件（グループ名/デバイス名）を設定して表示を絞り込みます。
デバイスグループ	デバイスグループを表示しています。グループ名をクリックすると、当該グループの「 モニタ > 概要 」ページへ移動します。グループ名下の「 タグ：+ 」をクリックしてグループにタグを指定できます。
デバイスグループタイプ	デバイスグループの種類を表示しています。
デバイス	所属しているデバイス数を表示しています。
オフラインデバイス	オフラインになっているデバイス数を表示しています。
クライアント	接続しているクライアント数を表示しています。
ファームウェア	現在のファームウェアバージョンを表示しています。 ファームウェアバージョン右横の をクリックすると別のファームウェアをグループに適用することができます。リストからファームウェアバージョンを選択し で適用、 でキャンセルします。
作成日	グループの作成日を表示しています。
アクション	当該のグループに対する動作を実行します。（ごみ箱アイコン）をクリックするとグループを削除します。
新しいデバイスグループ	新しいデバイスグループを作成します。クリックすると「デバイスグループ」の項目が表示され、新しいデバイスグループ名を入力します。その後「保存」をクリックしてデバイスグループの作成は完了です。
事前登録	デバイスを事前登録します。クリックすると「デバイス名」「デバイス UID」「デバイスグループを選択」「デバイスグループ名」が表示され、指定をして「保存」をクリックしてデバイスの事前登録は完了です。
読み込み	CSV ファイルのアップロードによるデバイスの読み込みを行います。CSV ファイルに保存されているデバイスをファイルをアップロードすることでクラウドに読み込むことが可能です。CSV ファイルの対応文字コードは、UTF-8 となります。 1. 「ファイルを選択」をクリックして CSV ファイルを指定し、「設定を検証」ボタンをクリックします。 2. 設定の検証が問題無く終了すると、「インポート実施」ボタンが有効になります。このボタンをクリックし、設定のインポートを実施します。

インベントリ

「インベントリ」では登録済のデバイスの一覧を表示します。

各デバイスの「名前」「デバイス UID」「所属デバイスグループ」「IP/MAC アドレス」「ハードウェア / ファームウェアバージョン」などが表示され、デバイスの事前登録、読み込み、または削除などが可能です。

管理 > インベントリをクリックし、以下の画面を表示します。

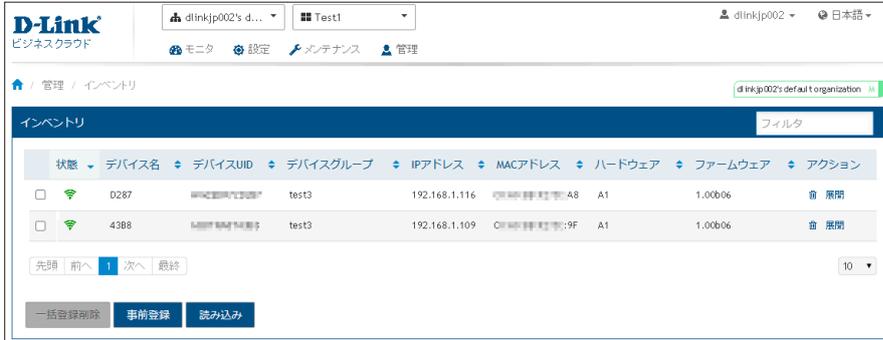


図 10-6 インベントリ 画面

本画面には以下の項目があります。

項目	説明
フィルタ	表示されている既存の「デバイス名」「デバイス UID」「デバイスグループ」「IP アドレス」「MAC アドレス」を検索条件として設定してリスト表示を絞り込みます。
状態	デバイスの電波状態を表示しています。
デバイス名	事前登録する「デバイス名」を表示しています。
デバイス UID	デバイスの識別番号（デバイス UID）を表示しています。
デバイスグループ	所属しているデバイスグループ名を表示しています。
IP アドレス	現在の IP アドレス表示しています。
MAC アドレス	現在の MAC アドレス表示しています。
ハードウェアバージョン	現在のハードウェアバージョンを表示しています。
ファームウェアバージョン	現在のファームウェアバージョンを表示しています。
アクション	<p> (ごみ箱アイコン) をクリックすると当該デバイスの登録情報がクラウドから削除され、デバイスが未登録状態となります。「展開」をクリックするとデバイスの「登録状況」「モデル」「ベンダ」について表示します。</p> <p>注意 デバイス登録情報をクラウドから削除する場合、デバイスの初期化が必要となります。デバイス登録情報をクラウドから削除する時、デバイスがオンライン状態であれば、初期化処理は自動的に実行されますが、デバイスがオフライン状態の場合には、初期化処理は自動的に実行されませんので、手動での初期化処理が必要となります。</p>
一括登録削除	チェックボックスにチェックを入れ、デバイスの一括削除を行います。
事前登録	デバイスを事前登録します。クリックすると「デバイス名」「デバイス UID」「デバイスグループを選択」「デバイスグループ名」が表示され、指定をして「保存」をクリックしてデバイスの事前登録は完了です。
読み込み	<p>デバイス UID を CSV ファイルでインポートすることができます。自身が管理する組織やデバイスグループを指定した形でデバイス UID を登録する事ができるため、組織やデバイスグループ跨ぎの UID 登録を、一回のインポートで行う事ができます。CSV ファイルは、A 列：デバイス名, B 列：デバイスグループ, C 列：UID, D 列：組織名を入力し、CSV ファイル形式で保存します。</p> <p>1. 「設定を検証」: デバイス UID を保存した CSV ファイルを指定し、「設定を検証」 ボタンをクリックすることで、CSV ファイルに設定された UID の検証が開始されます。</p> <p>2. 「インポート実施」: 設定の検証が問題無く終了すると、「インポート実施」 ボタンが有効になりますので、このボタンをクリックすることで、デバイス UID がインポートされます。</p> <p>サンプルの CSV ファイルが、下記サイトからダウンロード可能です。 https://www.dlink-jp.com/product/dba-1510p#product_firmware</p>

一括インポート

「一括インポート」では、100 組織までの設定情報を、エクセルファイル (.xls または .xlsx ファイル形式) で一括インポートすることができます。複数の組織を一括インポートすることができるため、複数組織を設定する時間を大幅に短縮することができます。

管理 > 一括インポートをクリックし、以下の画面を表示します。



図 10-7 一括インポート画面

本画面には以下の項目があります。

項目	説明
設定を検証	設定を保存したエクセルファイル (.xls または .xlsx ファイル形式) を指定し、「設定を検証」ボタンをクリックすることで、エクセルファイルに設定された項目の検証が開始されます。(この時点では、まだ設定は適用されていません。)
インポート実施	設定の検証が問題無く終了すると、「インポート実施」ボタンが有効になりますので、このボタンをクリックすることで、設定が各組織に適用されます。 一括インポート用エクセルファイルの各種設定項目は、下記の「一括インポート用エクセルファイルの設定」を参照ください。 また一括インポート用エクセルファイルのサンプルファイルが、下記サイトからダウンロード可能です。 https://www.dlink-jp.com/product/dba-1510p#product_firmware

一括インポート用エクセルファイルの設定

一括インポート用エクセルファイルの各種設定項目について説明します。エクセルファイルに各設定項目を記入して使用します。

1	Mode	Organization	DeviceGroup	SSID1	GuestAccess1	2.4G1	5G1	BandSteering1	BroadcastSSID1	StationsIsolation1	PSK1
2	N	D-Link Japan's Organization	MASSIP06	SSIDM1011	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	9876
3	N	D-Link Europe's Organization	MASSIP07	SSIDM1011	FALSE	TRUE	TRUE	FALSE	TRUE	FALSE	9876

図 10-8 一括インポート用エクセルファイル例

一括インポート用エクセルファイルの各種設定項目

設定項目 (列)	設定パラメータ	説明
Mode	N/C	組織を新規に生成する場合には" N " を選択、既存組織の設定変更を行う場合には" C " を選択 <ul style="list-style-type: none"> 同一エクセルファイル上で、同一組織に対する" N " と" C " を混在させることはできません。 同一エクセルファイル上で、同一組織に対する" N " を複数設定することはできません。 同一エクセルファイル上で、同一デバイスグループに対する設定が重複している場合、一番下の列に記載されている設定に上書きされます。 エクセルファイルへのパラメータ記入で、組織名とデバイスグループ名の記入は必須となります。SSID の設定を行う場合、全ての SSID 毎の設定パラメータの記入は必須となります。また" FWVersion " を除くデバイスグループ毎に設定する項目の記入は必須となります。
Organization	組織名 (1~64 文字)	1 ファイル 100 組織まで
DeviceGroup	デバイスグループ名 (1~64 文字)	
License1~3	ライセンス ID	設定可能数 3
DeviceName1~8	デバイス名 (AP 名) (1~64 文字)	設定可能数 8
UID1~8	デバイス UID	設定可能数 8
SSID1~8	SSID 名 (1~32 文字)	設定可能数 8
GuestAccess1~8	TRUE/FALSE	ゲストアクセス有効・無効設定 (SSID 毎に設定)
2.4G1~8	TRUE/FALSE	2.4G 有効・無効設定 (SSID 毎に設定)
5G1~8	TRUE/FALSE	5G 有効・無効設定 (SSID 毎に設定)
BandSteering1~8	TRUE/FALSE	バンドステアリング有効・無効設定 (SSID 毎に設定)
BroadcastSSID1~8	TRUE/FALSE	SSID ブロードキャスト有効・無効設定 (SSID 毎に設定)

「管理」メニュー

設定項目 (列)	設定パラメータ	説明
StationIsolation1~8	TRUE/FALSE	SSID 内パーティション有効・無効設定 (SSID 毎に設定)
PSK1~8	SSID パスワード (8~63 文字)	SSID パスワード設定 (SSID 毎に設定)
Bonjour1~8	TRUE/FALSE	Bonjour パケットフォワーディング有効・無効設定 (SSID 毎に設定)
IGMP1~8	TRUE/FALSE	IGMP スヌーピング有効・無効設定 (SSID 毎に設定)
2.4GMulticastRate	1,2,5,5,11,6,9,12,18,24, 36,48,54	2.4GHz 帯のマルチキャストレートを設定 (デバイスグループ毎に設定)
2.4GEnableUAPSD	TRUE/FALSE	2.4GHz 帯 UAPSD 有効・無効設定 (デバイスグループ毎に設定)
5GMulticastRate	6,9,12,18,24,36,48,54	5GHz 帯のマルチキャストレートを設定 (デバイスグループ毎に設定)
5GEnableUAPSD	TRUE/FALSE	5GHz 帯 UAPSD 有効・無効設定 (デバイスグループ毎に設定)
FWOrgScheduleDay	MONDAY,TUESDAY, WEDNESDAY,THURSDAY, FRIDAY,SATURDAY, SUNDAY	ファームウェアアップデートスケジュールの曜日設定 (デバイスグループ毎に設定)
FWOrgScheduleTime	0:00~23:59	ファームウェアアップデート時間設定 (デバイスグループ毎に設定)
FWVersion	当該組織で利用可能なファームウェアバージョンまたは AUTO を指定	ファームウェアバージョン設定 (デバイスグループ毎に設定) <ul style="list-style-type: none"> ・ 組織新規作成の場合は、最新ファームウェアバージョンが自動的に割り当てられます ・ 「AUTO」を指定することで、最新ファームウェアが自動的に割り当てられます。

タグ

「タグ」では様々な方法や形式でデバイスグループにタグを付与することができます。

タグはデバイスのフィルタリングなどで行われるデバイスの識別方法です。親タグ/子タグといったように階層構造にタグをつけることも可能です。

管理 > タグ をクリックし、以下の画面を表示します。

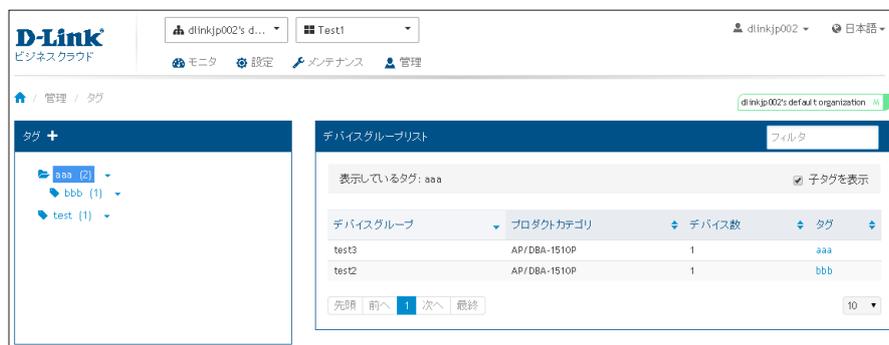


図 10-9 タグ画面

本画面には以下の項目があります。

項目	説明
タグ+	
タグ+	タグの一覧について表示します。タイトル右横の「+」をクリックすると、タグを追加することが可能です。表示される「タグ名」「親タグ」を指定し保存します。 タグ名左横がフォルダ型アイコンは「親タグ」を意味しており、クリックすると配下の「子タグ」がツリー上に表示されます。「タグ名」の右横の「▼」をクリックすると「名前の変更」「親タグに追加」「親タグから削除」「削除」の項目が表示されます。 <ul style="list-style-type: none"> 名前の変更 - タグの名前を変更します。 親タグに追加 - 親タグに追加し、当該のタグを子タグにすることができます。 親タグから削除 - 子タグの場合、所属している親タグから離脱させます。 削除 - タグを削除します。
デバイスグループリスト	
フィルタ	表示されている既存の「デバイスグループ」「プロダクトカテゴリ」「デバイス数」「タグ」を検索条件として設定してリスト表示を絞り込みます。
表示しているタグ	左の「タグ+」で選択したタグが表示されます。
子タグを表示	チェックを入れると選択したタグに子タグがある場合、子タグも同様に表示されます。
デバイスグループ	所属しているデバイスグループ名を表示しています。
プロダクトカテゴリ	プロダクトの種類を表示しています。
デバイス数	グループ内のデバイス数を表示しています。
タグ	付けられたタグの種類を表示しています。クリックすると当該のタグがリストに表示されます。「子タグを表示」にチェックがあると当該タグ配下のタグも表示されます。

Admin 管理

「Admin 管理」ではサーバ管理者とその権限について管理します。

管理者に対する権限はいくつかの種類に分かれており、この権限に従い組織内のユーザを何種類かに分離することが可能です。組織、タグ、そしてデバイスグループに適用する権限のレベルは5つに分かれています。この分割の目的は複数のユーザによって組織の管理やデバイスグループの設定などを行うようにするためです。例えば、デバイスグループにおいてモニタや編集をサポートされている人でも、組織内の他の情報にはアクセスする事ができない、といった形になります。

注意 1 組織あたりの最大管理者数は 100 です。

権限のレベルは以下の5つ、「閲覧者」「モニタ閲覧者」「編集者」「組織内管理者」「管理者」になります。

- ・ 管理者：最高レベルの権限です。コンフィグ設定、ライセンス登録など組織内で全ての設定・操作を行う事ができます。
- ・ 組織内管理者：特定組織内において、管理者に準ずる権限を持つ管理者です。組織への管理者の追加、ライセンスの削除ができません。
- ・ 編集者：メインメニューの " 設定 " の編集権限と閲覧権限を持つ管理者です。
- ・ 閲覧者：閲覧権限のみを持つ管理者です。
- ・ モニタ閲覧者：一部のモニタメニューのみ閲覧できる権限を持つ管理者です。

ユーザが何を閲覧できるのかはユーザが持つ既存の権限と許可の合成になります。例えば、デバイスグループで管理者に設定されたユーザはそのデバイスグループ内においてのみ管理することが可能ですが、組織においてはその他の権限はありません。ユーザが権限を持ち合わせていない場合、対応する動作項目は表示されません。

管理 > Admin 管理 をクリックし、以下の画面を表示します。



図 10-10 Admin 管理画面

本画面には以下の項目があります。

項目	説明
Admin 管理	
フィルタ	表示されている「名前」「ユーザ名」「メールアドレス」を検索条件として設定してリスト表示を絞り込みます。
名前	管理者の名前を表示しています。「権限」の横には当該管理者が権限を有している組織と権限の種類が表示されます。
ユーザ名	管理者のユーザ名を表示しています。
メールアドレス	管理者のメールアドレスを表示しています。
サブユーザ	サブユーザとしてのステータスを表示します。
最終接続日時	クラウド管理画面にアクセスした最終接続日時が表示されます。
アクション	クリックすると「管理者の編集」「管理者の削除」を行うことができます。 「管理者の編集」については「管理者の追加 / 編集」を参照ください。
管理者の追加	管理者を追加します。「管理者の追加 / 編集」を参照ください。
管理者を招待	D-Link ビジネスクラウドで既にアカウントを保持しているユーザを、自組織の「Admin 管理者」として招待する事ができます。招待する「Admin 管理者の権限」、「アラート通知」などを選択することができます。詳しくは「管理者の追加 / 編集」を参照ください。 招待されたアカウントには、登録 Email アドレスに招待メールが配信されますので、メールに記載されている承認リンクをクリックする事で、招待された組織の「Admin 管理者」として、組織を管理する事ができます。 注意 「Admin 管理者」を招待できるのは管理者権限を持ったアカウントのみです。

項目	説明
SAML ロール管理	
名前	ロール名を表示します。
ロール ID	ロール ID を表示します。
適用範囲	適用範囲を表示します。
サブユーザ	サブユーザとしてのステータスを表示します。
アクション	クリックすると「ロール編集」「ロール削除」を行うことができます。 「ロール編集」については「SAML ロールの追加 / 編集」を参照ください。
ロール追加	SAML ロールを追加します。「SAML ロールの追加 / 編集」を参照してください。

管理者の追加 / 編集

「管理者の追加」「管理者の編集」について説明します。

ユーザ権限はより細かいレベルで設定することが可能で、例えば全てのデバイスに対する全面的なアクセス権を付与する代わりに、全組織内のデバイスの表示と一部タグと一部グループへの管理権限でのアクセスを許可するなどの設定を行うことができます。ログイン中ユーザ（管理者）の属性を変更する場合には、画面上部のユーザ名を右クリックし、「ユーザプロフィール」からを編集します。

管理 > Admin 管理 をクリックし、「管理者の追加」または「アクション > 管理者の編集」をクリックし以下の画面を表示します。

The screenshot shows the 'Admin Management' interface. At the top, there's a search bar and a list of user details for '鈴木 玲理' (Rinri Suzuki). Below that, there's a navigation bar with '先頭', '前へ', '1', '次へ', '最終' and a dropdown for '10'. The main section is titled 'この組織に管理者を追加' (Add administrator to this organization). It contains several input fields with validation rules:

- 名前 (Name): 1 - 64 characters
- ユーザ名 (Username): 6 - 32 characters
- パスワード (Password): 10-16 characters, must include a-z, A-Z, and 0-9.
- パスワードの確認 (Password Confirmation): Same rules as Password.
- メールアドレス (Email Address): 1 - 254 characters, format: username@organization.com
- 会社名 (Company Name): Company Name
- サブユーザ (Subuser): checkbox
- 組織権限 (Role): dropdown menu with '閲覧者' (Viewer) selected.
- アラート通知 (Alerts): checkboxes for 'デバイスオンライン', 'デバイスオフライン', '新しい設定の適用', 'IPアドレスの変更', 'ファームウェアのアップグレード', 'デバイスの登録', 'デバイスの登録取り消し', 'ライセンスの不足', 'その他'.
- デバイスグループ/タグ権限 (Device Group/Tag Permissions): A table with 'ターゲット' (Target) and 'アクセス' (Access) columns.

 At the bottom, there are buttons for '+デバイスグループを追加' and '+タグを追加', and '保存' (Save) and 'キャンセル' (Cancel) buttons.

図 10-11 管理者の追加 / 編集 画面

本画面には以下の項目があります。

項目	説明
名前	管理者の名前を指定、編集します。
ユーザ名	ユーザの名前を指定、編集します。
パスワードを変更する (管理者を編集時のみ)	「管理者を編集」時のみ表示されます。 パスワードを変更する場合、チェックを入れます。
パスワード	追加アカウントをアクティベーションするためのパスワードを指定します。 追加アカウントのユーザは、アクティベーション時にパスワードを入力した後、このパスワードを変更する必要があります。
パスワードの確認	確認のため、上記パスワードを指定します。
メールアドレス	管理者のメールアドレスを指定、編集します。
会社名	所属する会社名を入力します。
サブユーザ	サブユーザを有効にしたアカウントは、新規組織を作成することができません。 新規組織の作成を制限したアカウントを作成したい場合、サブユーザを有効にしてください。

項目	説明
組織権限	<p>組織権限について指定します。次の6つから選択します。</p> <ul style="list-style-type: none"> 管理者：最高レベルの権限です。コンフィグ設定、ライセンス登録など組織内で全ての設定・操作を行う事ができます。 組織内管理者：特定組織内において、管理者に準ずる権限を持つ管理者です。組織への管理者の追加、ライセンスの削除ができません。 編集者：メインメニューの「設定」の編集権限と閲覧権限を持つ管理者です。 閲覧者：閲覧権限のみを持つ管理者です。 モニタ閲覧者：一部のモニタメニューのみ閲覧できる権限を持つ管理者です。 なし：組織に対する権限はありません。
アラート通知	<p>警告の通知について指定します。</p> <ul style="list-style-type: none"> デバイスオンライン - デバイスがオンライン時に通知されます。 デバイスオフライン - デバイスがオフライン時に通知されます。 新しい設定の適用 - 新しい設定適用時に通知されます。 IP アドレスの変更 - IP アドレス変更時に通知されます。 ファームウェアのアップグレード - ファームウェアアップグレード時に通知されます。 デバイスの登録 - デバイス登録時に通知されます。 デバイスの登録取り消し - デバイスの登録が外れた時に通知されます。 ライセンスの不足 - ライセンスの不足時に通知されます。
デバイスグループ/タグ権限	<p>「デバイスグループを追加」「タグを追加」をクリックし、各デバイスグループ、各タブへの権限をそれぞれ指定することができます。詳しくは「デバイスグループ/タグ権限」を参照ください。</p>

注意 ログイン中ユーザ（管理者）の「同時ログイン設定」「アイドルタイムアウト」の条件などの詳細設定は「[ログインユーザの詳細設定](#)」を参照してください。

デバイスグループ/タグ権限

「デバイスグループ/タグ権限」では当該の管理者に対して各デバイスグループや各タブへの権限の設定を行うことが可能です。

「[管理者の追加・管理者の編集](#)」画面で「[デバイスグループを追加](#)」「[タグを追加](#)」をクリックし以下の画面を表示します。

図 10-12 管理者の追加 / 編集 画面

本画面には以下の項目があります。

項目	説明
ターゲット	当該の管理者に設定済みの「デバイスグループ」「タグ」を表示します。
アクセス	当該の管理者に設定されている「デバイスグループ/タグ」の権限内容です。本項目で権限内容の編集を行うことも可能です。「組織権限」同様「管理者」「編集者」「閲覧者」「なし」から選択します。
削除	(ごみ箱アイコン) をクリックすると当該の設定権限を削除します。
デバイスグループを追加	クリックすると「デバイスグループへの権限追加」が表示されます。
タグを追加	クリックすると「タグへの権限追加」が表示されます。
デバイスグループへの権限追加	
デバイスグループ	当該の管理者に権限を付与する対象のデバイスグループを指定します。
権限	当該の管理者に付与するデバイスグループへの権限内容を指定します。
タグへの権限追加	
タグ	当該の管理者に権限を付与する対象のタグを指定します。
権限	当該の管理者に付与するタグへの権限内容を指定します。

「保存」をクリックして設定内容を保存します。

注意 管理者作成後、確認メールが自動送信されます。必ず確認メールによるアクティベーションが必要となります。

注意 ブラウザ（Google Chrome）の設定により「サイトのパスワード保存」に関するダイアログが表示される場合がありますが、「使用しない」（保存しない）をクリックしてください。



図 10-13 パスワード保存の確認メッセージ

SAML ロールの追加 / 編集

管理 > Admin 管理 をクリックし、「SAML ロール」セクションで「**ロール追加**」または「**アクション > ロール編集**」をクリックし以下の画面を表示します。

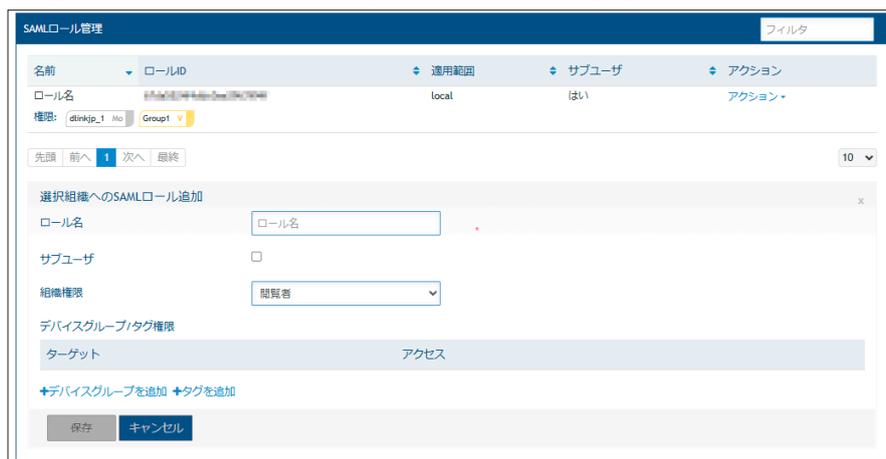


図 10-14 SAML ロールの追加 / 編集 画面

本画面には以下の項目があります。

項目	説明
ロール名	SAML ロールの名前を指定、編集します。
サブユーザ	サブユーザを有効にするかどうかを指定します。
組織権限	組織権限を「なし」「モニタ閲覧者」「閲覧者」「編集者」「組織内管理者」「管理者」から指定します。
デバイスグループ / タグ権限	「デバイスグループを追加」「タグを追加」をクリックし、各デバイスグループ、各タブへの権限をそれぞれ指定することができます。詳しくは「 デバイスグループ / タグ権限 」を参照ください。

ライセンス

「ライセンス」ではライセンス状態の確認、ライセンス履歴、ライセンス追加などを行います。

ライセンスが有効になって初めて組織は本製品をご利用頂くことが可能です。ライセンスの情報は常に本項目に更新され、それぞれのライセンスの処理状況などを確認することが可能です。

ライセンスはポイント型のシステムになっており、組織にライセンスが追加されるとポイントが加算され、組織内のデバイスの使用率やライセンス合意率の使用率などに基つきポイントは減少していきます。デバイス登録によりポイントは減少しますが、デバイスが非登録になるとポイントの消費は停止します。システムに十分なポイントが残されていない場合、組織には新しいデバイスの登録ができなくなります。ライセンスが枯渇状態になった場合は有効なポイントはなくなり、ビジネスクラウドによる組織内のデバイスの管理は不可能になります。

ライセンス状態

管理 > ライセンス > ライセンス状態をクリックし、以下の画面を表示します。

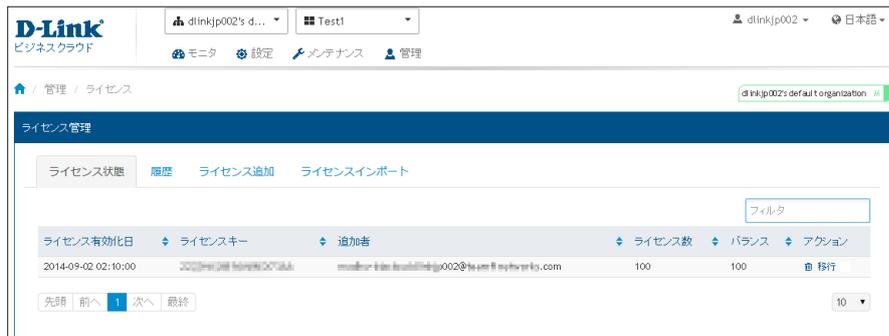


図 10-15 ライセンス状態 画面

本画面には以下の項目があります。

項目	説明
フィルタ	表示されている「フィルタ」欄に検索条件を設定してリスト表示を絞り込みます。
ライセンス有効化日	ライセンスを有効にした日付です。
ライセンスキー	ライセンスキーを表示しています。
追加者	ライセンスを追加した管理者を表示しています。
ライセンス数	ライセンス登録時のポイント数を表示しています。
バランス	該当ライセンスの未使用分のポイント数を表示しています。
アクション	<p>当該のライセンスに対する動作を実行します。🗑️ (ごみ箱アイコン) をクリックするとライセンスを削除します。</p> <p>「移行」をクリックするとライセンスの移動を実行します。</p> <p>警告 ライセンスを削除すると復元する事はできません。削除後にライセンスが必要になった場合は再購入頂くことになりますので、ライセンスの削除については十分に注意して実行してください。</p> <p>注意 当月末にポイント消費予定のあるライセンスキーは、削除することができません。</p> <p>「移行」をクリックするとライセンスキーの他組織への移動を行います。</p> <ul style="list-style-type: none"> ライセンスキー --- 別組織へ移行するライセンスキーが表示されています。 ライセンス移行元の組織 --- 移行元の組織が表示されています。 ライセンス移行先の組織 --- 移行先の組織をプルダウンから選択してください。 <p>「移行」をクリックするとライセンスの移動を実行します。</p> <p>注意 当月末にポイント消費予定のあるライセンスキーは、移行することができません。</p>

ライセンスインポート

CSV ファイルでのライセンスのインポートを行います。自身の管理する複数の組織のライセンス登録を一括で実行できるため、管理稼働を削減することができます。

管理 > ライセンス > ライセンスインポートをクリックし、以下の画面を表示します。



図 10-18 ライセンスインポート 画面

本画面には以下の項目があります。

項目	説明
設定を検証	ライセンスキーを保存した CSV ファイルを指定し、「設定を検証」ボタンをクリックすることで、CSV ファイルに設定されたライセンスキーの検証が開始されます。 CSV ファイルは、A 列: ライセンスキー B 列: 組織名を入力し、CSV ファイル形式で保存します。 ライセンスインポート用エクセルファイルの各種設定項目は、下記の「 ライセンスインポート用エクセルファイルの設定 」を参照ください。
インポート実施	設定の検証が問題無く終了すると、「インポート実施」ボタンが有効になりますので、このボタンをクリックすることで、ライセンスキーがインポートされます。 サンプルの CSV ファイルが、下記サイトからダウンロード可能です。 https://www.dlink-jp.com/product/dba-1510p#product_firmware

ライセンスインポート用エクセルファイルの設定

ライセンスインポート用エクセルファイルの各種設定項目について説明します。

	A	B
1	DJPDJPTTESTESTPC0089	dlinkjp's default organization
2	DJPDJPTTESTESTPC0088	dlinkin_1
3		

ライセンス 組織名

図 10-19 ライセンスインポート用エクセルファイル例

一括インポート用エクセルファイルの各種設定項目

設定項目 (列)	説明
ライセンス	ライセンスを記入します。
組織名	組織名を記入します。

システムログ

「システムログ」ではビジネスクラウドのシステムログについて表示します。

システム変更ログはデバイスグループ内で発生したイベントの詳細について表示し、特定のデバイスグループの管理者情報や、ログイン/ログアウト情報などの詳細について表示します。

管理 > システムログ をクリックし、以下の画面を表示します。

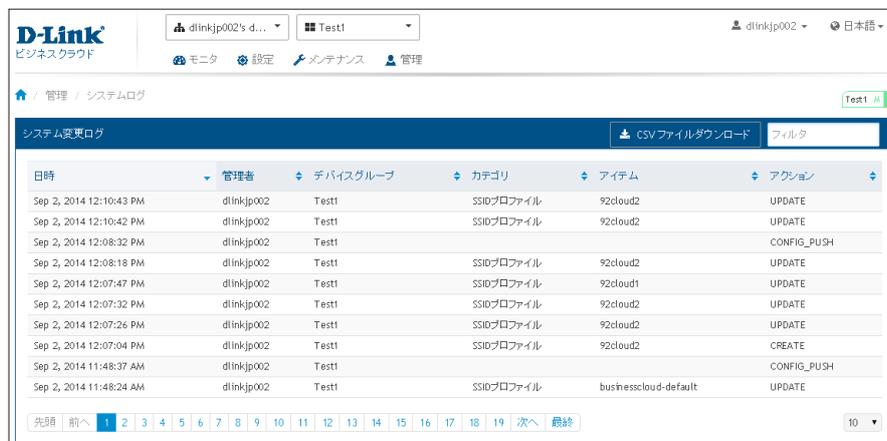


図 10-20 システムログ画面

本画面には以下の項目があります。

項目	説明
CSV ファイルダウンロード	システムログを CSV ファイル形式にてダウンロードすることが可能です。
フィルタ	表示されている「フィルタ」欄に検索条件を設定してリスト表示を絞り込みます。
日時	イベントが発生した日時です。
管理者	イベント発生を実行した管理者です。
デバイスグループ	イベント発生したデバイスグループです。
カテゴリ	発生イベントのカテゴリです。
アイテム	発生イベントのアイテムです。
アクション	発生イベントで実行された動作です。

組織設定

「組織設定」は組織についての管理項目です。

管理 > 組織設定 をクリックし、以下の画面を表示します。



図 10-21 組織設定画面

本画面には以下の項目があります。

項目	説明
フィルタ	表示されている「フィルタ」欄に検索条件を設定してリスト表示を絞り込みます。
ライセンス状態	組織のライセンス状態を表示しています。
組織名	組織名を表示しています。
ライセンスポイント	組織のライセンスポイントです。
日付	組織を登録した日時です。
アクション	当該の組織に対する動作を実行します。  (ごみ箱アイコン) をクリックすると組織を削除します。 「展開」をクリックすると組織の「UID」(識別番号) について表示します。 警告 組織を削除すると組織に関連する情報、設定情報、ライセンスなども一緒に削除され復元することができなくなります。組織を削除する際は十分に注意して実行してください。

付録 A 工場出荷時設定に戻す

リセットボタンを押下することで本製品の設定を工場出荷状態に戻します。

1. 必要に応じて設定ファイルのバックアップを行います。
2. 本製品の電源を入れた状態でリセットボタンを押します。ボタンを押す時間の長さにより動作は異なります。
 - ・再起動 - 2~5 秒ボタンを押し続けます。
 - ・初期化 - 6~15 秒ボタンを押し続けます。製品の設定が初期化されます。
 - ・起動ファームウェア変更 - 15 秒以上ボタンを押し続けると、ファームウェアアップデート前に使用していた旧ファームウェアバージョンで再起動します。
3. リセットボタンを放すと本製品は再起動します。

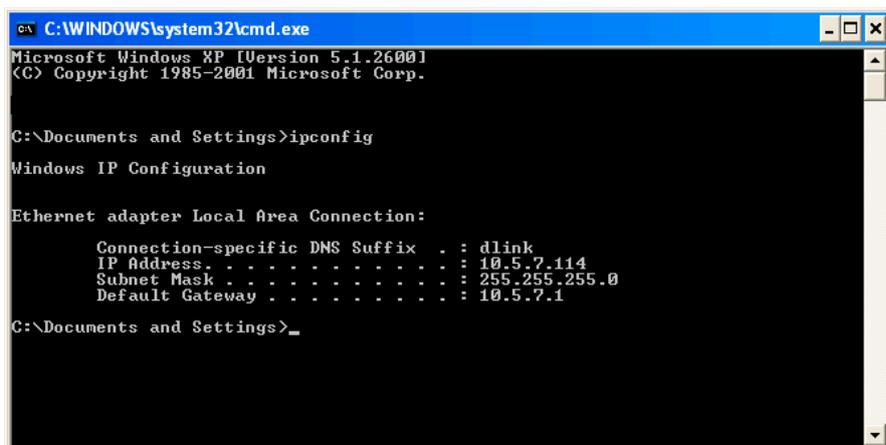
付録 B 基本的なネットワークの設定

IP アドレスのチェック

新しく無線アダプタをコンピュータに取り付けた後に、TCP/IP 設定の初期値は、自動的に IP アドレスを DHCP サーバ(すなわち無線ルータ)から取得するように設定される必要があります。

以下の手順で IP アドレスを確認します。

1. Windows の「スタート」メニュー>「ファイル名を指定して実行」を選択します。
2. 「ファイル名を指定して実行」ダイアログで「cmd」と入力し、「OK」ボタンをクリックします。(Windows Vista ユーザは「Start Search」ボックスに「cmd」と入力します。) プロンプトが表示されたら、「ipconfig」と入力し、「Enter」を押します。



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : dlink
    IP Address. . . . . : 10.5.7.114
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.5.7.1

C:\Documents and Settings>
```

図 B-1 ipconfig の実行画面

3. アダプタの IP アドレス、サブネットマスク、およびデフォルトゲートウェイが表示されます。アドレスが 0.0.0.0 である場合、アダプタのインストール、セキュリティ設定、およびルータの設定をチェックしてください。いくつかのファイアウォールソフトウェアプログラムは新しく取り付けられたアダプタ上の DHCP リクエストを防御する場合があります。ホットスポット(例えばホテル、コーヒーショップ、空港)で無線ネットワークと接続している場合、その無線ネットワーク設定については従業員または管理者にご確認ください。

固定 IP アドレスの割り当て

DHCP が有効でないゲートウェイ / ルータを使用している場合、または固定 IP アドレスを割り当てる必要がある場合、以下の手順で設定します。

1. Windows 7 では「スタート」-「コントロールパネル」-「ネットワークと共有センター」の順にクリックします。
2. 「アダプターの設定の変更」をクリックし、「ローカルエリア接続」アイコンを右クリックして「プロパティ」を選択します。
3. 「インターネットプロトコル (TCP/IPv4)」を選択し、「プロパティ」をクリックします。
4. 「次の IP アドレスを使う」をクリックし、ご使用のネットワークまたはルータ上の LAN 側 IP アドレスと同じサブネット上にある IP アドレスを入力します。

使用例:

ルータの LAN 側 IP アドレスが 192.168.0.1 である場合、192.168.0.X(X:2 ~ 99 の数字) とします。選択する番号がネットワーク上で使用されていないことを確認してください。「デフォルトゲートウェイ」をルータの LAN 側 IP アドレス (192.168.0.1) と同じにします。「優先 DNS サーバー」をルータの LAN 側 IP アドレス (192.168.0.1) と同じにします。「代替 DNS サーバー」は必要でないか、ご契約の ISP から通知されている DNS サーバを入力することができます。

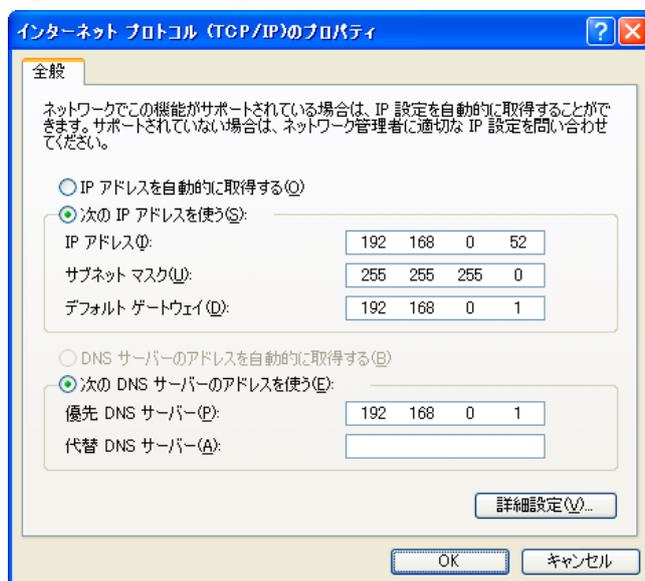


図 B-2 インターネットプロトコル

5. 「OK」ボタンをクリックし、設定を保存します。

付録C コマンドラインで Wi-Fi の設定を確認する場合

コンソール経由もしくはTELNETのコマンドラインを用いて、各VAPのSSID名とPSK、並びに各帯域で使用中のチャンネルを確認することができます。

注意 本機能は、ファームウェアバージョン 1.70 以上が DBA-1510P にインストールされている必要があります。通常時はこれらの情報は確認できませんが、クラウド管理画面上より「Wi-Fi 設定の取得」をクリックすることにより有効化され、60 分間確認できるようになります。

端末とコンソールポートの接続について

コンソール経由で Wi-Fi の設定を確認する場合、端末とコンソールポート間の接続に関しては、「第 4 章 クラウド AP の手動設定 (DBA-1510P)」の「コマンドラインインタフェース (CLI) の設定」をご確認ください。

Telnet の有効化について (Telnet 経由での確認の場合)

Telnet 経由で Wi-Fi の設定を確認する場合、Telnet 機能が有効になっている必要があります。

Telnet 機能の有効化に関しては、本マニュアルの「第 8 章 「設定」メニュー (D-Link Business Cloud)」の「一般設定」並びに「デバイスの設定」>「ツール」をご確認ください。

設定情報取得モード 有効化手順

1. ビジネスクラウド管理画面より、「モニタ」⇒「デバイスの設定」を選択します。
2. 以下の赤丸部をクリックし、該当のデバイス名を選択します。



図 C-1 該当デバイス名を選択

3. 「ツール」タブを選択します。
4. 「Wi-Fi 設定取得」ボタン (下図赤枠部) を押下すると "WIFI_DEBUG_SUCCESSFUL" メッセージが 2-3 秒表示され、60 分間、後述するコマンドで SSID 名・PSK を確認することができるようになります。
5. コンソールまたは Telnet にてデバイスにログインし、コマンドを実行してください。



図 C-2 Wi-Fi 設定取得

CLI コマンドについて

SSID 名と PSK を確認する

コマンド実行形式

```
get vap [vap0 | vap1 | vap2 | vap3 | vap4 | vap5 | vap6 | vap7] radio [radio0 | radio1] [ssid | wpa-personal-key]
```

オプション

オプション	説明
vap	次のオプションで SSID が紐付く無線インターフェース指定
vap0	1 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap1	2 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap2	3 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap3	4 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap4	5 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap5	6 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap6	7 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
vap7	8 つ目に作成した (2.4G or 5G の)SSID が紐付く無線インターフェース
radio	次のオプションで 2.4G or 5G を指定
radio0	確認する SSID が 2.4G 帯
radio1	確認する SSID が 5G 帯
ssid	SSID 名
wpa-personal-key	PSK

【例 1】1 つ目に作成した SSID の 2.4G の SSID 名を確認する場合

1 つ目に作成した SSID が紐付く無線インターフェースを指定

2.4G を指定

SSID 名を出力

```
CLOUD_CLI>> get vap vap0 radio radio0 ssid
```

Property	Value
ssid	SSID01

SSID 名が「SSID01」である事を意味しています。

図 C-3 1 つ目に作成した SSID の 2.4G の SSID 名を確認

【例 2】2 つ目に作成した SSID の 5G の PSK を確認する場合

2 つ目に作成した SSID が紐付く無線インターフェースを指定

5G を指定

PSK を出力

```
CLOUD_CLI>> get vap vap1 radio radio1 wpa-personal-key
```

Property	Value
wpa-personal-key	12345678

PSK が「12345678」である事を意味しています。

図 C-4 2 つ目に作成した SSID の 5G の PSK を確認する場合

チャンネルを確認する

コマンド実行形式

```
get radio [ radio0 | radio1 ] channel
```

オプション

オプション	説明
radio	次のオプションで 2.4G or 5G を指定
radio0	2.4G のチャンネルを確認
radio1	5G のチャンネルを確認
channel	(2.4G or 5G の) チャンネルを出力

【例 1】 2.4G のチャンネルを確認する場合

```
CLOUD_CLI>> get radio radio0 channel
Property          Value
-----
channel           8
```

2.4Gのチャンネルが「8」である事を意味しています。

図 C-3 2.4G のチャンネルを確認する場合

【例 2】 5G のチャンネルを確認する場合

```
CLOUD_CLI>> get radio radio1 channel
Property          Value
-----
channel           124
```

5G のチャンネルが「124」である事を意味しています。

図 C-4 5G のチャンネルを確認する場合

Telnet の無効化について（Telnet 経由での確認の場合）

Telnet 経由で Wi-Fi の設定確認を実施した場合、必要に応じて Telnet を無効化してください。

Telnet 機能の無効化に関しては、本マニュアルの「第 8 章 「設定」メニュー (D-Link Business Cloud)」の「[一般設定](#)」並びに「[デバイスの設定](#)」>「[ツール](#)」をご確認ください。

付録 D 機器故障の際は

DBA-1510P はビジネス向けネットワーク製品の長期無償保証サービス リミテッドライフタイム保証の対象製品です。故障時は当社 WEB サイト「各種お問い合わせ」ページ、故障・修理申請より申請ください。

故障・修理申請

<https://www.dlink-jp.com/support/contact>

D-Link ではリミテッドライフタイム保証の他に有償保守サービスを提供しています。有償保守サービス詳細については、次の URL より保守約款、仕様書をご確認ください。

有償保守サービス詳細

<https://www.dlink-jp.com/support/support-info>

注意 製品保証に基づき修理のご依頼を頂く場合、必ず事前にお客様にてクラウドからデバイス UID 削除をお願いします。デバイス UID を削除しない場合、修理期間中もポイントが消費されます。D-Link はお客様の設定画面に接続できないため、ご依頼を頂いてもデバイス UID の削除はできないため、デバイス UID 削除忘れ時のポイント消費について、苦情およびポイントの回復はお請けできません。

注意 有償保守サービス、その他理由による機器交換が発生した場合、必ずお客様にてクラウドから故障機器のデバイス UID 削除、並びに代替機のデバイス UID 登録をお願い致します。デバイス UID を削除しない場合、機器交換後も故障機器のポイントが消費され続けます。

注意 D-Link はお客様の設定画面に接続できないため、ご依頼を頂いてもデバイス UID の削除はできないため、UID 削除忘れ時のポイント消費について、苦情およびポイント回復はお請けできません。