



D-Link DBA シリーズ

(DBA-1210P/DBA-2520P/DBA-2620P/DBA-2720P/DBA-2820P/
DBA-3621P/DBA-X2830P/DBA-X1230P/DBA-X5480P)

D-Link Nuclias – Cloud networking solution

ユーザマニュアル
.....

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。

	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。
	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。
	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



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。



ぬれた手でさわらない
感電の原因となります。



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。



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。



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。



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。



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。



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。



電子レンジ、IH 調理器などの加熱調理機、圧力釜など高压容器に入れたり、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



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。



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、煙が出なくなつてから販売店に修理をご依頼ください。



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。



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。



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。



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。



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。



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。



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。



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、ほこ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。



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。



ガス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。



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。



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。



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。



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、聴覚などの耳の障害の原因となります。



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。



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。



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。



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。



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。



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。抜かずに行くと、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、海外で使えない。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る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もあるため、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

この装置は、クラス B 機器です。この装置は、住宅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下さい。

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でのご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。踏みつけられたり踏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ラベルや「Warranty Void Sticker」（シール）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。
※当社出荷時に「Warranty Void Sticker」（シール）が貼られていない製品もあります。

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 LAN ケーブルまたは PoE スイッチの電源を抜いてください。（別売りの AC アダプタ「PSE-M12V25A-I」使用時は AC アダプタを抜いてください。）

電源が再度供給できる状態になってから電源プラグや LAN ケーブルを再度接続します。

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、IEEE 802.11ac および IEEE 802.11ax に準拠しています。

● IEEE 802.11ax 規格

IEEE 802.11ax 規格は「Wi-Fi6」とも呼ばれ、最大通信速度は 9600Mbps です。2.4GHz 帯および 5GHz 帯の周波数を利用し、「OFDMA」技術をサポートしています。

● IEEE 802.11ac 規格

IEEE 802.11ac 規格の無線通信速度は、IEEE 802.11n 規格よりも高速化されており、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 400Mbps 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。

802.11n/802.11ac/802.11ax 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/WPA3 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。WPA3 は、無線 LAN の普及促進の業界団体である Wi-Fi Alliance によって 2018 年 6 月に策定された無線 LAN の暗号化技術の規格名称です。WPA2 に代る次世代セキュリティ規格で、よりセキュアな通信を実現します。

「WPA-Personal」「WPA2-Personal」「WPA3-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」「WPA2-Enterprise」「WPA3-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」「WPA2-Enterprise」「WPA3-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。

また、ここに記載の内容は一般的な無線技術の内容を多く含んでおり、当製品には実装されていない機能を含む場合がありますので予めご了承ください。

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、ご購入頂いた販売代理店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。

安全にお使いいただくために

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>

注意

製品に貼られているラベルや「Warranty Void Sticker」(シール)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。

※当社出荷時に「Warranty Void Sticker」(シール)が貼られていない製品もあります。

- 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	12
本マニュアルの対象者.....	12
本マニュアルの対象製品.....	12
第 1 章 Nuclias の概要	13
Nuclias の概要.....	13
Nuclias の用語とコンセプト.....	14
Nuclias 対応機器.....	15
Nuclias 基本仕様.....	16
第 2 章 Nuclias 用 AP のご利用にあたって	17
DBA-1210P の各部名称.....	17
DBA-1210P 前面パネル.....	17
DBA-1210P 背面パネル.....	18
DBA-2520P の各部名称.....	19
DBA-2520P 前面パネル.....	19
DBA-2520P 背面パネル.....	20
DBA-2520P 側面.....	20
DBA-2620P の各部名称.....	21
DBA-2620P 前面パネル.....	21
DBA-2620P 背面パネル.....	22
DBA-2620P 側面.....	22
DBA-2720P の各部名称.....	23
DBA-2720P 前面パネル.....	23
DBA-2720P 背面パネル.....	24
DBA-2720P 側面.....	24
DBA-2820P の各部名称.....	25
DBA-2820P 前面パネル.....	25
DBA-2820P 背面パネル.....	26
DBA-2820P 側面.....	26
DBA-3621P の各部名称.....	27
DBA-3621P 前面パネル / 背面パネル.....	27
DBA-3621P 底面.....	28
DBA-X2830P の各部名称.....	29
DBA-X2830P 前面パネル.....	29
DBA-X2830P 背面パネル.....	30
DBA-X2830P 側面.....	30
DBA-X1230P の各部名称.....	31
DBA-X1230P 前面パネル.....	31
DBA-X1230P 背面パネル.....	32
DBA-X5480P の各部名称.....	33
DBA-X5480P 前面パネル.....	33
DBA-X5480P 側面パネル.....	34
第 3 章 Nuclias 用 AP の設置	35
パッケージの内容.....	35
ネットワーク接続前の準備.....	36
Nuclias 用 AP の設定・設置.....	37
Nuclias と Nuclias 用 AP の接続.....	37
DBA-1210P の設置.....	39
DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P の設置.....	41
DBA-3621P の設置.....	44
イーサネットケーブルの接続.....	47
IP アドレスの設定について.....	47
電源の投入.....	47

第 4 章 Nuclias の基本設定	48
初期設定手順について	48
アカウントと組織の作成	49
ログイン	51
Nuclias ユーザインタフェースについて	51
プロファイルの作成	52
Wi-Fi ポリシーの設定	53
Wi-Fi ポリシーの設定 (SSID プロファイル編集)	54
サイトの作成	57
Nuclias 対応機器の登録	59
Nuclias 対応機器をオンラインにする	60
第 5 章 ユーザプロファイル	61
ユーザプロファイル	61
マイプロフィール	61
ログイン履歴	62
API アクセス	62
第 6 章 ダッシュボード	64
ダッシュボード	64
ダッシュボード > 概要エリア	64
ダッシュボード > マップ + アラート + レポート エリア	65
ダッシュボード > 最近 24 時間サマリ エリア	65
第 7 章 モニタ	66
アクセスポイント - デバイス	66
アクセスポイント - クライアント	67
アクセスポイント - イベントログ	68
地図	69
フロアプラン	70
近隣の AP	71
ネットワーク	72
第 8 章 デバイス設定	74
アクセスポイント - プロファイル	74
プロファイル - SSID	76
プロファイル - 無線	89
プロファイル - 設定	93
アクセスポイント - デバイス	94
デバイス - 基本	96
デバイス - サマリ	97
デバイス - SSID	98
デバイス - 無線	100
デバイス - ツール	102
デバイス - ライセンス	103
アクセスポイント - IP ACL	104
認証 - 認証サーバ	106
認証 - ローカル認証 DB	112
MAC ACL	114
ワールドガーデン	116
スケジュールポリシー	118
スプラッシュページ	120
第 9 章 レポート	123
変更ログ	123
サマリレポート	124
アラート	125
ライセンス (レポート)	126

第 10 章 管理	127
アカウント管理.....	127
組織管理.....	129
ライセンス管理.....	133
インベントリ	143
ファームウェア	144
アラート設定	147
証明書の管理	148
アドバンスド設定 > SAML 設定	150
アドバンスド設定 > SMS 設定	152
アドバンスド設定 > シスログサーバ 設定	153
デバイスの追加	154
デバイス一括インポート	155
第 11 章 ヘルプ	156
お知らせ.....	156
連絡をする	156
リソース.....	157
トラブルシューティング	157
チュートリアル.....	157
第 12 章 Web GUI、CLI からの設定について	158
Web GUI (Web ベース設定ユーティリティ) について	158
Web GUI 設定画面へのログイン	158
ステータス	159
システム > システム	160
システム > リセットとファームウェアアップグレード	161
ネットワーク > 基本設定	162
ネットワーク > 高度な設定	163
ログアウト	164
コマンドラインインタフェース (CLI) の設定	164
端末をコンソールポートに接続する	164
CLI コマンド一覧	165
付録	167
付録 A ライセンスの適用や開始等に関する詳細	167
付録 B E メール認証時の画面	168
付録 C 機器故障の際は.....	169

はじめに

- [本マニュアルの対象者](#)
- [本マニュアルの対象製品](#)

本マニュアルの対象者

本マニュアルは、本サービスの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。

本マニュアルの対象製品

本マニュアルは、「Nuclias」および「Nuclias」に登録して使用する以下の製品について記載しています。

- DBA-1210P^{※1}
- DBA-2520P^{※1}
- DBA-2620P^{※1}
- DBA-2720P^{※1}
- DBA-2820P^{※1}
- DBA-3621P^{※2}
- DBA-X2830P
- DBA-X1230P
- DBA-X5480P^{※2}

※1 販売終了

※2 販売終了予定

第 1 章 Nuclias の概要

- Nuclias の概要
- Nuclias の用語とコンセプト
- Nuclias 対応機器
- Nuclias 基本仕様

Nuclias の概要

Nuclias は、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。Nuclias 対応ネットワーク機器は、Nuclias サーバとの間で管理用トンネルセッションを維持し、Nuclias 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ます。そのためネットワーク管理者は、Nuclias サーバ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。

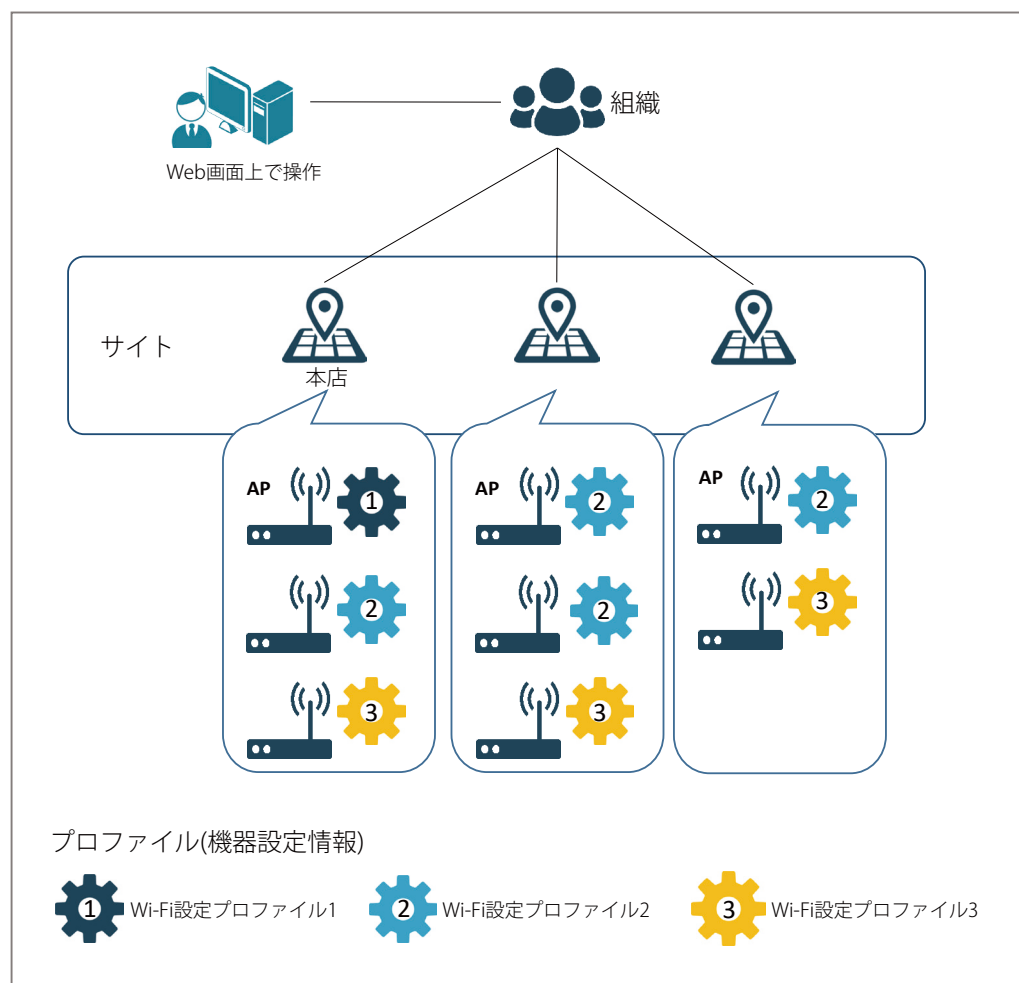


図 1-1 Nuclias 構成概要

Nuclias の用語とコンセプト

Nuclias に関しては下記の用語があります。

項目	説明
組織	Nuclias の利用を開始する際に、お客様は 1 つの組織を作成する必要があります。 この組織の中で、設定やデバイス、ライセンスを管理します。
サイトタグ	「サイトタグ」は、複数のサイトを一つにまとめて管理や閲覧が行えます。 また、組織内の特定のユーザに対して、組織全体ではなく一部のサイトタグにのみアクセスできるように設定することもできます。
サイト	「サイト」はデバイスの物理的な位置を示し、複数のデバイスをグループにし、取り扱いしやすいようにしたものです。 また、組織内の特定のユーザに対して、組織全体ではなく一部のサイトにのみアクセスできるように設定することもできます。
プロファイル	「プロファイル」は Wi-Fi 設定ポリシーをまとめたものです。組織内に複数作成することができます。 各 Nuclias 管理下デバイスには必ず 1 つのプロファイルが紐づけられている必要があります。

各ユーザアカウントが Nuclias にて行える操作に関して、下記の通り 4 種類の権限があります。

項目	説明
管理者	全ての設定並びに情報の閲覧が可能です。
編集者	既に作成されている設定の変更を行うことができます。 ただし、ユーザやデバイス、設定情報などの追加 / 削除の操作はできません。
閲覧者	デバイスの利用状況や無線クライアントの情報を閲覧することができます。設定の追加、変更、削除はできません。 Wi-Fi ポリシーの設定については、追加、変更、削除だけでなく閲覧することもできません。 アラート、ライセンス、インベントリの情報の閲覧は可能です。
モニタ閲覧者	デバイス使用状況や無線クライアントの情報の閲覧のみが可能です。

Nuclias 対応機器

Nuclias では以下の機器をサポートしています。(2025 年 5 月現在)

■ DBA シリーズ



DBA-1210P ※ 1



DBA-2520P ※ 1



DBA-2620P ※ 1



DBA-2720P ※ 1



DBA-2820P ※ 1



DBA-3621P ※ 2



DBA-X2830P



DBA-X1230P

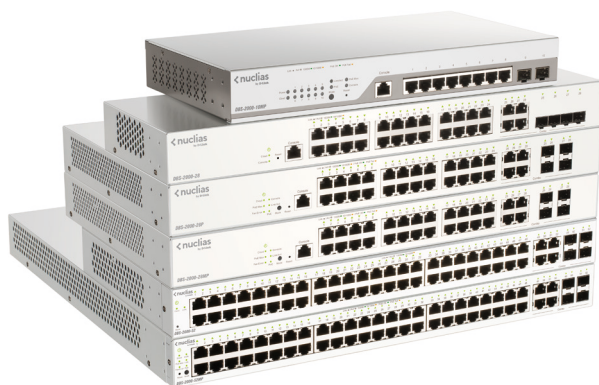


DBA-X5480P

※ 1 販売終了

※ 2 販売終了予定

■ DBS シリーズ



DBS-2000 シリーズ

■ DBG シリーズ



DBG-2000



DBG-X1000

Nuclias 基本仕様

Nuclias 対応ネットワーク機器は、リンクアップし、IP アドレスを取得すると Nuclias との間で SSL セッションを確立します。この時点でネットワーク機器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。ネットワーク機器がクラウドとの接続を完了すると、Nuclias 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、ネットワーク機器は Nuclias 用機器として動作を開始します。Nuclias 管理用 SSL セッションは維持され、Nuclias 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、Nuclias から各デバイスを管理する用途で利用されます。

プロトコル	用途・備考
TCP 443 (SSL)	Nuclias 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)	名前解決用
TCP 53 (DNS)	名前解決用

また、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

■ 推奨ブラウザ

Nuclias の推奨ブラウザは以下です。

- Google Chrome

注意 ライセンス切れとなった機器の動作については、動作保証外になります。

第 2 章 Nuclias 用 AP のご利用にあたって

- DBA-1210P の各部名称
- DBA-2520P の各部名称
- DBA-2620P の各部名称
- DBA-2720P の各部名称
- DBA-2820P の各部名称
- DBA-3621P の各部名称
- DBA-X2830P の各部名称
- DBA-X1230P の各部名称
- DBA-X5480P の各部名称

DBA-1210P の各部名称

DBA-1210P 前面パネル

DBA-1210P の前面パネルには、ステータス LED が配置されています。



図 2-1 DBA-1210P 前面パネル

ステータス LED は以下の状態を表示します。

LED 状態	DBA-1210P 状態
● 緑点灯	Nuclias と正常に接続されており、管理モードで動作している状態です。
● 緑点滅	Nuclias へ接続を試みている状態です。
● 橙点灯	起動処理中の状態です。
● 橙点滅	初期化中の状態です。
● 赤点灯	Nuclias サーバと正常に接続できていない状態です。 IP アドレスの設定がご利用のネットワーク環境に即していない場合等が考えられます。
● 消灯	電源が入っていません。

DBA-1210P 背面パネル

DBA-1210P の背面パネルには、LAN ポート（PoE）（10BASE-T/100BASE-TX/1000BASE-T）、電源コネクタ、リセットボタンおよびロックソケットが配置されています。

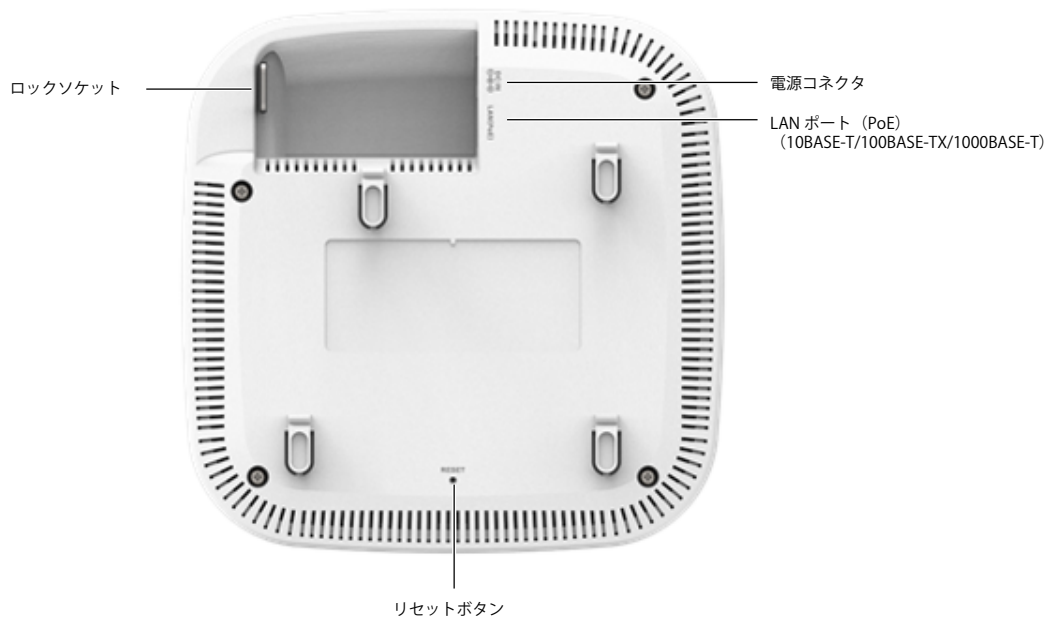


図 2-2 DBA-1210P 背面パネル

部位	機能
LAN ポート（PoE） （10BASE-T/100BASE-TX/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。IEEE802.3af に準拠した 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ドカテゴリ 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。
電源コネクタ	付属の AC アダプタを接続します。
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。 - 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、製品の設定が初期化され、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。
ロックソケット	別途、南京錠やワイヤー等をご準備いただくと、DBA-1210P 本体とマウントプレートを物理的にロックすることができます。

DBA-2520P の各部名称

DBA-2520P 前面パネル

DBA-2520P の前面パネルには、ステータス LED が配置されています。

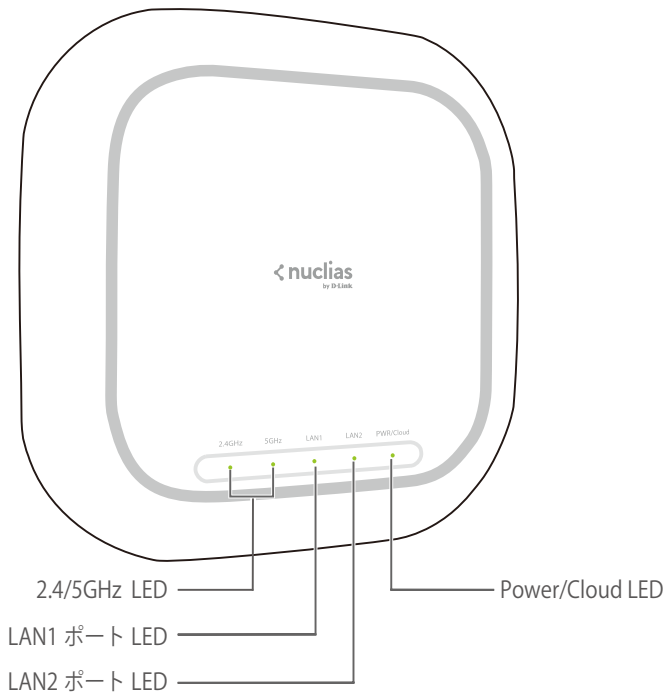


図 2-3 DBA-2520P 前面パネル

ステータス LED は以下の状態を表します。

LED	LED 状態	DBA-2520P 状態
2.4GHz/5GHz LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータの送受信を行っていません。
LAN1/LAN2 ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-2520P 背面パネル

DBA-2520P の背面パネルの各部名称について説明します。

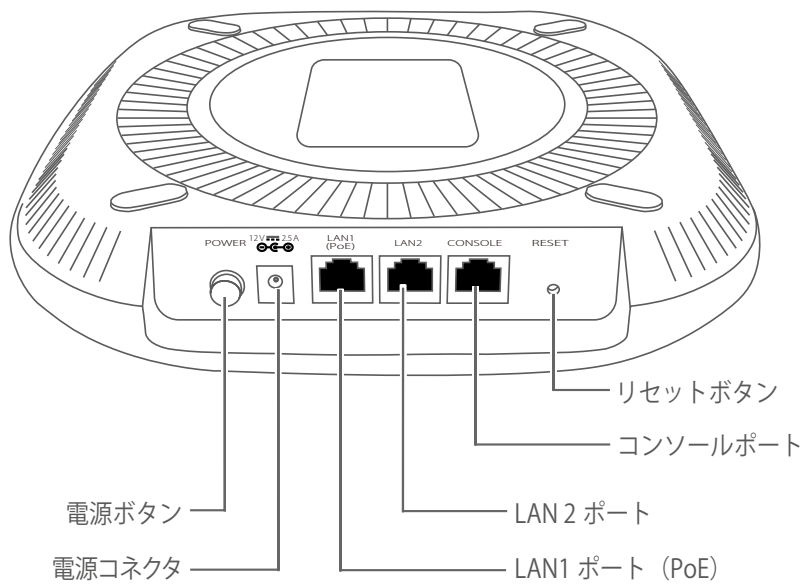


図 2-4 DBA-2520P 背面パネル

部位	機能
電源ボタン	電源の ON/OFF を行います。 注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) / LAN2 ポート (10BASE-T/100BASE-TX/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、LAN1 ポートは 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。 LAN2 ポートは PoE 受電には対応していません。 LAN1 ポートと LAN2 ポートでリンクアグリゲーションを設定、使用することもできます。 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。
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。 - 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、製品の設定が初期化され、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。

※ 1 : AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-2520P 側面

DBA-2520P 下部の側面には、セキュリティスロットが搭載されています。
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。

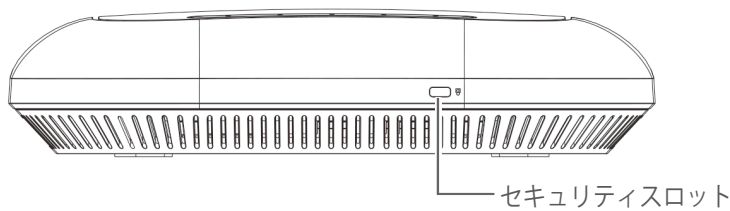


図 2-5 DBA-2520P 側面

DBA-2620P の各部名称

DBA-2620P 前面パネル

DBA-2620P の前面パネルには、ステータス LED が配置されています。

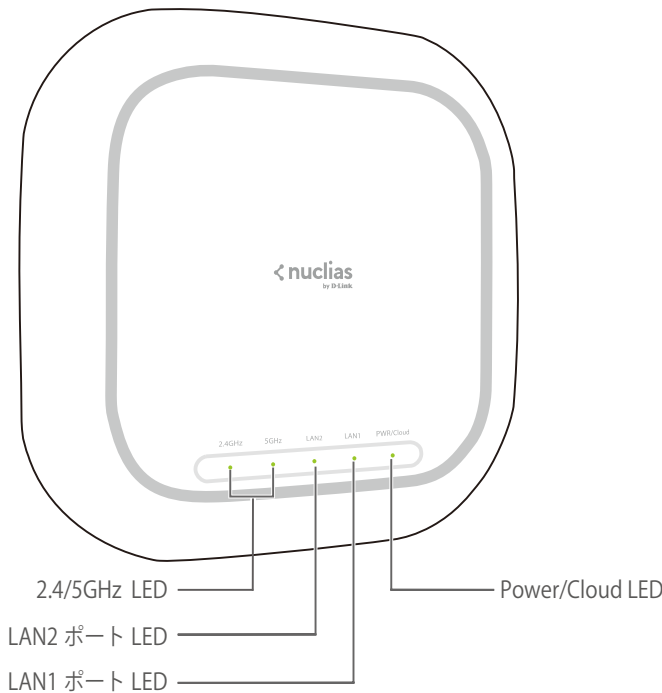


図 2-6 DBA-2620P 前面パネル

ステータス LED は以下の状態を表します。

LED	LED 状態	DBA-2620P 状態
2.4GHz/5GHz LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータを送受信を行っていません。
LAN1/LAN2 ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-2620P 背面パネル

DBA-2620P の背面パネルの各部名称について説明します。

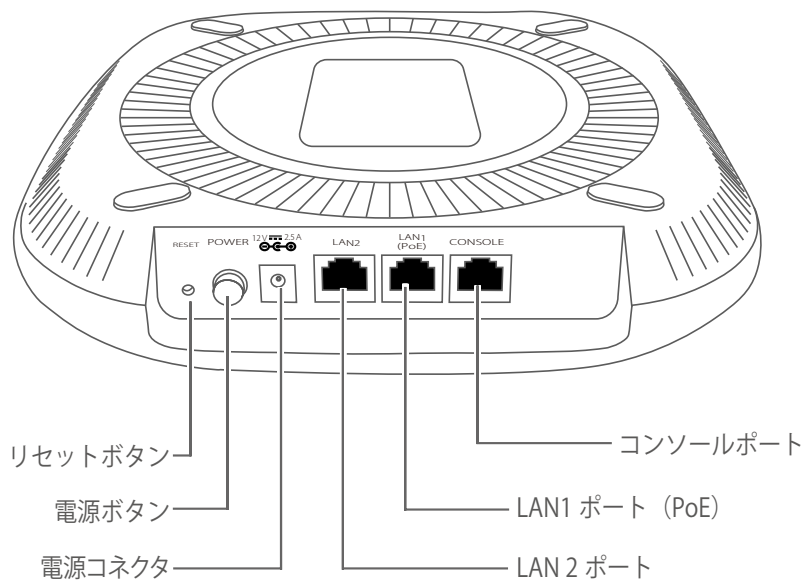


図 2-7 DBA-2620P 背面パネル

部位	機能
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。 - 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、製品の設定が初期化され、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。
電源ボタン	電源の ON/OFF を行います。 注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) / LAN2 ポート (10BASE-T/100BASE-TX/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、LAN1 ポートは 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。LAN2 ポートは PoE 受電には対応していません。LAN1 ポートと LAN2 ポートでリンクアグリゲーションを設定、使用することもできます。 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。

※ 1：AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-2620P 側面

DBA-2620P 下部の側面には、セキュリティスロットが搭載されています。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。

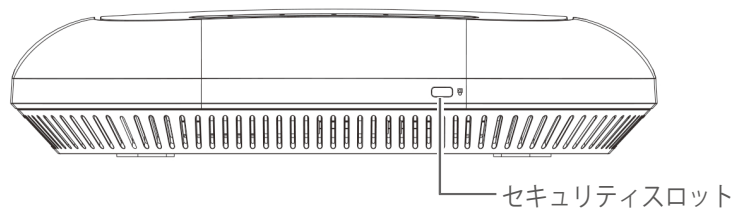


図 2-8 DBA-2620P 側面

DBA-2720P の各部名称

DBA-2720P 前面パネル

DBA-2720P の前面パネルには、ステータス LED が配置されています。

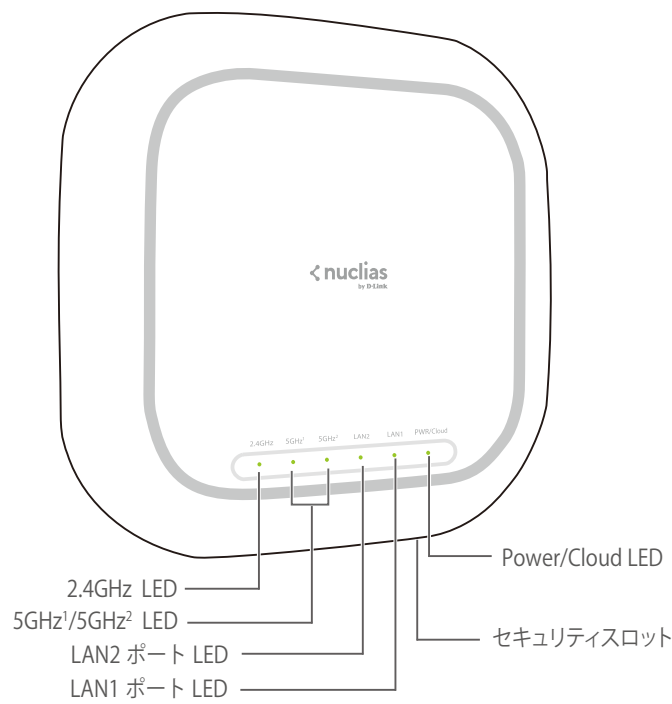


図 2-9 DBA-2720P 前面パネル

ステータス LED は以下の状態を表します。

LED	LED 状態	DBA-2720P 状態
2.4GHz/ 5GHz¹/5GHz² LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータの送受信を行っていません。
LAN1/LAN2 ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-2720P 背面パネル

DBA-2720P の背面パネルの各部名称について説明します。

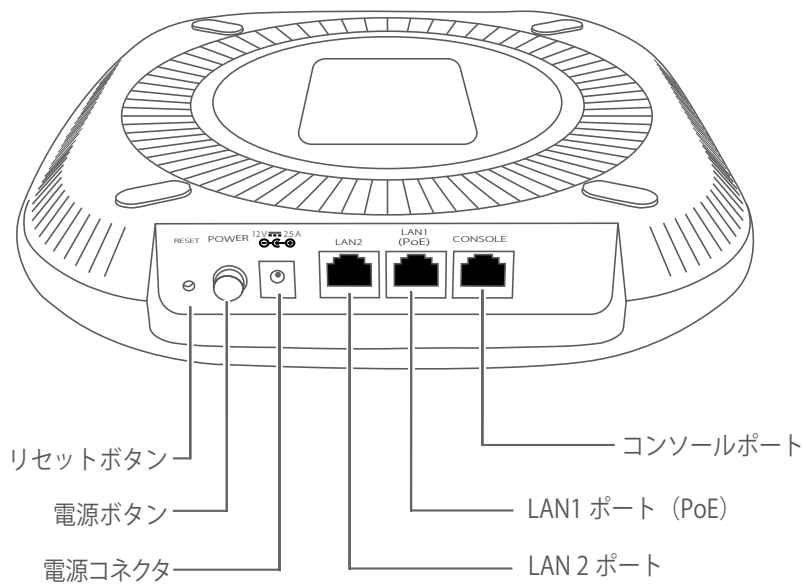


図 2-10 DBA-2720P 背面パネル

部位	機能
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。 - 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、製品の設定が初期化され、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。
電源ボタン	電源の ON/OFF を行います。 注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) / LAN2 ポート (10BASE-T/100BASE-TX/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、LAN1 ポートは 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。LAN2 ポートは PoE 受電には対応していません。LAN1 ポートと LAN2 ポートでリンクアグリゲーションを設定、使用することもできます。 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。

※ 1：AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-2720P 側面

DBA-2720P 下部の側面には、セキュリティスロットが搭載されています。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。

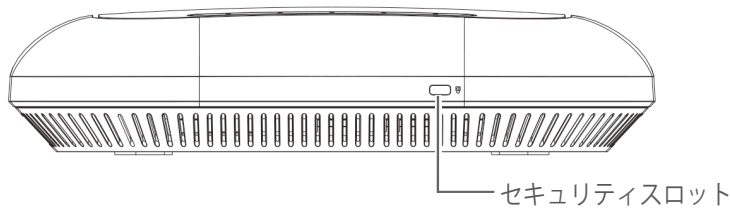


図 2-11 DBA-2720P 側面

DBA-2820P の各部名称

DBA-2820P 前面パネル

DBA-2820P の前面パネルには、ステータス LED が配置されています。

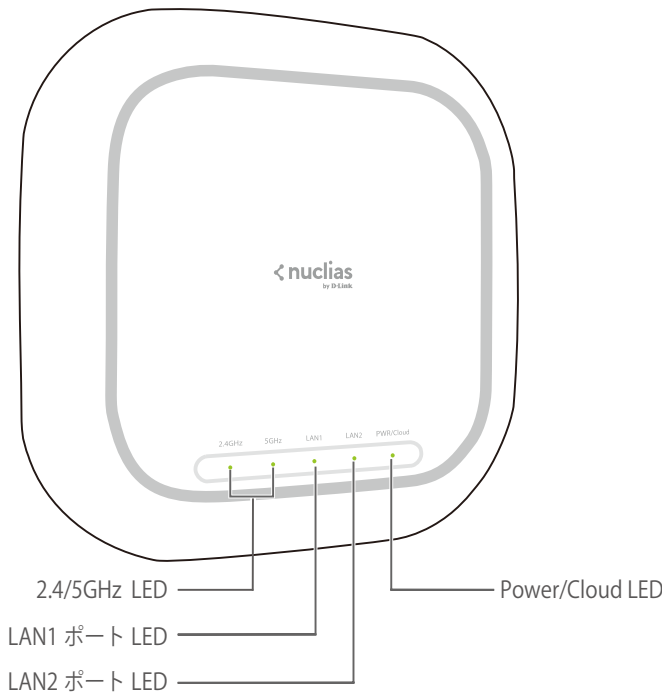


図 2-12 DBA-2820P 前面パネル

ステータス LED は以下の状態を表します。

LED	LED 状態	DBA-2820P 状態
2.4GHz/5GHz LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータの送受信を行っていません。
LAN1/LAN2 ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-2820P 背面パネル

DBA-2820P の背面パネルの各部名称について説明します。

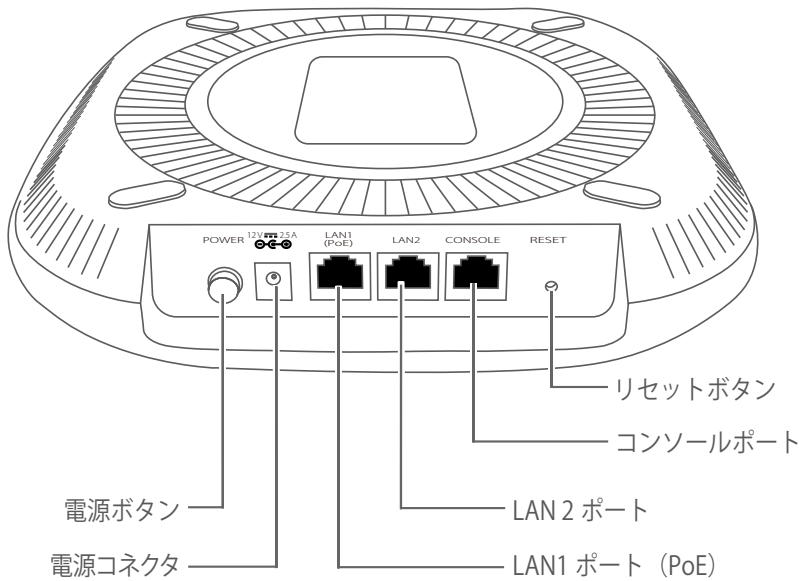


図 2-13 DBA-2820P 背面パネル

部位	機能
電源ボタン	電源の ON/OFF を行います。 注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) / LAN2 ポート (10BASE-T/100BASE-TX/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、LAN1 ポートは 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。 LAN2 ポートは PoE 受電には対応していません。 LAN1 ポートと LAN2 ポートでリンクアグリゲーションを設定、使用することもできます。 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。
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。 - 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、製品の設定が初期化され、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。

※ 1：AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-1」をご使用ください。

DBA-2820P 側面

DBA-2820P 下部の側面には、セキュリティスロットが搭載されています。
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。

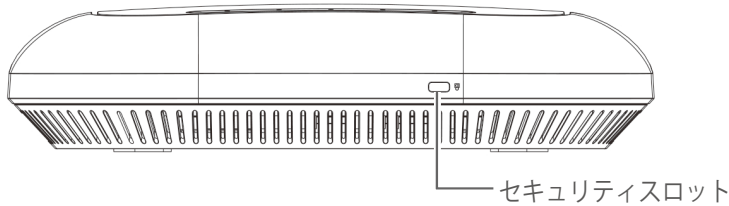


図 2-14 DBA-2820P 側面

DBA-3621P の各部名称

DBA-3621P 前面パネル / 背面パネル

DBA-3621P の前面パネルと背面パネルについて説明します。

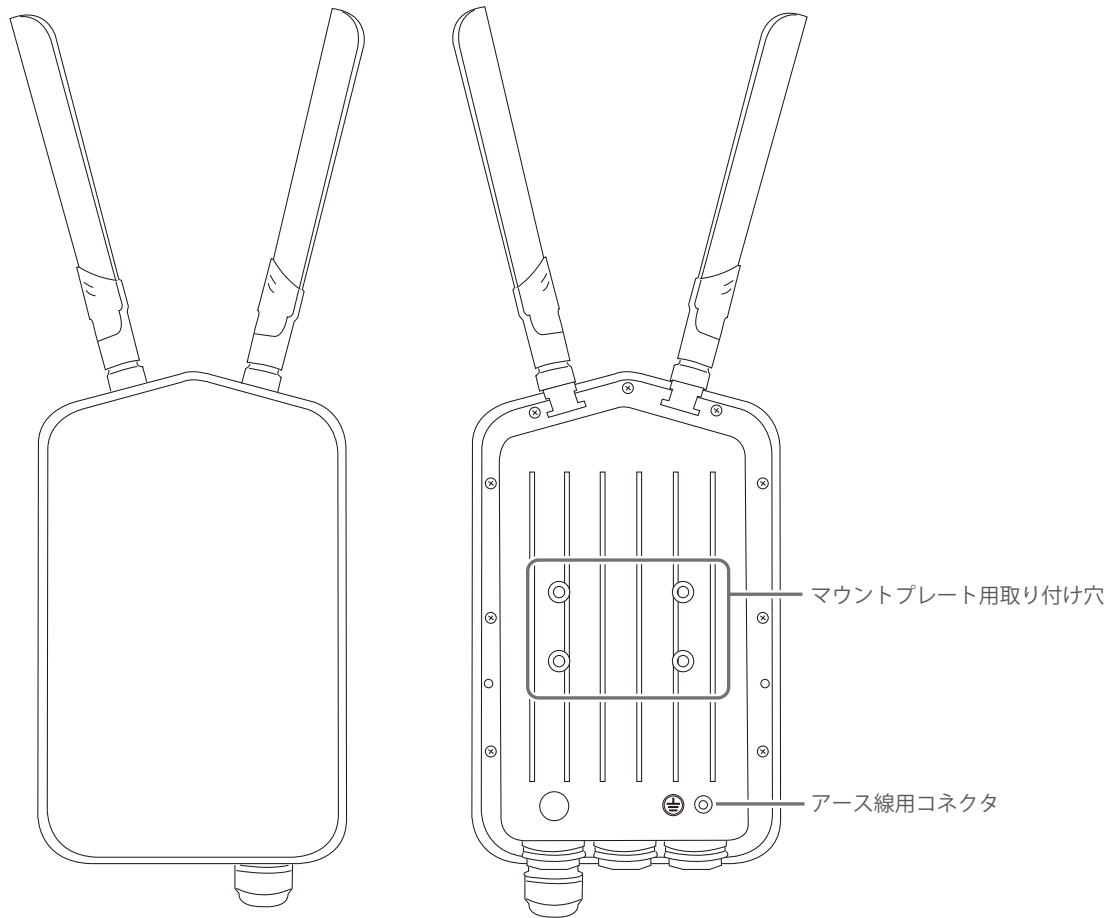


図 2-15 DBA-3621P 前面/パネル / 背面パネル

部位	機能
マウントプレート用取り付け穴	付属のマウントプレートを取り付ける際に使用します。
アース線用コネクタ	アース線を接続します。

DBA-3621P 底面

DBA-3621P の底面の部位について説明します。

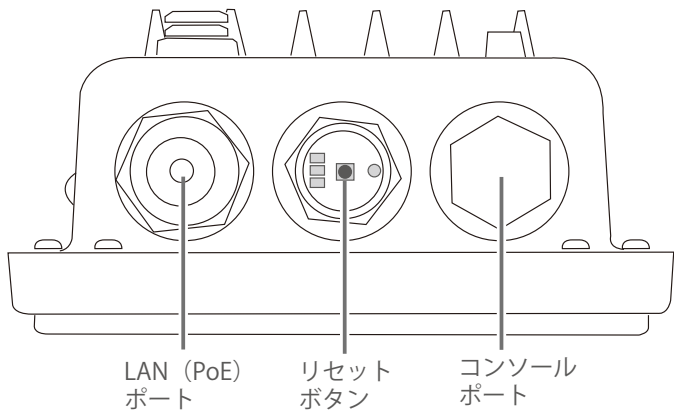


図 2-16 DBA-3621P 底面

部位	機能
LAN (PoE) ポート	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。
リセットボタン	機器のリセットボタンです。10 秒押し続けると、製品の設定が初期化されます。
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。

DBA-3621P LED 表示

DBA-3621P の LED は本体底面にあります。

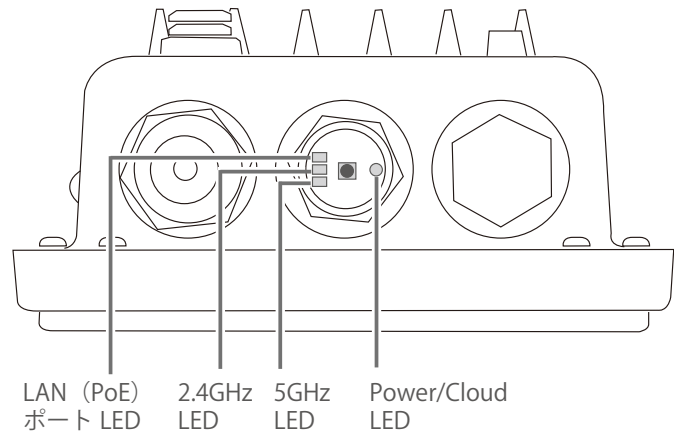


図 2-17 DBA-3621P LED 表示

LED	LED 状態	DBA-3621P 状態
LAN (PoE) ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
2.4GHz/5GHz LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータの送受信を行っていません。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	設定のリセット中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-X2830P の各部名称

DBA-X2830P 前面パネル

DBA-X2830P の前面パネルには、ステータス LED が配置されています。

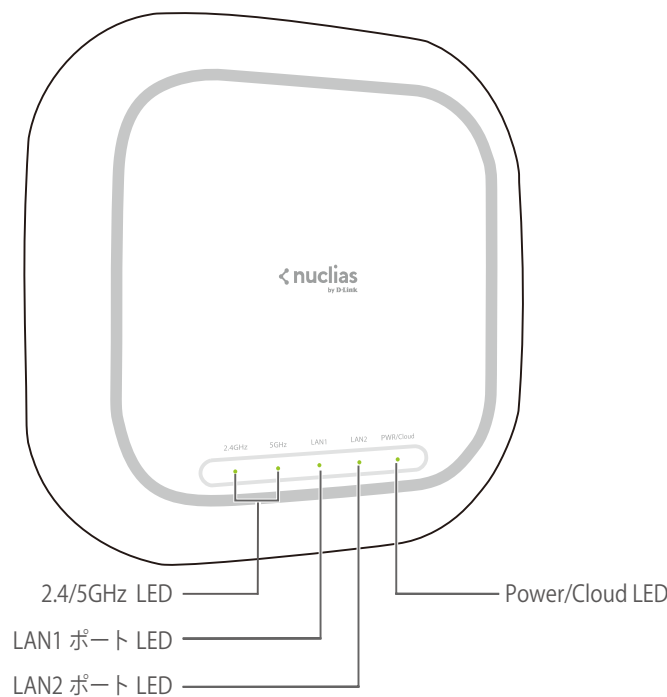


図 2-18 DBA-X2830P 前面パネル

ステータス LED は以下の状態を表します。

LED	LED 状態	DBA-X2830P 状態
2.4GHz/5GHz LED	● 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。
	● 緑点滅	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。
	● 消灯	無線 LAN による通信及びデータを送受信を行っていません。
LAN1/LAN2 ポート LED	● 緑点灯	ネットワークにリンクしています。
	● 緑点滅	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。
Power/Cloud LED	● 橙点灯	起動中です。
	● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
	● 緑点滅	Nuclias へ接続を試みている状態です。
	● 緑点灯	Nuclias による管理モードで動作しています。
	● 赤点灯	正しく動作していません。
	● 消灯	電源が入っていません。

DBA-X2830P 背面パネル

DBA-X2830P の背面パネルの各部名称について説明します。

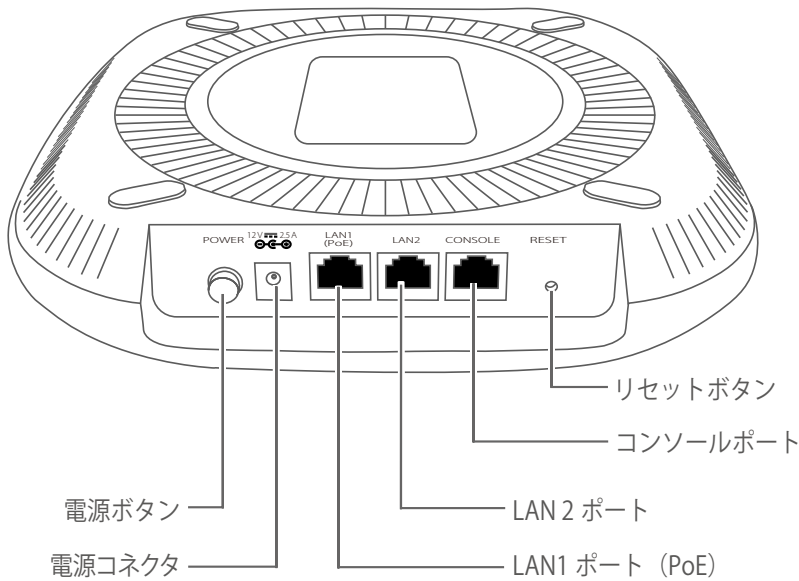


図 2-19 DBA-X2830P 背面パネル

部位	機能
電源ボタン	電源の ON/OFF を行います。 注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) / LAN2 ポート (10BASE-T/100BASE-TX/1000BASE-T/2.5G BASE-T)	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T /2.5G BASE-T イーサネットへの接続が可能です。 また、LAN1 ポートは 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。 LAN2 ポートは PoE 受電には対応していません。 LAN1 ポートと LAN2 ポートでリンクアグリゲーションを設定、使用することもできます。 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 /2.5G BASE-T の場合はエンハンスドカテゴリ 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。
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。 - 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、製品の設定が初期化され、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。

※ 1：AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-X2830P 側面

DBA-X2830P 下部の側面には、セキュリティスロットが搭載されています。
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。

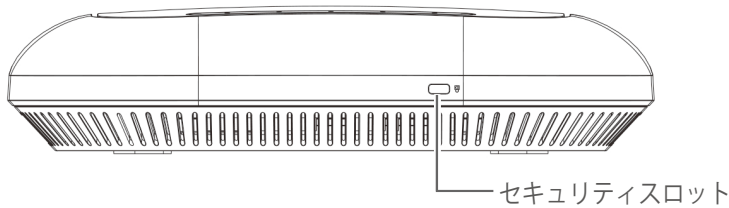


図 2-20 DBA-X2830P 側面

DBA-X1230P の各部名称

DBA-X1230P 前面パネル

DBA-X1230P の前面/パネルには、Power/Cloud LED が配置されています。

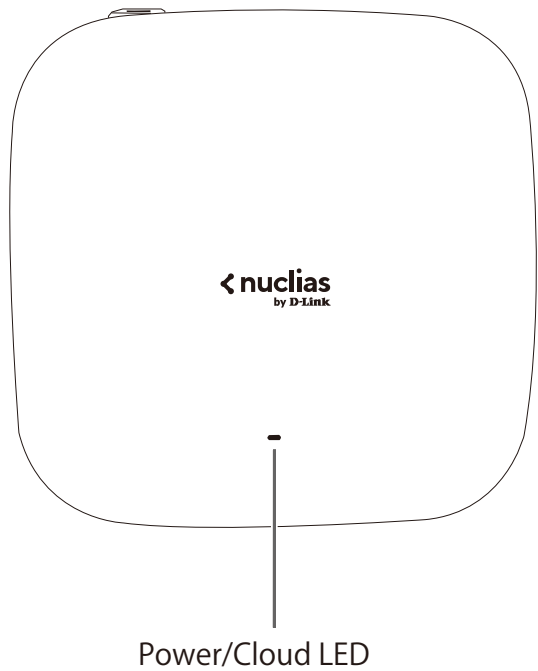


図 2-21 DBA-X1230P 前面/パネル

Power/Cloud LED は以下の状態を表示します。

LED 状態	DBA-X1230P 状態
● 緑点灯	Nuclias と正常に接続されており、管理モードで動作している状態です。
● 緑点滅	Nuclias へ接続を試みている状態です。
● 橙点灯	起動中です。
● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
● 赤点灯	正しく動作していません。
● 消灯	電源が入っていません。

DBA-X1230P 背面パネル

DBA-X1230P の背面パネルの各部名称について説明します。

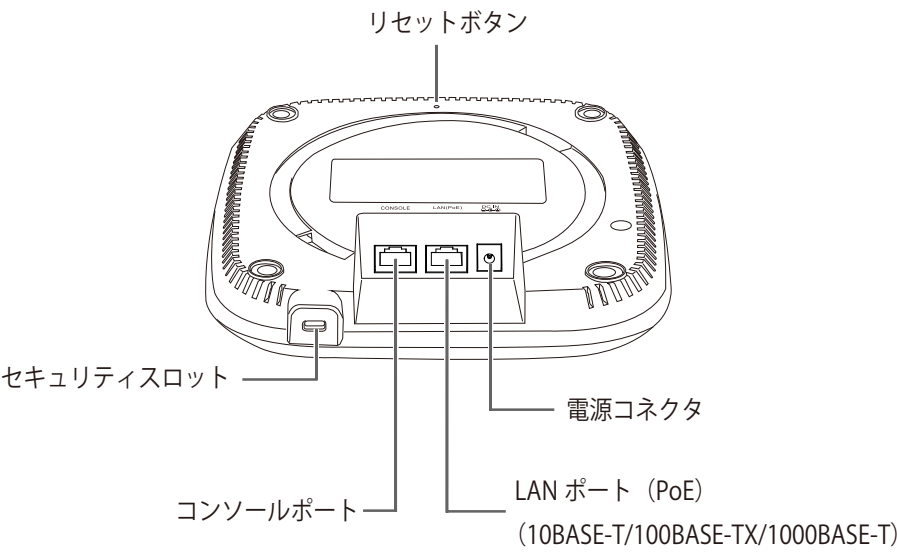


図 2-22 DBA-X1230P 背面パネル

部位	機能
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN ポート (PoE) (10BASE-T/100BASE-TX/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ドカテゴリ 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。
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。
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。 ・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、製品の設定が初期化され、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。

※ 1 : AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-X5480P の各部名称

DBA-X5480P 前面パネル

DBA-X5480P の前面/パネルには、Power/Cloud LED が配置されています。

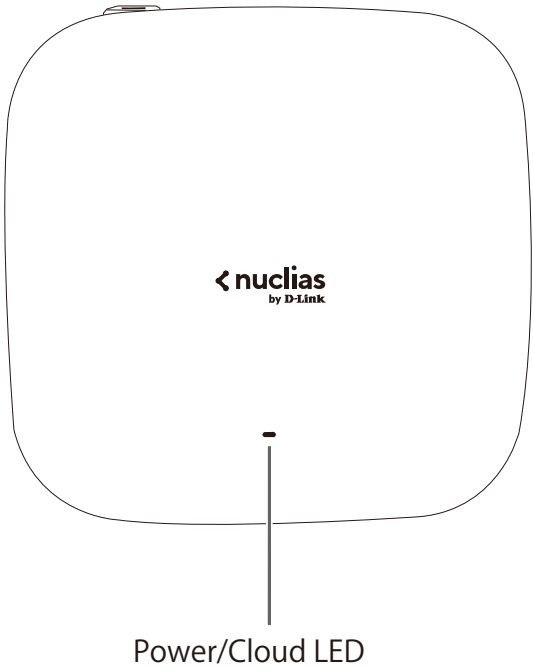


図 2-23 DBA-X5480P 前面パネル

Power/Cloud LED は以下の状態を表示します。

LED 状態	DBA-X5480P 状態
● 緑点灯	Nuclias と正常に接続されており、管理モードで動作している状態です。
● 緑点滅	Nuclias へ接続を試みている状態です。
● 橙点灯	起動中です。
● 橙点滅	初期設定へのリセット中、またはファームウェアのアップグレード中です。
● 赤点灯	正しく動作していません。
● 赤点滅	リカバリモードで動作中です。
● 消灯	電源が入っていません。

第2章 Nuclias用APのご利用にあたって

DBA-X5480P 側面パネル

DBA-X5480P の側面パネルの各部名称について説明します。

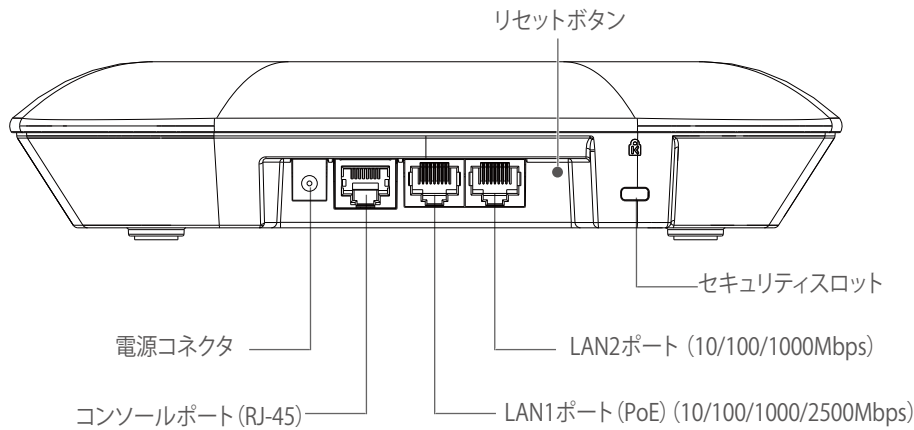


図 2-24 DBA-X5480P 背面パネル

部位	機能
電源コネクタ	AC アダプタ※ ¹ を接続します。
LAN1 ポート (PoE) (10BASE-T/100BASE-TX/ 1000BASE-T/2.5G BASE-T)	RJ-45 コネクタが搭載され、10BASE-T/100BASE-TX/1000BASE-T /2.5G BASE-T イーサネットへの接続が可能です。 また、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 /2.5G BASE-T の場合はエンハンスドカテゴリ 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。
LAN2 ポート (10BASE-T/100BASE-TX/ 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。 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ドカテゴリ 5 以上の UTP/STP ケーブルを接続します。
コンソールポート	コンソールケーブル※ ² を接続します。
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。
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。 - 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、製品の設定が初期化され、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。

※ 1：AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

※ 2：コンソールケーブルは同梱されていません。

注意 DBA-X5480P の LAN(PoE) + LAN は同時利用できません。

第3章 Nuclias 用 AP の設置

- パッケージの内容
- ネットワーク接続前の準備
- Nuclias 用 AP 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。
万一、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、ご購入いただいた販売代理店までご連絡ください。

注意 天井など、人の頭上に落下する可能性がある場所に本製品を設置する場合は、別途落下防止の対策を行ってください。

DBA-1210P の同梱物

- ・ 本体 x 1
- ・ ゴム足 x 4
- ・ AC アダプタ x 1
- ・ イーサネットケーブル x 1
- ・ クイックインストールガイド x 1
- ・ PL シート x 1
- ・ GPL Code Statement x 1
- ・ マウントキット
 - マウントプレート x 1
 - セキュリティ金具 x 1
 - セキュリティ金具カバー x 1
 - セキュリティ金具取り付け用ネジ x 2
 - 壁または天井取り付け用ネジ x 2
 - 壁または天井取り付け用アンカー x 2

DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P の同梱物

- ・ 本体 x 1
- ・ コンソールケーブル (RJ-45/RS-232)※ x 1
- ・ クイックスタートガイド x 1
- ・ PL シート x 1
- ・ GPL Code Statement x 1
- ・ マウントキット
 - マウントプレート x 1
 - 壁または天井取り付け用ネジ x 2
 - 壁または天井取り付け用アンカー x 2
 - 天井クロスバー取り付け用ブラケット x 6 (大中小サイズ各2個ずつ)
 - 天井クロスバー取り付け用ネジ x 2

※ DBA-X5480P にはコンソールケーブルは同梱されていません。

AC アダプタは同梱されていません。本製品を PoE で使用しない場合は、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

DBA-3621P の同梱物

- ・ 本体 x 1
- ・ コンソールケーブル (RJ-45/RS-232) x 1
- ・ アンテナ x 2
- ・ アース線 x 1
- ・ アース線用ネジ x 2
- ・ クイックスタートガイド x 1
- ・ PL シート x 1
- ・ GPL Code Statement x 1
- ・ 柱用マウントキット
 - 柱用マウントベース x 1
 - U ボルト x 2
 - U ボルト固定用ナット x 4
 - マウントベース用ネジ x 4
 - マウントベース用ワッシャー x 4
 - 柱用取付ベルト x 1
- ・ 壁用マウントキット
 - 壁用マウントプレート x 1

第3章 Nuclias用APの設置

- マウントプレート用ネジ x 4
- マウントプレート用ワッシャー x 4
- 壁取り付け用アンカー x 4
- 壁取り付け用ネジ x 4

AC アダプタは同梱されていません。PoE でご利用ください。

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、材質、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、一般的な動作範囲は 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。信号が障害物に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が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-2520P/DBA-2620P/DBA-2720P/DBA-2820P/DBA-X2830P/DBA-X1230P/DBA-X5480P には AC アダプタが付属していません。
PoE でご使用いただくか、別売りの AC アダプタ「PSE-M12V25A-I」をご使用ください。

※ DBA-3621P には AC アダプタが付属していません。PoE でご使用ください。

Nuclias 用 AP の設定・設置

Nuclias と Nuclias 用 AP の接続

Nuclias 用 AP の設定や管理は、インターネットに接続することで Nuclias を経由して行われます。

管理用 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、Nuclias に登録した複数の AP を一度に設定・管理できます。インターネット環境にある Nuclias 用 AP は、Nuclias に自動的に接続し、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 Nuclias 用 AP は通常、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。
ただし、以下のような場合はローカル Web GUI からの設定が必要となります。

- ・ 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
- ・ 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

注意 ローカル Web GUI からは IP アドレスなど、一部の項目のみ設定することができます。
ローカル Web GUI についての詳細は「[第 12 章 Web GUI、CLI からの設定について](#)」を参照してください。

Nuclias を経由した接続例

以下は Nuclias を経由し接続例の図です。

Nuclias 経由で Nuclias 用 AP とコンピュータを接続します。複数の Nuclias 用 AP を一度に設定、管理することができます。

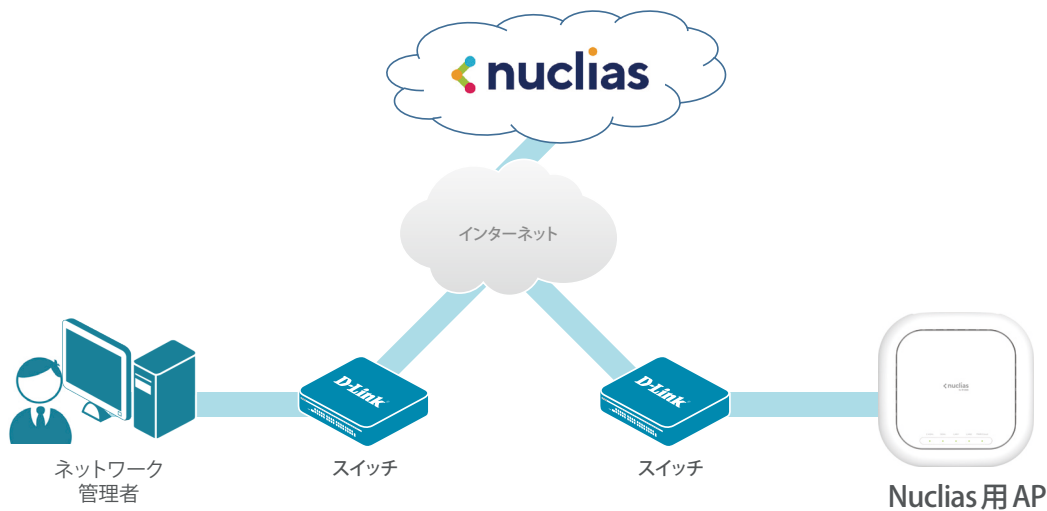


図 3-1 Nuclias を経由した接続例

具体的な接続設定方法については、第 4 章以降の章を参照してください。

第3章 Nuclias用APの設置

■ Nuclias を経由しない接続例

DHCP 環境ではなかったり、事前に VLAN を設定しないとインターネットに接続できないような環境の場合には、以下の方法によりローカル Web GUI へ接続し、Nuclias へ接続する前の事前設定を行うことができます。

(ローカル Web GUI からは IP アドレスなど、一部の項目のみ設定することができます)

● 直接接続

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



図 3-2 直接接続

● ローカルネットワークで接続

Nuclias 用 AP 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。

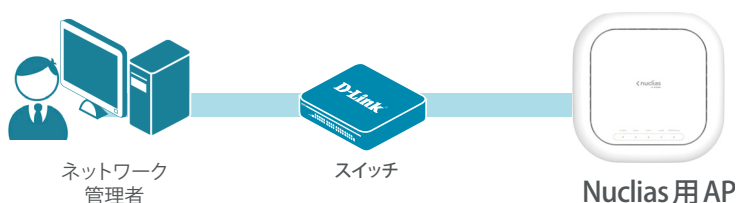


図 3-3 ローカルネットワーク接続

● SSID 「DBA-XXXX-YYYY」 から無線で接続

無線を使用して Nuclias 用 AP に接続します。



図 3-4 無線接続 (SSID)

ローカル Web GUI へのログイン方法

ブラウザのアドレス欄に Nuclias 用 AP のホスト名を入力し、Enter を押下します。

- ・ ホスト名の初期値: 「DBA-XXXX-YYYY」
 - 「XXXX」は、Nuclias 用 AP の製品名です。
お使いの機種を確認し「1210P」「2520P」「2620P」「2720P」「2820P」「3621P」「X2830P」「X1230P」「X5480P」のいずれかを入力してください。
 - 「YYYY」は、Nuclias 用 AP 本体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 ケタです。
DBA-2820P の例: `http://DBA-2820P-YYYY`

ローカル Web GUI の詳細は「[第 12 章 Web GUI、CLI からの設定について](#)」を参照してください。

DBA-1210P の設置

DBA-1210P 本体の設置方法について説明します。

DBA-1210P 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。

- ・ マウントプレート（付属）
- ・ セキュリティ金具と取り付け用ネジ（付属）
- ・ 天井または壁面取り付け用のネジとアンカー（付属）
- ・ ドリル（※壁面に穴をあけるために使用します）
- ・ ドライバー

1. セキュリティ金具を利用する場合、同梱されているネジを使用し、マウントプレートにセキュリティ金具を取り付けます。

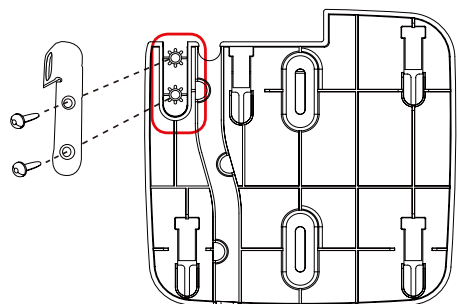


図 3-5 DBA-1210P セキュリティ金具の取り付け

2. 設置する場所（壁もしくは天井）にマウントプレートを合わせ、ネジを差し込む場所にしるしを付けます。

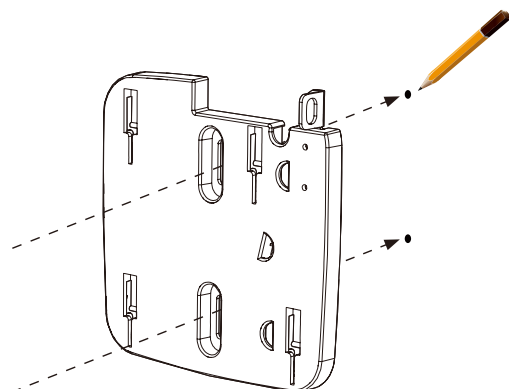


図 3-6 DBA-1210P 位置確認（壁面設置）

3. 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。

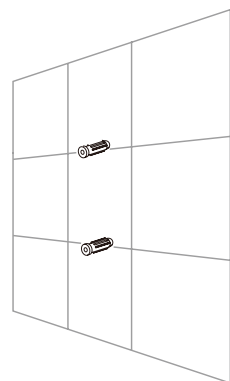


図 3-7 DBA-1210P アンカー挿入

第3章 Nuclias用APの設置

4. アンカーの位置にマウントプレートを合わせ、同梱のネジを使って壁に取り付けます。

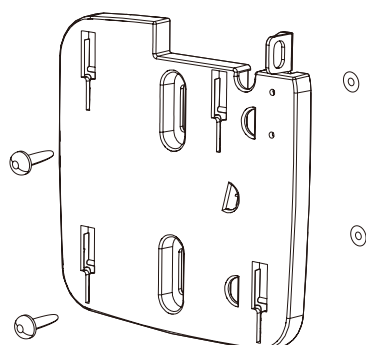


図 3-8 DBA-1210P マウントプレートネジ止め

5. DBA-1210P の LAN ポートにイーサネットケーブルを接続します。
6. DBA-1210P 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-1210P の電源コネクタに AC アダプタを接続します。
7. マウントプレートに DBA-1210P を取り付けます。

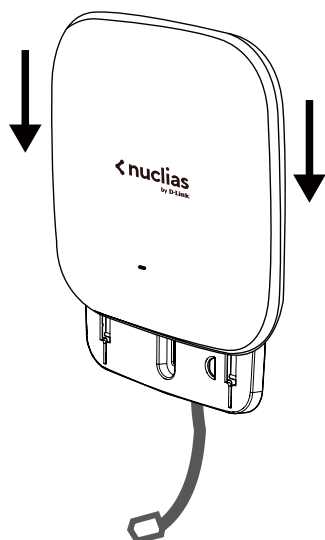


図 3-9 DBA-1210P 機器の設置

DBA-1210P 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場合、背面に同梱のゴム足を取り付けてください。

DBA-1210P のロック

マウントプレートにセキュリティ金具が取り付けられている場合、本体のロックスロットを使用して安全に固定することができます。

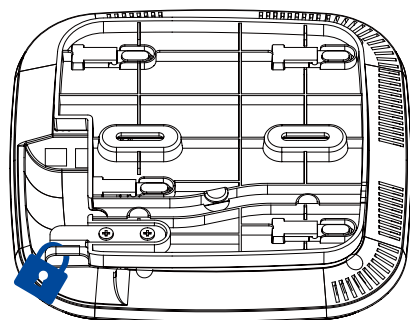


図 3-10 DBA-1210P のロック

DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P の設置

以下の製品について、本体の設置方法を説明します。

- DBA-2520P
- DBA-2620P
- DBA-2720P
- DBA-2820P
- DBA-X2830P
- DBA-X1230P
- DBA-X5480P

本製品を設置するために以下のものをご用意ください。

- マウントプレート（付属）
- 天井または壁面取り付け用のネジとアンカー（付属）
- 天井クロスバー取り付け用のブラケットとネジ（付属）
- ドリル（※壁面に穴をあけるために使用します）
- ドライバー

天井または壁面への設置

1. マウントプレートを使用し、壁または天井のドリルで穴をあける位置にマークを付けます。
2. マークにドリルで穴を開け、付属のアンカーを穴に配置します。
3. マウントプレートをアンカーの上に配置し、付属のネジを使用してマウントプレートを表面に固定します。

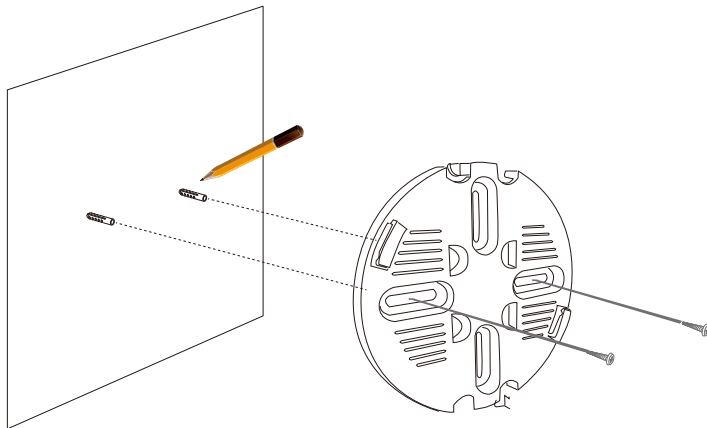


図 3-11 天井または壁面への設置（DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P）

4. イーサネットケーブルを本製品の LAN ポートに接続します。
DBA-2520P/2620P/2720P/2820P/X2830P/X5480P の場合、PoE で使用するには「LAN1（PoE）ポート」を選択してください。
5. 本製品をマウントプレートに取り付け、本製品が所定の位置にロックされるまで時計回りに回します。

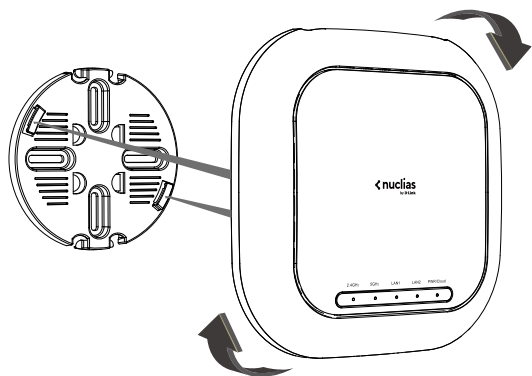


図 3-12 マウントプレートへの取り付け（DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P）

天井クロスバーへの設置

1. 同梱されている天井ブラケットのうち2つを天井クロスバーに取り付けます。
2つのブラケットが互いに直列に配置されていることを確認します。
2. 天井クロスバー取り付け用のネジを使用し、マウントプレートを天井ブラケットに固定します。

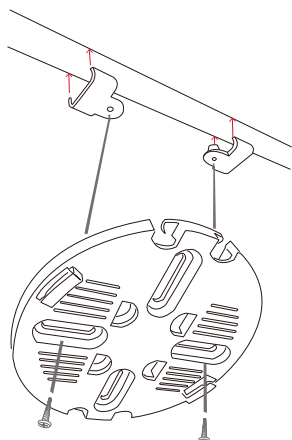


図 3-13 ブラケットとマウントプレートの取り付け (DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P)

3. イーサネットケーブルを本製品の LAN ポートに接続します。
DBA-2520P/2620P/2720P/2820P/X2830P/X5480P の場合、本製品を PoE で使用するには「LAN1 (PoE) ポート」を選択してください。
4. 本製品をマウントプレートに取り付け、本製品が所定の位置にロックされるまで時計回りに回します。

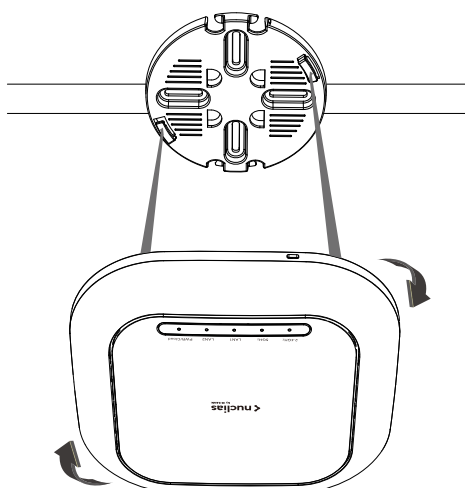


図 3-14 マウントプレートへの取り付け (DBA-2520P/2620P/2720P/2820P/X2830P/X1230P/X5480P)

製品のロック

本体の側面には、セキュリティスロットが搭載されています。
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。

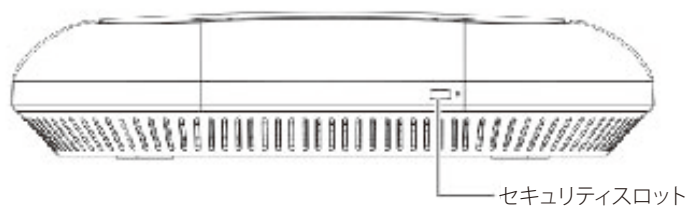


図 3-15 ロック (DBA-2520P/2620P/2720P/2820P/X2830P)

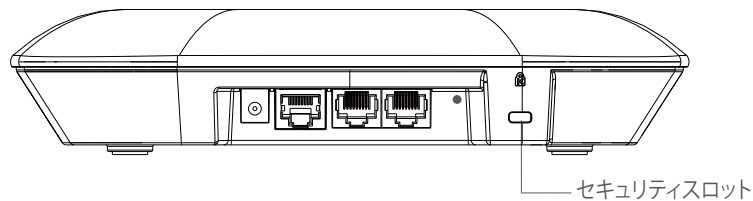


図 3-16 ロック (DBA-X5480P)

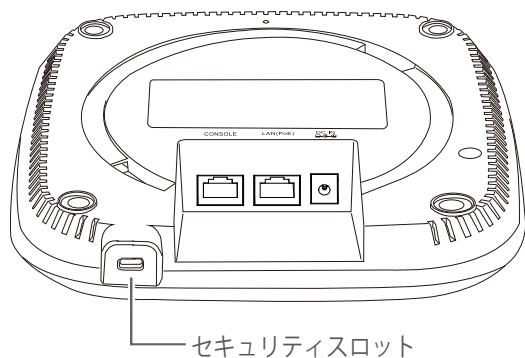


図 3-17 ロック (DBA-X1230P)

DBA-3621P の設置

DBA-3621P 本体の設置方法について説明します。

本製品を設置するために以下のものをご用意ください。

- ・ 柱用マウントキット (付属)
- ・ 壁用マウントキット (付属)
- ・ アース線 (付属) とアース線用ネジ (付属)
- ・ ドリル (※壁面に穴をあけるために使用します)
- ・ ドライバー

防水コネクタの装着

1. イーサネットケーブルに防水コネクタを装着し、DBA-3621P の LAN (PoE) ポートに接続します。
防水コネクタは以下のように装着してください。

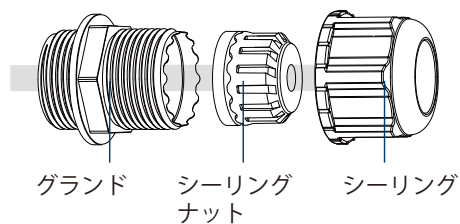


図 3-18 DBA-3621P 防水コネクタ

柱への設置

DBA-3621P を柱へ設置する場合は、以下の手順を参照してください。

注意 U ボルトと柱のサイズが合わない場合は、付属の柱用取付ベルトをご使用ください。

1. 付属の U ボルトとナットを使用し、柱用マウントプレートに柱に固定します。

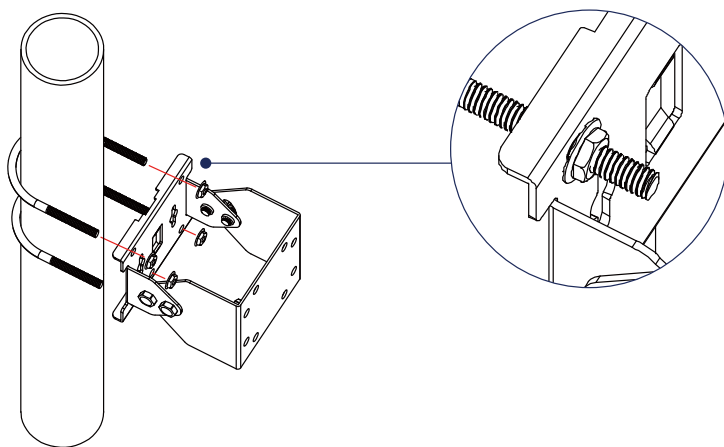


図 3-19 DBA-3621P 柱への設置

2. 付属のネジとワッシャーを使用し、DBA-3621P を柱用マウントプレートに固定します。

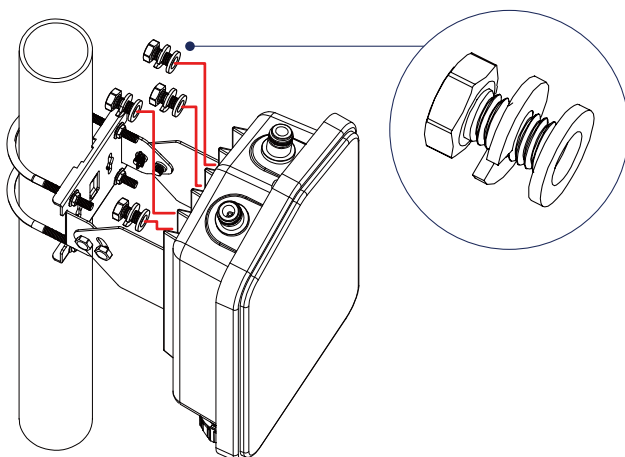


図 3-20 DBA-3621P 柱用マウントプレートへの取り付け

壁への設置

DBA-3621P を壁へ設置する場合は、以下の手順を参照してください。

1. 付属のネジとワッシャーを使用し、DBA-3621P を壁用マウントプレートに固定します。

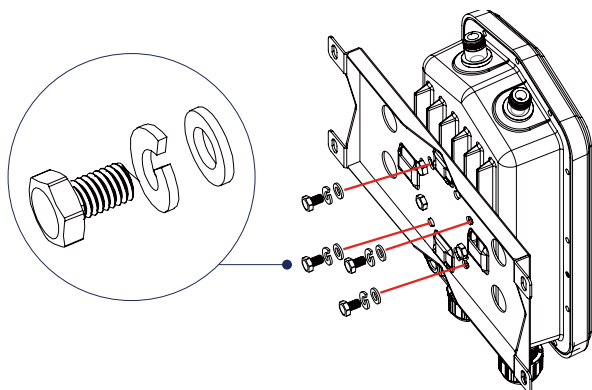


図 3-21 DBA-3621P マウントプレートの取り付け

2. 壁用マウントプレートを取り付ける位置に合わせ、ドリルで穴をあける箇所に印をつけます。
3. 印をつけた位置にドリルで穴をあけ、付属のアンカーを挿入します。
4. 壁用マウントプレートをアンカーの位置に合わせて置き、付属のネジを使用して壁に固定します。

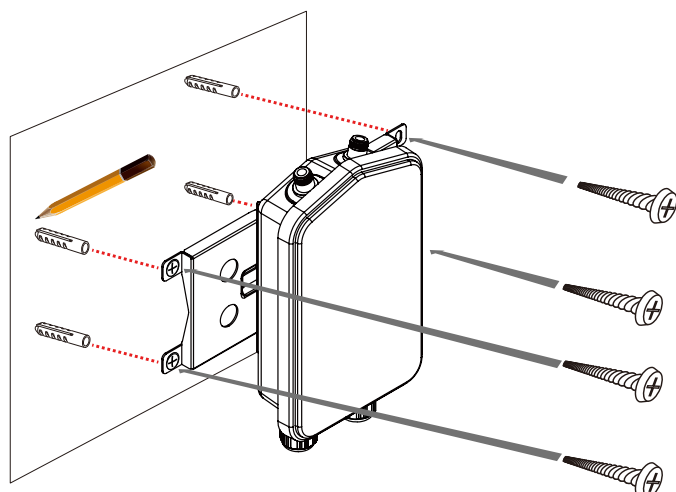


図 3-22 DBA-3621P 壁への取り付け

アース線の接続

DBA-3621P を落雷や静電気から保護するために、アース線を接続します。

1. 付属のネジを使用し、アース線を DBA-3621P に接続します。

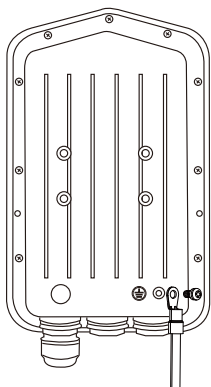


図 3-23 DBA-3621P アース線の接続

2. ドライバーを使用し、アース線がしっかり固定されるようにネジを締めてください。

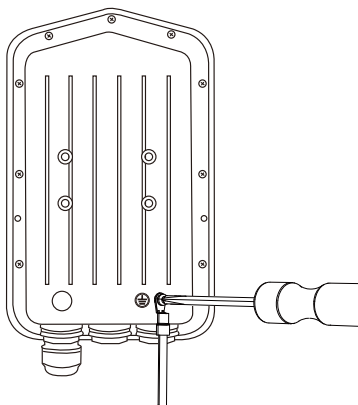


図 3-24 DBA-3621P アース線の固定

3. アース線のもう片方を柱または壁に取り付けます。

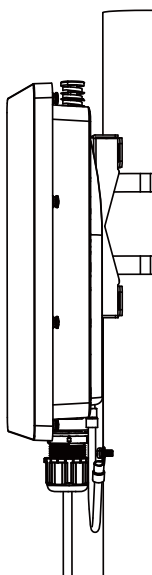


図 3-25 DBA-3621P アース線の取り付け

イーサネットケーブルの接続

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、もう一端をルータ、スイッチ等のネットワーク機器に接続します。

IP アドレスの設定について

Nuclias 用 AP の電源を入ると、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。IP アドレスを自動的に取得できない場合は、Web ベースユーティリティ（Web GUI）を使用して手動で IP アドレスを割り振るなど、必要なネットワーク設定を行う事ができます。

Web GUI の設定方法については「第 12 章 Web GUI、CLI からの設定について」を参照してください。

電源の投入

注意 PoE 受電に対しては電源ボタンによる電源のオン・オフはできません。

DBA-1210P 電源の投入

AC アダプタを使用する場合：

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 給電機器を使用する場合：

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、ステータス LED が点灯します。

DBA-2520P/2620P/2720P/2820P/X2830P 電源の投入

AC アダプタ（PSE-M12V25A-I）を使用する場合：

1. 別売りの AC アダプタ（PSE-M12V25A-I）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/Cloud LED が点灯します。

情報 Power/Cloud LED が点灯しない場合は、電源ボタンを押下してください。

PoE 給電機器を使用する場合：

1. イーサネットケーブルの一端を本製品の背面にある「LAN1 (PoE) ポート」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/Cloud LED が点灯します。

DBA-3621P 電源の投入

情報 AC アダプタは同梱されていません。PoE でお使いください。

1. イーサネットケーブルの一端を本製品の底面にある「LAN (PoE) ポート」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/Cloud LED が点灯します。

DBA-X1230P/X5480P 電源の投入

AC アダプタ（PSE-M12V25A-I）を使用する場合：

1. 別売りの AC アダプタ（PSE-M12V25A-I）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/Cloud LED が点灯します。

PoE 給電機器を使用する場合：

1. イーサネットケーブルの一端を本製品の背面にある「LAN ポート (PoE)」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/Cloud LED が点灯します。

第 4 章 Nuclias の基本設定

- 初期設定手順について
- アカウントと組織の作成
- ログイン
- Nuclias ユーザインタフェースについて
- プロファイルの作成
- Wi-Fi ポリシーの設定
- サイトの作成
- Nuclias 対応機器の登録
- Nuclias 対応機器をオンラインにする

ネットワーク機器や Nuclias をはじめて使用する際の基本的な設置、設定方法について説明します。

まず「Nuclias」へアクセスし、アカウントと組織を作成します。

次に、Nuclias でプロファイルやサイトの設定、Wi-Fi ポリシーの設定等を行い、管理する Nuclias 対応機器を登録します。

最後に Nuclias 対応機器をインターネット並びに Nuclias へと接続し、オンライン状態にします。

初期設定手順について

以下が基本的な初期設定作業のながれです。

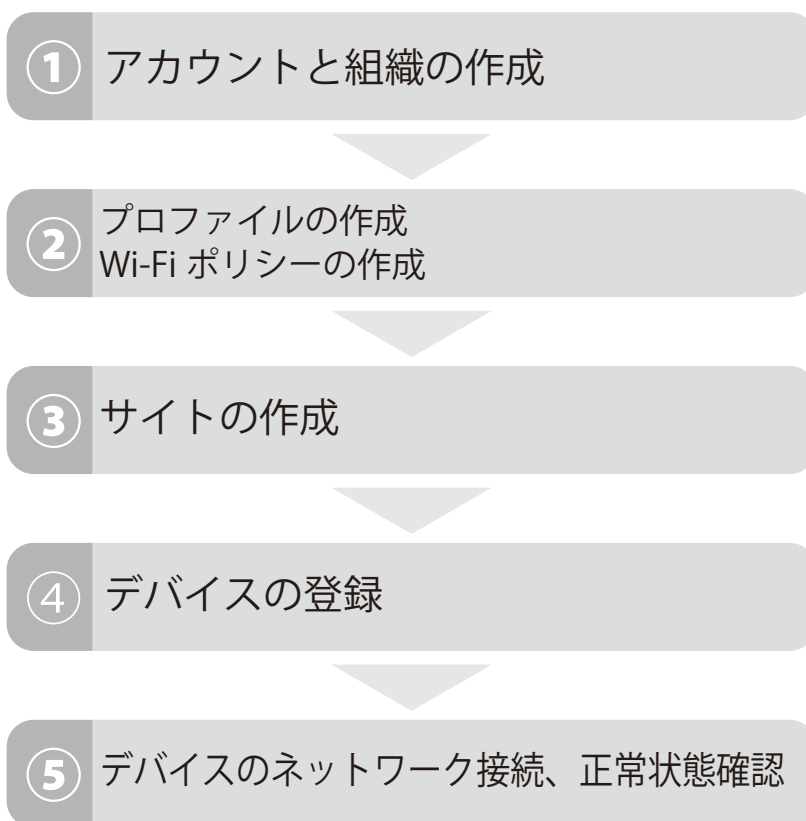


図 4-1 初期設定手順

アカウントと組織の作成

Nuclias アカウントの作成を行います。

「Nuclias」の URL： <https://jp.nuclias.com>



図 4-2 Nuclias サイト

1. Nuclias の URL をブラウザで開き、表示されるページから「アカウントの作成」をクリックします。



図 4-3 ログイン（「アカウントの作成」をクリック）

2. 地域を「Asia」、国を「Japan」に設定します。



図 4-4 国・地域設定

注意 異なる国を設定した場合、デバイスが正常に登録できなくなる可能性があります。

第4章 Nucliasの基本設定

3. アカウントで使用する以下の情報を入力します。
- メールアドレス（ログイン時や、各通知を受け取る際に使用）
 - ユーザ名
 - ログイン用パスワード
 - 作成する組織の名称
 - 住所

注意 1つのアカウントで管理可能な組織は最大1つです。複数の組織の設定を後から統合することはできません。

注意 1つのメールアドレスにつきアカウントは1つとなります。

注意 登録したメールアドレスは変更することができません。

ステップ2
ユーザ、組織、サイトを作成してください。

nuclias

Eメール

フルネーム

パスワード

パスワード

組織名

Japan

Asia/Tokyo(UTC+09:00)

住所

☐ [利用規約](#)と[プライバシーポリシー](#)を読み、同意します。

☐ D-Link製品のアップデートやオファーをメールでお知らせします。

☐ 私は人間です

hCaptcha
プライバシー 保護

アカウントの作成

図 4-5 アカウント情報設定

4. 入力後、「アカウントの作成」をクリックします。

アカウント作成後、登録したメールアドレスへ Nuclias 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 をクリックし、アクティベーションを行ってください。

ログイン

Nuclias のログインについて説明します。

1. ログイン画面を表示します。「Nuclias」の URL : <https://jp.nuclias.com>



図 4-6 ログイン画面

2. アクティベーション済みユーザアカウントのメールアドレス、パスワードを入力します。
3. 「ログイン」をクリック、または Enter キーを押します。
4. Nuclias 管理画面が表示されます。

Nuclias ユーザインタフェースについて

Nuclias 管理画面上部のユーザインタフェースは下記の通りです。

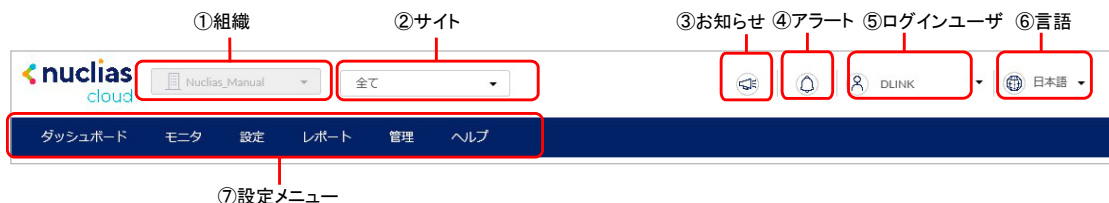


図 4-7 ユーザインタフェース

項目	説明
①組織	現在選択されている組織です。
②サイト	現在選択されているサイト、またはサイトタグです。「全て」は全てのサイトの情報を表示します。ファームウェアアップグレードなど、特定の設定項目を使用する場合はサイトを指定する必要があります。
③お知らせ	ファームウェアのリリース、新機能のサポートなどのお知らせを通知します。お知らせがある場合、アイコンをクリックするとヘルプ > お知らせ画面に移動します。
④アラート	アイコンをクリックするとアラートの詳細を確認できます。
⑤ログインユーザ	現在ログインしているユーザ名が表示されます。ユーザプロフィールの閲覧や変更、ログアウトはここをクリックして実施します。 また、アイコンをクリックすると「Nuclias Connect へのログイン」の項目が表示されます。本項目を選択すると、Nuclias Connect にログインできます。
⑥言語	言語を選択します。
⑦設定メニュー	設定メニューです。各項目の詳細については本マニュアルの 6 章～ 11 章を参照してください。

プロファイルの作成

プロファイルとは、SSID、チャネル設定等、ネットワーク機器へ配信する設定をまとめたものです。

1. 設定 > アクセスポイント > プロファイルの順にクリックします。



図 4-8 プロファイルメニュー

2. 「プロファイルの作成」をクリックします。



図 4-9 プロファイルの作成

3. プロファイルの作成ウィンドウが表示されるので、以下の通りに入力します。



図 4-10 プロファイル作成画面

本画面には以下の項目があります。

項目	説明
① プロファイル名	Nuclias 上で管理するためのプロファイル名を指定します。
② モデル名	プロファイルを適用する機器名（製品名）をプルダウンから指定します。
③ アクセスレベル	アクセスレベルを「組織」「サイトタグ」「サイト」から選択します。 サイトタグおよびサイトを選択した場合は、管理サイトタグまたは管理サイトを設定します。
④ 設定	作成するプロファイルの元データを指定します。 「デフォルトコンフィグを使用する」：各モデルに適応した初期コンフィグがありますので、それらを指定します。管理者はデフォルトコンフィグを編集し、ユーザ環境に合わせた設定を作成できます。 「既存プロファイルを複製する」：同じ組織内に、既に同じモデル用のプロファイルが作成されている場合、それを複製し、編集することができます。

4. 設定後、「プロファイルの作成」をクリックします。

プロファイルの一覧表に作成したプロファイルが表示されます。

#	状態	名前	モデル名	アクセスレベル	デバイス	最終更新日時	プッシュの予定	アクション
1	🟡	DBA-1210P	DBA-1210P	組織	1	2021/11/24 10:47:49	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定
2	🟢	Profile1	DBA-2520P	組織	0	2021/11/24 10:58:38	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定
3	🟢	Profile2	DBA-1210P	組織	0	2021/08/18 10:58:52	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定

図 4-11 プロファイル一覧

Wi-Fi ポリシーの設定

設定 > アクセスポイント > プロファイル画面から Wi-Fi ポリシーの登録、または設定変更を行います。

#	状態	名前	モデル名	アクセスレベル	デバイス	最終更新日時	プッシュの予定	アクション
1	🟢	DBA-2520P	DBA-2520P	組織	0	2020/01/07 11:19:19	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定
2	🟡	DBA-2720P	DBA-2720P	組織	1	2021/07/27 15:39:40	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定
3	🟢	DBA-X1230P	DBA-X1230P	組織	0	2021/04/23 14:13:02	スケジュール未作成	SSID (🔒) 無線 (🔒) 設定

①チェックボックス ②状態 ③名前 ④モデル名 ⑤アクセスレベル ⑥デバイス ⑦最終更新日時 ⑧プッシュの予定 ⑨アクション

図 4-12 プロファイル一覧

項目	説明
①チェックボックス	プロファイルを削除する場合、設定のプッシュを行う場合に使用します。
②状態	プロファイルの同期状態を表示します。 🔴：設定や接続の問題により、同期に失敗しました。プロファイルはデバイスに未同期の状態です。 🟡：プロファイルの設定が変更されました。最新のプロファイルは、紐づけされているデバイスに同期されていません。 🟢：スケジュール設定済みで未同期（実行待ち）の状態です。 🟢：最新のプロファイルがデバイスに同期済みです。または、プロファイルがデバイスに紐づけられていません。
③名前	プロファイル名が表示されています。プロファイルの名称を変更する場合は、直接ここをクリックしてください。
④モデル名	プロファイルのモデルを表示します。
⑤アクセスレベル	プロファイルのアクセスレベルを表示します。
⑥デバイス	プロファイルに登録されているデバイスの数を表示します。 数字をクリックすると、デバイスの一覧が表示されます。
⑦最終更新日時	プロファイルを最後に更新した日時を表示します。
⑧プッシュの予定	プロファイルをデバイスに同期する予定の日時を表示します。 同期を行う予定がない場合は「スケジュール未作成」と表示されます。
⑨アクション	SSID の設定、無線の設定、その他設定のページに移行します。

SSID の情報をカスタマイズする場合は「SSID」をクリックします。

以下のような画面が表示されますので、設定する SSID 名をクリックします。

SSID	2.4 GHz	5 GHz	ブロードキャストSSID	セキュリティ
Nuclias_Guest	☑	☑	☑	Open
Nuclias_Office	☑	☑	☑	WPA + WPA2

図 4-13 SSID 一覧

プロファイルの作成時に「デフォルトコンフィグを使用する」を適用した場合、自動的に「Nuclias_Guest」「Nuclias_Office」の 2 つの SSID が作成されます。

Wi-Fi ポリシーの設定（SSID プロファイル編集）

SSID 名をクリックすると、下記の画面が表示されます。

設定 / アクセスポイント / プロファイル / DBA-1210P / Nuclias_Office

設定のプッシュ

SSID無線設定

基本キャプティブポータルアクセスコントロールスケジュール設定高度な設定

SSID名*
Nuclias_Office

セキュリティ ?
WPA / WPA2

認証方式
PSK

暗号化
AES

事前共有鍵 (PSK) *

グループキー更新間隔*
3600 秒

ブロードキャストSSID
☒ 有効 ☐ 無効

バンド選択 ?
☒ 2.4 GHz ☒ 5 GHz ☐ バンドステアリング

ゲストアクセスモード
☐ 有効 ☒ 無効

NATモード ?
☐ 有効 ☒ 無効

VLAN
☐ 有効 ☒ 無効

SSID内/パーティション
☐ 有効 ☒ 無効

NAS-ID ?
3-48 文字

キャンセル保存

図 4-14 SSID プロファイル編集

本画面には以下の項目があります。

項目	説明						
SSID 名	SSID 名を指定します。無線ネットワークを識別する 1-32 文字の固有の ID です。 注意 ASCII 印字可能文字表（https://ja.wikipedia.org/wiki/ASCII）の『ASCII 印字可能文字』に記載されている文字が使用可能です。特殊文字については下記の制限があります。<table><tr><th>特殊文字</th><th>制限概要</th></tr><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></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。						
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の設定項目については、「 セキュリティモード設定 」を参照してください。						
ブロードキャスト SSID	当該の SSID をブロードキャストする場合、「有効」を選択します。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。本機能を無効にした場合、当該 SSID は無線クライアント側の SSID 一覧に表示されません。						
バンド選択	SSID のバンド（帯域）を選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2820P/DBA-3621P の場合： - 「2.4GHz」「5GHz」 ● DBA-2720P の場合： - 「2.4GHz」「5GHz1」「5GHz2」 ● DBA-X5480P の場合： - 「2.4GHz」「5GHz」「6GHz」 「バンドステアリング」にもチェックを入れると、6GHz > 5GHz > 2.4GHz の順で優先されます。 「6GHz」は、「Enhanced Open」「WPA3」を選択している場合に指定可能です。						

項目	説明
ゲストアクセスモード	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。 ・ 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 宛てのパケットを破棄します。 ・ DHCP サーバ機能 - 10.229.x.x の IP アドレスが帰属端末に割り当てられます。 ・ 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。 ・ NAT モード - 帰属端末からのパケットを機器の管理 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 - 帰属端末同士の通信を遮断します。
NAT モード	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。 ・ DHCP サーバ機能 - 10.229.x.x の IP アドレスが帰属端末に割り当てられます。「DHCP プールの追加」をクリックし、DHCP プールを作成することも可能です。 ・ 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。 ゲストアクセスモードを有効にすると、NAT モードも自動的に有効となります。 ゲストアクセスモードを無効にすると、NAT モードの有効 / 無効を選択できます。NAT モードを有効にした場合は以下の項目が表示されます。 ・ 「DHCP 2.4GHz / 5GHz / 6GHz」（6GHz は DBA-X5480P のみ）：各帯域に対して DHCP プールを選択、または「Auto」（自動）を選択します。 ・ 「DHCP プールの追加」：表示される画面で DHCP プールを追加します。詳細は「DHCP プールの追加」を参照してください。 ・ 「DHCP プールリスト」：DHCP プールリストを表示します。また、追加した DHCP プールを編集および削除できます。 注意 「NAT モード」が有効な SSID がある場合は、Web ベース設定ユーティリティ（Web GUI）で AP の VLAN を設定済みであっても、以下の画面から VLAN の設定を行う必要があります。 設定 > アクセスポイント > プロファイル > 設定 > マネジメント VLAN
VLAN	ネットワークの VLAN を有効にし、「VLAN モード」と「VLAN タグ」を指定します。（「VLAN モード」と「VLAN タグ」は VLAN 有効時のみ表示されます。） 注意 「NAT モード」を有効にした場合、「VLAN」は表示されません。
SSID 内パーティション	有効にした場合、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。
NAS-ID	NAS-ID（ネットワークアクセスサーバ識別子）を入力します。（3-48 文字以内） NAS-ID により、RADIUS サーバはどの AP が要求を送信したかを判別します。 注意 使用可能な文字列は、アルファベット大文字（A-Z）、小文字（a-z）、数字（0 - 9）、ハイフン（-）およびアンダーバー（_）のみで、文字数は 3 文字以上 48 文字以下である必要があります。スペースについても使用できません。また、記号（ハイフンとアンダーバー）については、先頭と末尾には使用できず、連続して同じ記号を使用することもできませんのでご注意ください。 初期値では、SSID 作成時に自動で NAS-ID も初期値として SSID 名と同じものが割り当てられます。ただし、プロファイルページで 2 文字以下の SSID 名を設定した場合は、NAS-ID 欄は空欄になります。また、プロファイル設定の使用を無効にしてデバイスページで SSID を設定した場合に、2 文字以下の SSID 名を設定した場合は、そのデバイスの UID 12 文字が NAS-ID に適用されます。

セキュリティモード設定

セキュリティモード「Enhanced Open」または「Enhanced Open + Open」を選択時	
暗号化	「AES」が自動的に選択されます。

セキュリティモード「WPA2」「WPA/WPA2」「WPA3」「WPA2/WPA3」のいずれかを選択時	
認証方式	認証方式を以下から選択します。 - 「PSK」「SAE」「PSK/SAE」「RADIUS」 選択したセキュリティモードによって表示される項目は異なります。 注意 WPA3 Enterprise 192-bit 暗号化には対応していません。
暗号化	暗号化方式を選択します。「AES」「AES/TKIP」から選択します。 セキュリティモードに「WPA3」を選択している場合は、「AES」が自動的に選択され、変更できません。

第4章 Nucliasの基本設定

セキュリティモード「WPA2」「WPA/WPA2」「WPA3」「WPA2/WPA3」のいずれかを選択時	
事前共有鍵（PSK）	「認証方式」で「PSK」または「SAE」を選択した場合に表示されます。 PSK（Pre-Shared Key/ 事前共有鍵）を以下のルールに従い入力します。 - 入力可能文字数：8-63 文字 - 入力可能な文字：ASCII 印字可能文字表（https://ja.wikipedia.org/wiki/ASCII）の『ASCII 印字可能文字』に記載されている文字 目のアイコンをクリックすると、入力した文字が表示されます。
グループキー更新間隔	グループキーの更新間隔を 3600-84600 秒の範囲で指定します。
プライマリ RADIUS サーバ セカンダリ RADIUS サーバ	「認証方式」で「RADIUS」を選択した場合に表示されます。プルダウンメニューから RADIUS サーバを選択します。 RADIUS サーバの追加 「RADIUS サーバの追加」をクリックし、RADIUS サーバを追加することもできます。追加する場合は以下の項目を入力します。 「サーバ名」「IP アドレス」「ポート」「シークレット」「認証方法」「RADIUS アカウンティング」 注意 RADIUS サーバ設定における「RADIUS アカウンティング」項目は DBS-2000 シリーズではサポートされていません。 注意 RADIUS サーバ設定における「認証方法」項目には以下の制限があります。 - DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 - DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。

入力後、「保存」をクリックします。

DHCP プールの追加

DHCPプールの追加

DHCPプールを有効にする

DHCPプール名*

リースタイム

リースIPレンジ

サブネットマスク

ゲートウェイ*

DNSサーバ

プライマリ*

セカンダリ*

ドメインを検索

キャンセル

保存

図 4-15 DHCP プールの追加

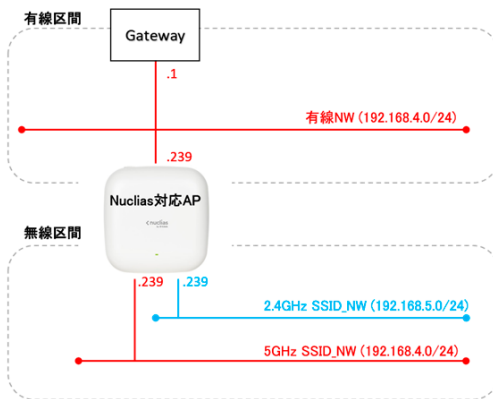
項目	説明
DHCP プールを有効にする	
DHCP プール名	DHCP プール名を入力します。(1-64 文字以内)
リースタイム	IP をリースする期間を設定します。 リース期間が終了すると、クライアントにはプールから新しい IP アドレスが割り当てられます。
リース IP レンジ	
開始 IP	プールの開始 IP アドレスを入力します。開始 IP/ 終了 IP の範囲内の IP アドレスのみがクライアントに割り当てられます。
終了 IP	プールの終了 IP アドレスを入力します。開始 IP/ 終了 IP の範囲内の IP アドレスのみがクライアントに割り当てられます。
サブネットマスク	サブネットマスクを表示します。
ゲートウェイ	ゲートウェイを入力します。
DNS サーバ	
プライマリ	プライマリ DNS サーバを入力します。
セカンダリ	セカンダリ DNS サーバを入力します。
ドメインを検索	DNS 検索ドメインを入力します。

入力後、「保存」をクリックします。

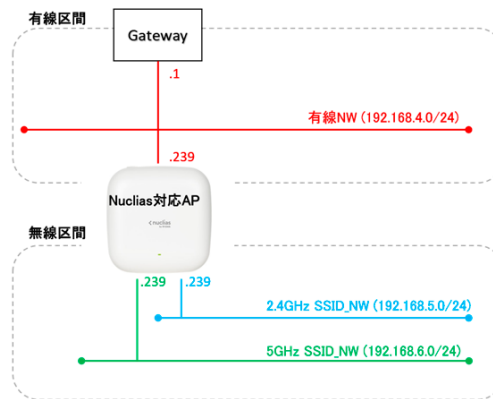
■ DHCP プール設定時の注意事項

DHCP プールを設定する場合、APの有線区間のネットワークアドレスと、無線区間のネットワークアドレスが重複しないように設定してください。有線区間と無線区間でネットワークアドレスが重複していると、NAT（NAPT）機能が正しく動作せず、無線区間から有線区間への通信ができなくなる可能性があります。

NG設定



OK設定



NG 設定の例：有線区間と無線区間（5GHz SSID）のネットワークアドレスが重複しています。

OK 設定の例：有線区間と無線区間のネットワークアドレスが重複していません。

サイトの作成

サイトとは、ネットワーク機器の設置場所（設置先住所）を示したものです。

複数の Nuclias 対応機器が同一施設や同一店舗内等に設置されている場合、それらのログや使用状況などをまとめて確認できます。

また、ファームウェアアップグレードのスケジュール設定等をサイトごとに行うことができます。

1. 管理 > 組織管理の順にクリックします。



図 4-16 組織管理メニュー

2. 「サイトの作成」をクリックします。



図 4-17 組織管理

3. 以下の項目を入力、選択します。
 - 「サイト名」を入力
 - 「国・地域のタイムゾーン」から「Japan」を選択
 その他の項目は特に変更、入力不要です。

サイトの作成

サイト名 *

1-64文字

国・地域のタイムゾーン *

Japan

サイトタグ

None

Asia/Tokyo(UTC+09:00, ...)

住所

デバイス資格情報

デバイス資格情報のユーザー名とパスワードは、ローカルのWebページからログインする際に使用されます。パスワードの長さは8~64文字に設定する必要があります。

ユーザー名

admin

パスワード *

.....

NTP情報

NTPサーバ 1 *

ntp.nuclias.com

NTPサーバ 2

連絡先情報

名前

1-64文字

電話

1-32文字

Eメールアドレス

1-128文字

閉じる

適用

図 4-18 サイトの作成

4. 「適用」をクリックします。

-
- The screenshot shows the Nuclias cloud management interface. The '管理' (Management) menu is open, displaying a list of management options. The option 'デバイスの追加' (Add Device) is highlighted with a red rectangular box. The background dashboard shows status indicators for 'オンライン' (Online), 'オフライン' (Offline), and '警告' (Warning), all showing '0'. The 'ゲートウェイ' (Gateway) status is also shown as '0/0'.

The screenshot shows a 'デバイスの追加' (Add Device) dialog box. It contains the following elements:

- ① デバイスUID**: Points to the 'デバイスUID' field, which has a red asterisk and a tooltip that reads: '登録するデバイスのUIDを入力してください。UID フォーマットは XXXX-XXXX-XXXX または XXXXXXXXXXXXXXXX です。' (Please enter the UID of the device to be registered. The UID format is XXXX-XXXX-XXXX or XXXXXXXXXXXXXXXX).
- ② デバイス名**: Points to the 'デバイス名' field, which has a red asterisk and a tooltip that reads: '1-64文字' (1-64 characters).
- ③ サイト**: Points to the 'サイト' field, which has a red asterisk and a dropdown arrow.
- ④ プロファイル**: Points to the 'プロファイル' field, which has a red asterisk and a dropdown arrow.
- ⑤ ライセンスキー**: Points to the '① 更にライセンスを追加する' button.
- 保存**: Points to the '保存' (Save) button at the bottom right.

項目	説明
①デバイス UID	デバイス UID を入力します。
②デバイス名	Nuclias 上で管理するためのデバイス名を入力します。
③サイト	デバイスに適用するサイトをプルダウンで選択します。
④プロファイル	デバイスに適用するプロファイルをプルダウンで選択します。
⑤ライセンスキー	「更にライセンスを追加する」をクリックし、ライセンスキーを紐づけます。 枠をクリックすると、そのデバイスで使用可能なライセンスキーがプルダウンで表示されますので、選択することができます。 使用可能なライセンスキーとは、デバイスに初期状態で紐づけられているライセンスキー、または既に組織に登録されているライセンスキーです。これらとは異なるライセンスキーを使用する場合は、枠に直接入力してください。 選択可能なライセンスキーが複数ある場合の詳細については、巻末の「付録A ライセンスの適用や開始等に関する詳細」をご確認ください。 注意 デバイスに紐づけられているフリーライセンスは最初にデバイスを登録した組織に保存され、他の組織で使用することはできません。該当デバイスを本組織から削除し、他の組織へ登録し直す場合、別途ライセンスを用意頂く必要があります。

- 59

Nuclias 対応機器をオンラインにする

1. Nuclias 対応機器をインターネット環境に接続します。

Nuclias 対応機器が正常に Nuclias サーバに接続されると、いったんオンライン状態になったあと、ファームウェアの確認並びにアップグレード後、設定プロファイルの確認、更新が実施されます。

注意

機器がオンライン状態になった後はファームウェアアップグレードが実施される可能性があります。

ネットワーク切断や電源 OFF 等を実施する場合は本体の LED 等がファームウェアアップグレード状態でないかをご確認ください。

(例) DBA-2820P の場合、ファームウェアアップグレード中は本体の PWR/Cloud LED が橙色で点滅します。

ファームウェアアップグレード中にネットワーク切断や電源 OFF 等を実施した場合、システムが故障し、Nuclias 対応機器が起動しなくなる恐れがあります。

2. メニューの「ダッシュボード」をクリックし、Nuclias 対応機器がオンラインになったことを確認します。



図 4-21 ダッシュボード画面

以上で Nuclias の基本的な設定は終了です。

設定の詳細に関しては各項目のページをご確認ください。

項目	説明
D-Link からプロモーションと製品のアップデートを受け取る。	チェックを入れた場合、D-Link からプロモーションと製品のアップデートのお知らせを受け取ることができます。
ユーザアイコン	ユーザのアイコン画像が表示されます。 「画像のアップロード」から画像のアップロード、「画像の削除」から画像の削除ができます。
アクセス権限	アカウントのアクセス権限が表示されます。
ページのメール送信	ユーザ情報を自身のアドレスに送信します。
アカウントの削除	自身のアカウントを削除します。 注意 本項目からアカウントを削除するには、管理者権限に設定されている必要があります。

ログイン履歴

ユーザがログインした履歴を確認できます。
Nuclias 管理画面の右上部のユーザ名から「ユーザプロフィール」をクリックし、「最近のログイン」タブをクリックします。

ユーザプロフィール / 最近のログイン

マイプロフィール

最近のログイン

APIアクセス

あなたの最近のログイン

#	IPアドレス	ロケーション	日 / 時
1	125.100.149.234	Shinjuku / Japan	06/15/2020 12:14
2	125.100.149.234	Shinjuku / Japan	06/15/2020 12:09
3	125.100.149.234	Shinjuku / Japan	06/15/2020 11:31
4	125.100.149.234	Shinjuku / Japan	06/12/2020 15:05
5	125.100.149.234	Shinjuku / Japan	06/12/2020 10:31
6	125.100.149.234	Shinjuku / Japan	06/11/2020 16:42
7	125.100.149.234	Shinjuku / Japan	06/11/2020 14:38
8	125.100.149.234	Shinjuku / Japan	06/10/2020 16:46
9	125.100.149.234	Shinjuku / Japan	06/10/2020 14:06
10	125.100.149.234	Shinjuku / Japan	06/09/2020 15:18

前 1 2 次 10 ▼

図 5-2 ログイン履歴

API アクセス

API キーの確認、生成、無効化を実行できます。

Nuclias Cloud API は、他のソフトウェアが Nuclias および Nuclias の管理デバイスと機能を共有するためのインターフェースです。API には、Nuclias Cloud と通信するソフトウェアおよびアプリケーションを構築するエンドポイントが含まれます。プロビジョニング、外部キャプティブポータル、モニタリングやレポートなどの機能を使用する場合に有用です。
Nuclias Cloud API は、URL への HTTPS リクエストと、JSON（JavaScript Object Notation）形式を使用する RESTful API です。

注意 生成した API キーは、無効化できますが削除することはできません。

Nuclias 管理画面の右上部のユーザ名から「ユーザプロフィール」をクリックし、「API アクセス」タブをクリックします。

ユーザプロフィール / API アクセス

マイプロフィール

最近のログイン

APIアクセス

APIアクセス

Nuclias Cloud APIは、ソフトウェアがNuclias CloudプラットフォームおよびNuclias Cloud管理デバイスと直接対話するためのインターフェースです。APIには、プロビジョニング、外部キャプティブポータル、モニタリング、レポートなどのユースケースのためにNuclias Cloudと通信するソフトウェアおよびアプリケーションを構築するためのエンドポイントと呼ばれる一連のツールが含まれています。Nuclias Cloud APIは、URLへのHTTPSリクエストと人が読める形式のJSONを使用するRESTful APIです。専用のドキュメントについてはnuclias.ts.dlinkcore.com/にお問い合わせください。

Nuclias Cloud APIにアクセスするためのBASE URLとして、以下のAPIエンドポイントURLを使用します。

APIエンドポイントURL `https://nuclias.com`

API keyの生成 無効化

#	APIキー名	APIキー	最終アクセスIPアドレス	最終アクセスロケーション	最終アクセス日時	状態	作成者	作成日時
1	123456	9b46*****9a1a	-/-	-/-	2021/11/24 14:08	NORMAL	tsind@1001101+@gmail.com	2021/11/24 14:08

前 1 次 10 ▼

図 5-3 API アクセス

■ API キーの生成

1. 「API key の生成」をクリックし、以下の画面を表示します。

API keyの生成

APIキー名*

1~64文字

新しいAPIキーの作成にはしばらく時間がかかります。

生成

図 5-4 API key の生成

2. API キーの名前を入力→「生成」をクリックします。
3. 以下の画面に結果が表示されます。「ダウンロード API キー」をクリックすると CSV 形式でダウンロードできます。

図 5-5 API キーの生成結果

■ API キーの無効化

1. 無効化する API キーにチェックをいれます。
2. 「無効化」をクリックします
3. 確認画面で「無効化」をクリックします。

図 5-6 API キーの無効化

注意 無効化した API キーを再度有効化することはできません。

第 6 章 ダッシュボード

- ダッシュボード

ダッシュボード

ダッシュボード画面では、Nuclias で管理している機器の状態を確認できます。

組織内全体の使用状況を確認できるほか、サイト単位で状況確認することもできます。
画面上部のドロップダウンリストからサイトを選択してください。

画面右上の  アイコンをクリックすると、ダッシュボード画面に表示する項目をカスタマイズできます。



図 6-1 ダッシュボード（カスタマイズメニュー）

■ ダッシュボードのカスタマイズメニュー

- ・ カスタマイズ: ダッシュボード画面に表示する項目を選択します。
 - 概要: Nuclias に登録されている機器の状態と数を表示します。
 - マップ+アラート+レポート: 地図、アラート、レポートを表示します。
 - 最近 24 時間サマリ: 過去 24 時間のデバイス使用状況の要約を表示します。デバイスは「アクセスポイント」「スイッチ」「ゲートウェイ」から選択できます。
- ・ 位置変更: ダッシュボード画面に表示されている項目を移動します。
- ・ リセット: ダッシュボードの表示を初期状態にリセットします。
- ・ 保存 / 閉じる: ダッシュボードの設定を変更した場合、「保存」をクリックします。設定変更をしていない場合は「閉じる」が表示されます。

ダッシュボード > 概要エリア

指定したサイト内に登録されているデバイスの数とその状態を表示します。



図 6-2 ダッシュボード（概要）

各デバイスの数字をクリックすると、デバイスの詳細が表示されます。
デバイス名のリンクをクリックすると、各デバイスの設定画面に移動します。



図 6-3 ダッシュボード（デバイス）

ダッシュボード>マップ+アラート+レポートエリア

地図、アラート、レポートを表示します。

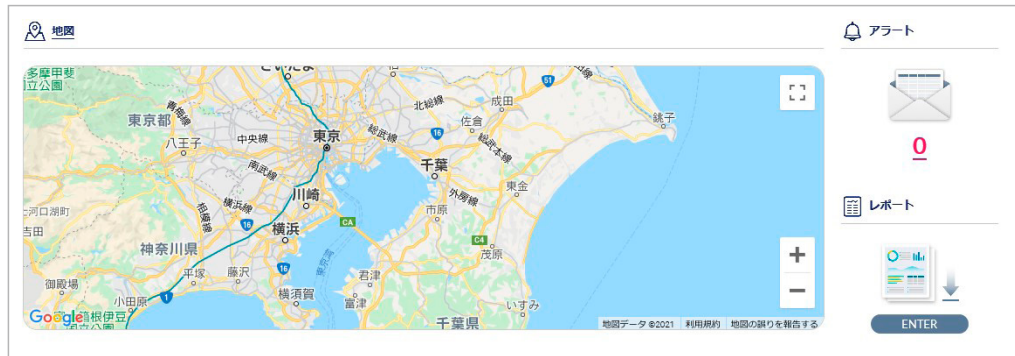


図 6-4 ダッシュボード（マップ+アラート+レポート）

本画面には以下の項目があります。

項目	説明
地図	地図を表示します。 「地図」のリンクをクリックすると、モニタ>地図画面に移動します。
アラート	アラートの数を表示します。 アイコンをクリックすると、レポート>アラート画面に移動します。
レポート	アイコンをクリックすると、レポート>サマリレポート画面に移動します。

ダッシュボード>最近 24 時間サマリ エリア

過去 24 時間のデバイスの使用状況を表示します。



図 6-5 ダッシュボード（最近 24 時間サマリ）

第 7 章 モニタ

- [アクセスポイント-デバイス](#)
- [アクセスポイント-クライアント](#)
- [アクセスポイント-イベントログ](#)
- [地図](#)
- [フロアプラン](#)
- [近隣の AP](#)
- [ネットワーク](#)

アクセスポイント-デバイス

モニタ>アクセスポイント>デバイスの順にクリックし、各デバイスの状況を確認することができます。



図 7-1 デバイス一覧

表の各項目の説明は下記の通りです。

項目	説明
状態	各機器のステータスを以下の色で表示します。 ・ 緑色：オンライン / 赤色：オフライン / 灰色：休止状態
デバイス名	Nuclias 上でのデバイス名を表示します。本項目をクリックすると、各デバイスの設定画面へ移行します。
MAC アドレス	デバイスの MAC アドレスを表示します。
グローバル IP アドレス	デバイスのグローバル IP アドレスを表示します。
ローカル IP アドレス	デバイス本体に割り振られているローカル IP アドレスを表示します。
モデル名	デバイスのモデル名を表示します。
接続	デバイスの直近のステータスをタイムバーで表示します。緑色がオンライン、赤色がオフラインを表します。 タイムバーの期間は「タイムフレーム」で設定できます。ただし、設定したタイムフレームの期間より、該当デバイスのオンライン期間が短かった場合、タイムバーの左端はデバイスが最初にオンラインになったときに調整されます。 マウスカーソルをバーに合わせると、オンラインまたはオフラインとなっていた時間帯を確認できます。
同期ステータス	デバイスに Nuclias 上の最新の設定が同期されているかを表示します。
デバイス UID	デバイスの UID を表示します。
プロファイル	デバイスが紐づいているプロファイルを表示します。
サイト	デバイスが紐づいているサイトを表示します。
サイトタグ	上記のサイトがサイトタグに紐づいている場合、それを表示します。
シリアル番号	デバイスのシリアル番号を表示します。
ファームウェアバージョン	デバイスのファームウェアバージョンを表示します。
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を表示します。
最終閲覧	最終接続日時を表示します。
ライセンス状態	デバイスに紐づけられているライセンスのステータスを表示します。
登録日	デバイスを Nuclias に登録した日を表示します。
期限日	デバイスに紐づけられたライセンスの期限を表示します。
現在のクライアント	現在デバイスに接続しているクライアント数を表示します。
使用量	デバイスが最後に起動してから現在までの総通信量を表示します。
チャンネル	デバイス（AP）に設定されているチャンネルを表示します。「2.4GHz/5GHz/6GHz のチャンネル」が表示されています。 表示される帯域は製品により異なります。
送信電波出力	2.4GHz/5GHz/6GHz の電波出力を表示します。表示される帯域は製品により異なります。
LACP	デバイスの LACP の状態を表示します。

注意 DBA-X5480P は Nuclias Cloud サーバとの接続に IPv6 アドレスを優先して使用、ローカル IP としては IPv4 アドレスを通知します。

■ 表示する期間の変更

「タイムフレーム」で表内の「接続」欄に表示する期間を設定します。

■ 表示する項目の選択

 をクリックすると表示できる項目の一覧が表示されます。表示する項目にチェックをいれます。

■ デバイス情報のダウンロード

 をクリックし、デバイスの情報を CSV 形式でダウンロードします。

アクセスポイント - クライアント

モニタ > アクセスポイント > クライアントの順にクリックし、アクセスポイントに接続されている、または接続されていたクライアントの状態を確認することができます。



図 7-2 クライアント一覧

表の各項目の説明は下記の通りです。

項目	説明
状態	クライアントの状態を表示します。 ・ 緑色：現在接続しているクライアントです。 ・ 赤色：過去に接続していたクライアントです。現在は接続していません。
クライアント名	クライアントの名前を表示します。クライアント名は編集することができます。
MAC アドレス	クライアントの MAC アドレスを表示します。
IPv4 アドレス	クライアントの IP アドレスを表示します。
接続先	クライアントが接続しているデバイス名を表示します。
SSID	クライアントが接続している SSID 名を表示します。
チャンネル	クライアントが接続しているチャンネルを表示します。
RSSI	RSSI (Received Signal Strength Indicator) の値を表示します。 RSSI は、クライアントのデバイスがアクセスポイントから受信する電波の強さを表します。
Wi-Fi 規格	使用している Wi-Fi 規格を表示します。
SNR	SNR (Signal Noise Rate) の値を表示します。SNR は、「受信する電波の強さ (RSSI)」から「受信するノイズの強度」を引いた値です。値が大きいほど電波の品質がよいと判断されます。 注意 本項目は、DBA-2520P、DBA-2620P、DBA-2720P では未サポートです。
使用量	クライアントの通信容量を表示します。
初回確認	クライアントが最初に認識された日時を表示します。
最終閲覧	クライアントが最後に認識された日時を表示します。
ベンダー	クライアントの製造ベンダーを表示します。
キャプティブポータル	キャプティブポータルの状況を確認します。
ユーザ ID	ユーザ ID を表示します。
E メール	キャプティブポータルで使用する E メールアドレスが表示されます。

■ 表示する期間の変更

「タイムフレーム」で表示する期間を設定します。

■ クライアントの検索

検索画面では、以下の項目で検索を行うことができます。

状態:

全て

MAC アドレス:

e.g. 3C:1E:04:16:53:20

接続先:

全て

SSID:

全て

ベンダー:

全て

図 7-3 クライアントの検索

■ 表示する項目の選択

 をクリックすると表示できる項目の一覧が表示されます。表示する項目にチェックをいれます。

■ クライアント情報のダウンロード

 をクリックし、クライアントの情報を CSV 形式でダウンロードします。

アクセスポイント - イベントログ

モニタ>アクセスポイント>イベントログ 画面では、サイト内で発生したイベントを確認できます。
イベントの期間やタイプを選択し、「フィルタ」をクリックするとイベントが表示されます。

開始日

2025/03/06

08:14:08

終了日

2025/03/06

09:14:08

重大性

全て

カテゴリ / イベントタイプ

全て

デバイス

全て

フィルタのリセット

フィルタ

ダウンロード

検索

#	時間	アクセスポイント	サイト	MAC アドレス	重大性	SSID	クライアント	イベントタイプ	イベントの内容
1	03/11/2021 11:53:16	Site_03	Site_03	情報	-	-	-	再起動	アクセスポイントの再詳細: 新ファームウェア
2	03/11/2021 11:50:02	Site_03	Site_03	情報	-	-	-	再起動	アクセスポイントは再
3	03/11/2021 11:50:02	Site_03	Site_03	警告	-	-	-	再起動	アクセスポイントは再詳細: 新しいファームウェア
4	03/11/2021 11:50:02	Site_03	Site_03	情報	-	-	-	ファームウェアアップグレード	ファームウェアアップ

図 7-4 イベントログ

表の各項目の説明は下記の通りです。

項目	説明
時間	イベントの発生日時を表示します。
アクセスポイント	イベントの発生したアクセスポイントを表示します。
サイト	イベントの発生したサイトを表示します。
MAC アドレス	イベントが発生したアクセスポイントの MAC アドレスを表示します。
重大性	イベントの重大性を表示します。
SSID	イベントが発生した SSID を表示します。
クライアント	イベントが発生したクライアントを表示します。
イベントタイプ	イベントのカテゴリとタイプを表示します。
イベントの内容	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、ベンダーなど）を表示します。

■ イベントログのダウンロード

「ダウンロード」をクリックし、デバイスの情報を CSV 形式で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。

■ イベントログのフィルタ

条件を指定して、イベントのリストを絞り込むことができます。
フィルタができる項目は下記の通りです。

項目	説明
開始日	検索範囲の開始日（60 日前から当日までを指定可能）と開始時刻を指定します。
終了日	検索範囲の終了日と終了時刻を指定します。
重大性	イベントの重大性（「重大」「警告」「情報」）を指定します。
カテゴリ / イベントタイプ	発生したイベントの種類を指定します。
デバイス	イベントの発生したデバイスを指定します。

「フィルタ」をクリックすると、設定した条件をもとにイベントログが更新されます。

地図

モニタ > 地図を選択すると、各サイトの情報を地図上で確認できます。

マップ上では、各サイトの設定に紐づけられた住所にプロットが設定されています。

- ・ 緑色：全てのデバイスがオンラインであることを示しています。
- ・ 赤色：1台以上のデバイスがオフラインであることを示しています。
- ・ 灰色：デバイスがサイトに登録されていない、または登録されたデバイスが1週間以上オフライン状態です。

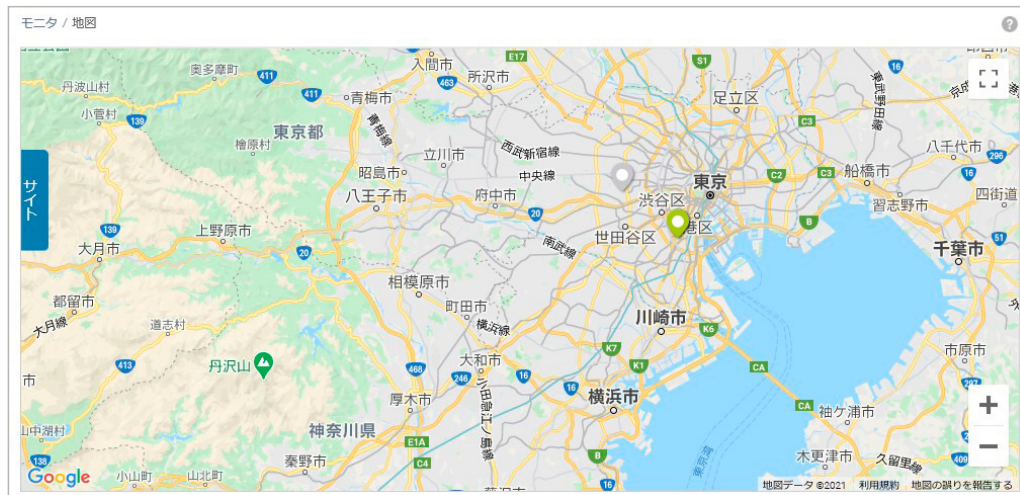


図 7-5 地図

サイトのアイコンをクリックすると、サイト名、住所、並びに各状態のデバイスの数を確認できます。

- ・ 緑：オンライン / 赤：オフライン / 灰色：休止状態（1週間以上オフライン）

サイト名をクリックするとそのサイトのダッシュボードが表示されます。

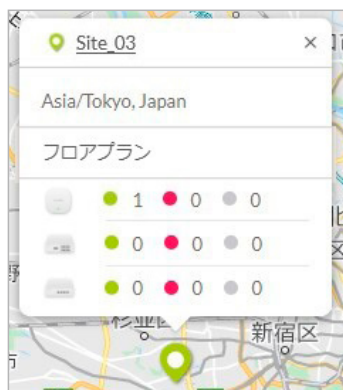


図 7-6 地図 - サイト情報

地図左端の「サイト」のタブをクリックすると、左側にサイトの一覧が表示されます。

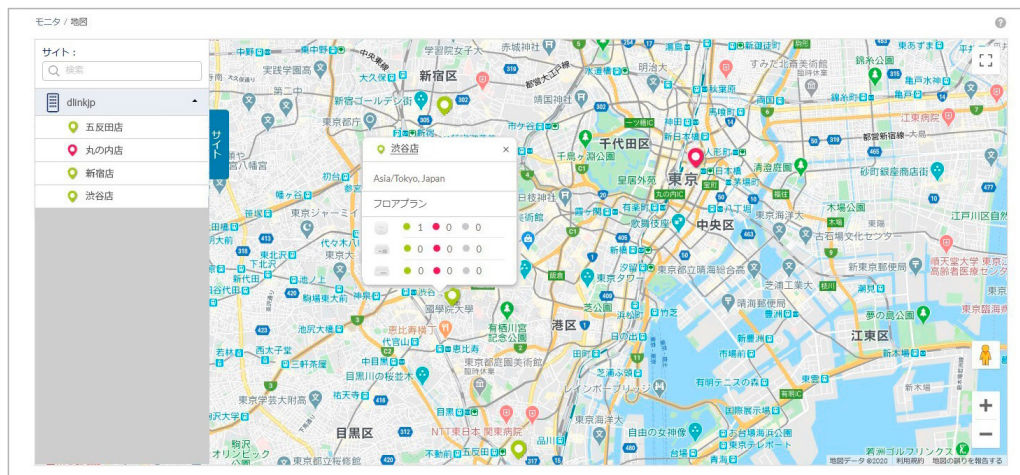


図 7-7 地図 - サイトのリスト

フロアプラン

ユーザが作成、準備したフロア画像を Nuclias にアップロードし、その画像にネットワーク機器のアイコンをドラッグ＆ドロップすることにより、視覚的な機器管理が可能です。フロアプラン上では、各デバイスのオンライン / オフラインの状況を確認できます。

■ フロアプランの追加

1. **モニタ>フロアプラン** を選択します。

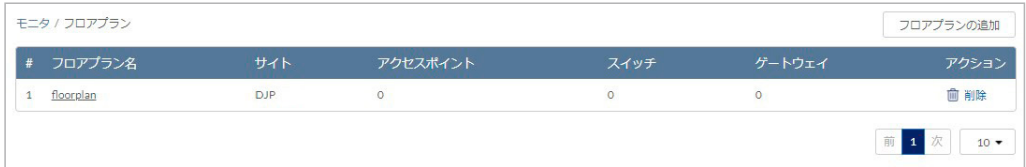


図 7-8 フロアプラン

2. 「フロアプランの追加」をクリックし、フロアプランの名前とサイトを設定します。



図 7-9 フロアプランの追加

3. 「保存」をクリックすると、以下の画面が表示されます。

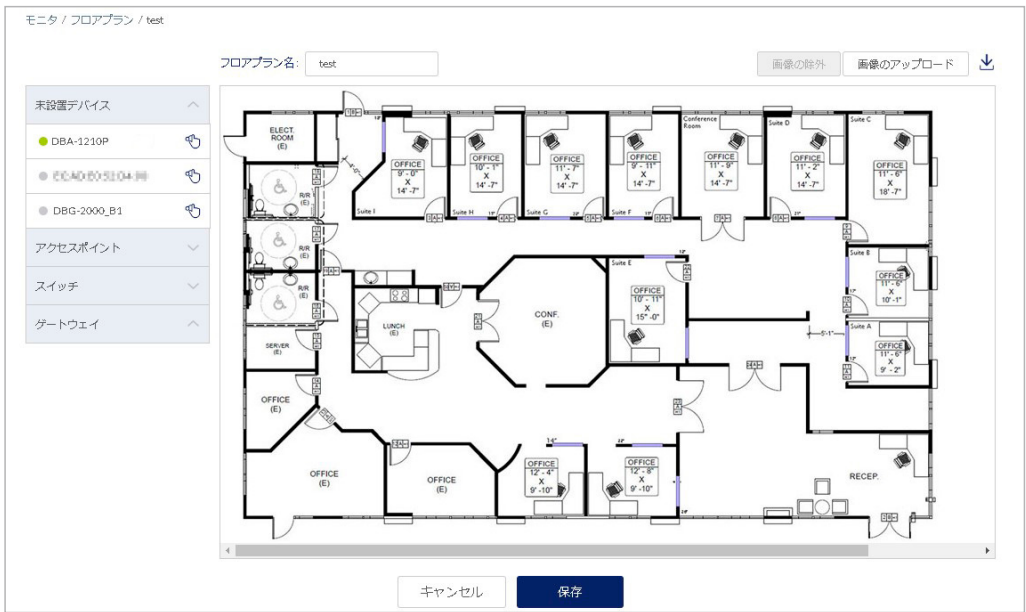


図 7-10 フロアプランの編集

4. フロアマップを編集します。
 - ・フロアマップ等の画像をアップロードする場合は、「画像のアップロード」から実行します。
 - ・アップロードした画像を削除する場合は「画像の除外」をクリックします。
 - ・画面右端の  をクリックすると、画像をダウンロードできます。
 - ・「未設置デバイス」を開くと未設置のデバイスが表示されます。ドラッグして適切な場所に移動させ、ドロップしてアイコンの位置を確定します。
 - ・フロア上のデバイスを削除する場合は左側のデバイスリスト欄の「×」をクリックします。
5. 設定後、「保存」をクリックします。

フロアマップ上のデバイスアイコンの色は以下の状態を表します。

- ・ 緑色：オンライン状態 / 赤色：オフライン状態 / 灰色：休止状態（デバイスが登録済だが、Nuclias に未接続である状態）

■ フロアプランの削除

モニタ>フロアプラン画面で、「アクション」欄の「削除」をクリックします。

近隣の AP

モニタ > 近隣の AP の順にクリックし、近くにあるアクセスポイントを検知し、画面に表示します。

近隣のアクセスポイントを検知する機能は、5 分に 1 回の頻度でアクセスポイントの SSID を検知します。また、検知した SSID の情報を、Nuclias サーバへ報告します。

- ・ 2.4GHz 帯では、現在使用しているチャンネルの± 1 の範囲のチャンネルにおいて、SSID を検知します。(例：8ch で動作 → 7, 8, 9ch で検知)
- ・ 5GHz 帯では、現在使用しているチャンネルの± 4 の範囲のチャンネルにおいて、SSID を検知します。(例：108ch で動作 → 104, 108, 112ch で検知)
- ・ 6GHz 帯では、現在使用しているチャンネルの± 1 の 20MHz の範囲のチャンネルにおいて、SSID を検知します。(例：69ch で動作 → 65, 69, 73ch で検知)

注意 一度検知された SSID は、その後検知されない状態になった場合でも、およそ 60 分間は Nuclias の画面上に表示され続けます。



The screenshot shows a web interface titled 'モニタ / 近隣のAP'. It contains a table with the following columns: #, 状態 (Status), 検知元 (Detected by), MAC, SSID, セキュリティ (Security), RSSI, 無線 (Wireless), チャンネル (Channel), サポートモード (Support mode), and ベンダー (Vendor). The table lists 5 detected APs. The first four are 'UNKNOWN' and the fifth is 'UNKNOWN_ROGUE'. The interface also includes a search bar, a pagination bar showing '1' of 10 items, and a refresh button.

#	状態	検知元	MAC	SSID	セキュリティ	RSSI	無線	チャンネル	サポートモード	ベンダー
1	UNKNOWN	[MAC Address]	[MAC Address]	vjsueinj	WPA2	-87	2.4 GHz	8	b,g,n	
2	UNKNOWN	[MAC Address]	[MAC Address]	vjsueink	WPA2	-86	2.4 GHz	8	b,g,n	
3	UNKNOWN	[MAC Address]	[MAC Address]	ssw-pc-462c83	WPA2	-90	2.4 GHz	10	b,g,n	Covia, Inc.
4	UNKNOWN	[MAC Address]	[MAC Address]	ssw-wep-462c83	WEP	-93	2.4 GHz	10	b,g	Covia, Inc.
5	UNKNOWN_ROGUE	[MAC Address]	[MAC Address]	A4933FA9550A-2G	WPA+WPA2	-51	2.4 GHz	8	b,g,n	HUAWEI TECHNOLOGIE

図 7-11 近隣の AP

表の各項目の説明は下記の通りです。

項目	説明
状態	アクセスポイントの状態を表示します。 ・ 「UNKNOWN_ROGUE」：RSSI 値が 0 ～ - 55 の範囲内にある場合に表示します。 ・ 「UNKNOWN」：RSSI 値が - 55 より低い場合に表示します。
検知元	情報を検知したアクセスポイントを表示します。
MAC	検知したアクセスポイントの MAC アドレスを表示します。
SSID	検知したアクセスポイントの SSID を表示します。
セキュリティ	検知したアクセスポイントのセキュリティを表示します。
RSSI	検知したアクセスポイントの電波強度を表示します。
無線	検知したアクセスポイントの無線周波数帯を表示します。
チャンネル	検知したアクセスポイントのチャンネルを表示します。
サポートモード	検知したアクセスポイントのサポート規格を表示します。
ベンダー	検知したアクセスポイントのベンダーを表示します。

モニタ > ネットワークの順にクリックし、ネットワークの使用状況を表示します。

本画面では、デバイス可用性に関する統計、帯域の使用量、すべての接続クライアントの情報を表示します。無線ネットワークではチャンネル干渉に関する情報も表示されます。ユーザのアクセス権限に応じて、管理対象のデバイスのみが表示されます。

モニタ / ネットワーク

デバイス稼働時間の可用性

タイムフレーム: 最近24時間

検索

↓

#	デバイス名	オフライン/稼働時間	利用可能状態
1	DBA-1210P	0s / 1d 0h 0m 0s	100 %
2	DBG-2000_B1	1d 0h 0m 0s / 0s	0 %
3	DBG-2000_B1	1d 0h 0m 0s / 0s	0 %

前

1

次

10

使用帯域

タイムフレーム: 最近24時間

検索

↓

#	サイト名	使用量
データがありません		

前

次

10

クライアントオーバービュー

タイムフレーム: 最近24時間

検索

↓

#	タイプ	クライアント名	サイト	MAC アドレス	IPv4アドレス	接続先	使用量	RSSI	SNR
データがありません									

前

次

10

チャンネルオーバービュー

デバイス: 全て

↓

#	チャンネル	干渉	使用
1	8	11	
2	9	12	DBA-1210P
3	10	11	
4	56	8	
5	60	5	DBA-1210P
6	64	11	

前

1

次

10

図 7-12 ネットワーク

■ デバイス稼働時間の可用性

本画面には以下の項目が含まれます。

項目	説明
デバイス名	デバイス名を表示します。
オフライン / 稼働時間	「タイムフレーム」で指定した期間のオフライン時間 / 稼働時間を表示します。
利用可能状態	「タイムフレーム」で指定した期間でデバイスが稼働している時間のパーセンテージを表示します。

 をクリックすると、表示している情報を CSV 形式でダウンロードできます。

特定の文字列を含むログを検索する場合は、検索ウィンドウに文字を入力します。検索ウィンドウ右側の  をクリックしてサイトを指定し、特定のサイトに属するデバイスを表示することもできます。

■ 使用帯域

本画面には以下の項目が含まれます。

項目	説明
サイト名	サイト名を表示します。
使用量	「タイムフレーム」で指定した期間のインターネット帯域の合計使用量を表示します。

 をクリックすると、表示している情報を CSV 形式でダウンロードできます。

特定の文字列を含むログを検索する場合は、検索ウィンドウに文字を入力します。検索ウィンドウ右側の  をクリックして、特定のサイトを指定、表示することもできます。

72

■ クライアントオーバービュー

本画面には以下の項目が含まれます。

項目	説明
タイプ	クライアントの接続タイプ（無線または有線）をアイコンで表示します。
クライアント名	「タイムフレーム」で指定した期間に接続されたクライアント名を表示します。
サイト	サイト名を表示します。
MAC アドレス	クライアントの MAC アドレスを表示します。
IPv4 アドレス	クライアントの IP アドレスを表示します。
接続先	クライアントの接続先デバイスを表示します。
使用量	インターネット帯域の使用量を表示します。
RSSI	無線接続の場合は、RSSI（Received Signal Strength Indicator）の値を表示します。RSSI は、クライアントが受信する電波の強さを表します。
SNR	無線接続の場合は、SNR (Signal Noise Rate) の値を表示します。SNR は、「受信する電波の強さ（RSSI）」から「受信するノイズの強度」を引いた値です。値が大きいほど電波の品質はよいと判断されます。



をクリックすると、表示している情報を CSV 形式でダウンロードできます。

特定の文字列を含むログを検索する場合は、検索ウィンドウに文字を入力します。検索ウィンドウ右側の▼をクリックして、特定のサイトを指定、表示することもできます。

■ チャネルオーバービュー

本画面には以下の項目が含まれます。

項目	説明
チャネル	干渉を検出したチャネルを表示します。
干渉	このチャネルで動作している Nuclias 管理対象外の無線ネットワーク（SSID）を表示します。
使用	このチャネルを使用している Nuclias デバイスを表示します。



をクリックすると、表示している情報を CSV 形式でダウンロードできます。



をクリックして特定のデバイスを指定、表示することができます。

第 8 章 デバイス設定

- アクセスポイント - プロファイル
- アクセスポイント - デバイス
- アクセスポイント - IP ACL
- 認証 - 認証サーバ
- 認証 - ローカル認証 DB
- MAC ACL
- ウォールドガーデン
- スケジュールポリシー
- スプラッシュページ

アクセスポイント - プロファイル

設定 > アクセスポイント > プロファイルを選択し、アクセスポイントに適用するための Wi-Fi ポリシーを記載したプロファイルを作成、編集するページを表示します。



図 8-1 プロファイル一覧

本画面には以下の項目があります。

項目	説明
チェックボックス	プロファイルを削除する場合、設定のプッシュを行う場合に使用します。
状態	プロファイルの同期状態を表示します。 ：設定や接続の問題により、同期に失敗しました。プロファイルはデバイスに未同期の状態です。 ：プロファイルの設定が変更されました。最新のプロファイルは、紐づけされているデバイスに同期されていません。 ：スケジュール設定済みで未同期（実行待ち）の状態です。 ：最新のプロファイルがデバイスに同期済みです。または、プロファイルがデバイスに紐づけられていません。
名前	プロファイル名が表示されています。プロファイルの名称を変更する場合は、直接ここをクリックしてください。
モデル名	プロファイルのモデルを表示します。
アクセスレベル	プロファイルのアクセスレベルを表示します。
デバイス	プロファイルに登録されているデバイスの数を表示します。 数字をクリックすると、デバイスの一覧が表示されます。
最終更新日時	プロファイルを最後に更新した日時を表示します。
プッシュの予定	プロファイルをデバイスに同期する予定の日時を表示します。 同期を行う予定がない場合は「スケジュール未作成」と表示されます。
アクション	以下の項目をクリックし、プロファイルの設定を行います。 「SSID」：SSID 設定を行う画面に移行します。詳細は「プロファイル - SSID」を参照してください。 「無線」：無線設定を行う画面に移行します。詳細は「プロファイル - 無線」を参照してください。 「設定」：プロキシ、IPv6、ファストローミング、マネジメント VLAN の設定画面に移行します。詳細は「プロファイル - 設定」を参照してください。

なお、画面右上の検索ウィンドウより、サイトタグやサイトを指定してプロファイルを表示することもできます。

注意 サイトまたはサイトタグを指定して検索した場合、指定したサイトまたはサイトタグ配下のプロファイルのみ検索結果に表示されます。

■ プロファイルの作成

1. 設定>アクセスポイント>プロファイル画面の「プロファイルの作成」をクリックし、以下の画面で設定を行います。

図 8-2 プロファイルの作成

本画面には以下の項目があります。

項目	説明
プロファイル名	Nuclias 上で管理するためのプロファイル名を指定します。
モデル名	プロファイルを適用する機器名（製品名）をプルダウンから選択します。
アクセスレベル	アクセスレベルを「組織」「サイトタグ」「サイト」から選択します。 サイトタグおよびサイトを選択した場合は、管理サイトタグまたは管理サイトを設定します。
設定	作成するプロファイルの元データを指定します。 「デフォルトコンフィグを使用する」：各モデルに適応した初期コンフィグがありますので、それらを指定します。管理者はデフォルトコンフィグを編集し、ユーザ環境に合わせた設定を作成できます。 「既存プロファイルを複製する」：同じ組織内に、既に同じモデル用のプロファイルが作成されている場合、それを複製し、編集することができます。

2. 設定後、「プロファイルの作成」をクリックします。

■ プロファイルの削除

1. 設定>アクセスポイント>プロファイル画面のチェックボックスにチェックを入れ、「プロファイルの削除」をクリックします。
2. 確認画面で「はい」を選択します。

注意 デバイスが紐づいているプロファイルは削除できません。

■ 設定のプッシュ

プロファイルをデバイスに同期するには、「設定のプッシュ」を行います。

1. 設定>アクセスポイント>プロファイル画面のチェックボックスにチェックを入れ、「設定のプッシュ」をクリックします。
2. 以下の画面で設定のプッシュを実行する方法を選択します。

図 8-3 設定のプッシュ

「今すぐ設定のプッシュ」：すぐに設定のプッシュを行います。

「設定のプッシュの時間を設定してください」：設定のプッシュを実行する日時を選択します。

3. 「スケジュール変更」をクリックします。
4. 設定>アクセスポイント>プロファイル画面の「プッシュの予定」に、設定のプッシュを行う日時が表示されます。

注意 オフライン状態のデバイスに「設定のプッシュ」を行った場合は、プロファイルを同期できません。

注意 プロファイルの「SSID」「無線」「設定」タブの各画面からも「設定のプッシュ」を実行できます。
最新のプロファイルがデバイスに適用されていない場合、「設定のプッシュ」アイコンには橙色のマークが表示されます。



■ プロファイル SSID の一覧

設定 > アクセスポイント > プロファイル画面で「アクション」欄の「SSID」をクリックすると、SSID の一覧が表示されます。



図 8-4 SSID 一覧

本画面には以下の項目があります。

項目	説明
SSID	SSID 名を表示します。クリックすると設定画面へ移行します。
2.4GHz	当該 SSID を 2.4GHz 帯で有効化する場合はチェックを入れます。デバイスにより、同時に有効化できる SSID 数の上限は決まっています。
5GHz	当該 SSID を 5GHz 帯で有効化する場合はチェックを入れます。デバイスにより、同時に有効化できる SSID 数の上限は決まっています。 DBA-2720P のプロファイルの場合は「5 GHz 1」と「5 GHz 2」が表示されます。
6GHz (DBA-X5480P)	当該 SSID を 6GHz 帯で有効化する場合はチェックを入れます。
ブロードキャスト SSID	当該 SSID をブロードキャストする場合はチェックを入れます。ステルス状態にする場合はチェックを外します。
セキュリティ	SSID のセキュリティを表示します。セキュリティは SSID の設定で変更できます。

プロファイル - SSID

SSID の追加方法と設定方法について説明します。

■ プロファイル SSID の追加

1. 設定 > アクセスポイント > プロファイル画面で「アクション」欄の「SSID」をクリックします。
2. 「SSID の追加」をクリックします。



図 8-5 SSID 一覧

3. SSID 名を入力し、「バンド選択」で使用する帯域を選択します。



図 8-6 SSID 一覧

4. 「保存」をクリックします。

■ プロファイル SSID の編集

1. 設定 > アクセスポイント > プロファイル画面で「アクション」欄の「SSID」をクリックします。
2. 設定を行う SSID のリンクをクリックします。

設定 / アクセスポイント / プロファイル / DBA-2820P / SSID

設定のプッシュ ?

SSID

SSIDの追加 削除

SSID	2.4 GHz	5 GHz	ブロードキャストSSID	セキュリティ
☐ Nucias_Guest	☒	☒	☒	Open
☐ Nucias_Office	☒	☒	☒	WPA + WPA2

前 1 次 10 ▼

図 8-7 SSID 一覧

3. 以下のタブについて設定を行います。
 - 基本：詳細は「[プロファイル - SSID - 基本タブ](#)」を参照してください。
 - キャプティブポータル：詳細は「[プロファイル - SSID - キャプティブポータルタブ](#)」を参照してください。
 - アクセスコントロール：詳細は「[プロファイル - SSID - アクセスコントロールタブ](#)」を参照してください。
 - スケジュール設定：詳細は「[プロファイル - SSID - スケジュール設定タブ](#)」を参照してください。
 - 高度な設定：詳細は「[プロファイル - SSID - 高度な設定タブ](#)」を参照してください。

設定 / アクセスポイント / プロファイル / DBA-2820P / Nucias_Office

設定のプッシュ

SSID

無線 設定

基本 キャプティブポータル アクセスコントロール スケジュール設定 高度な設定

SSID名* [Nucias_Office](#)

セキュリティ ? WPA / WPA2 ▼

図 8-8 SSID 設定画面

プロファイル - SSID - 基本タブ

「基本」タブを選択すると以下の画面が表示されます。

設定 / アクセスポイント / プロファイル / Profile1 / Nuclias_Office

設定のプッシュ ?

SSID

無線

設定

基本

キャプティブータル

アクセスコントロール

スケジュール設定

高度な設定

SSID名*

Nuclias_Office

セキュリティ ?

WPA / WPA2

認証方式

PSK

暗号化

AES

事前共有鍵 (PSK) *

.....

グループキー更新間隔*

3600

秒

ブロードキャストSSID

☒ 有効 ☐ 無効

バンド選択

☒ 2.4 GHz ☒ 5 GHz ☐ バンドステアリング

ゲストアクセスモード

☐ 有効 ☒ 無効

NATモード ?

☐ 有効 ☒ 無効

VLAN

☐ 有効 ☒ 無効

SSID内バージョン

☐ 有効 ☒ 無効

NAS-ID ?

Nuclias_Office

キャンセル

保存

図 8-9 プロファイル - SSID - 基本タブ

本画面には以下の項目があります。

項目	説明						
SSID 名	SSID 名を指定します。無線ネットワークを識別する 1-32 文字の固有の ID です。 注意 ASCII 印字可能文字表 (https://ja.wikipedia.org/wiki/ASCII) の『ASCII 印字可能文字』に記載されている文字が使用可能です。特殊文字については下記の制限があります。<table><tr><th>特殊文字</th><th>制限概要</th></tr><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></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。						
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の設定項目については、「 セキュリティモード設定 」を参照してください。						
ブロードキャスト SSID	当該の SSID をブロードキャストする場合、「有効」を選択します。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。本機能を無効にした場合、当該 SSID は無線クライアント側の SSID 一覧に表示されません。						
バンド選択	SSID のバンド（帯域）を選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2820P/DBA-3621P の場合： - 「2.4GHz」 「5GHz」 ● DBA-2720P の場合： - 「2.4GHz」 「5GHz1」 「5GHz2」 ● DBA-X5480P の場合： - 「2.4GHz」 「5GHz」 「6GHz」 「バンドステアリング」にもチェックを入れると、6GHz > 5GHz > 2.4GHz の順で優先されます。「6GHz」は、「Enhanced Open」「WPA3」を選択している場合に指定可能です。						

項目	説明
ゲストアクセスモード	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。 ・ 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 宛てのパケットを破棄します。 ・ DHCP サーバ機能：10.229.x.x の IP アドレスが帰属端末に割り当てられます。 ・ 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。 ・ NAT モード：帰属端末からのパケットを機器の管理 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：帰属端末同士の通信を遮断します。
NAT モード	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。 ・ DHCP サーバ機能 - 10.229.x.x の IP アドレスが帰属端末に割り当てられます。「DHCP プールの追加」をクリックし、DHCP プールを作成することも可能です。 ・ 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。 ゲストアクセスモードを有効にすると、NAT モードも自動的に有効となります。 ゲストアクセスモードを無効にすると、NAT モードの有効 / 無効を選択できます。NAT モードを有効にした場合は以下の項目が表示されます。 ・ 「DHCP 2.4GHz / 5GHz / 6GHz」（6GHz は DBA-X5480P のみ）：各帯域に対して DHCP プールを選択、または「Auto」（自動）を選択します。 ・ 「DHCP プールの追加」：表示される画面で DHCP プールを追加します。詳細は「DHCP プールの追加」を参照してください。 ・ 「DHCP プールリスト」：DHCP プールリストを表示します。また、追加した DHCP プールを編集及び削除できます。 注意 「NAT モード」が有効な SSID がある場合は、Web ベース設定ユーティリティ（Web GUI）で AP の VLAN を設定済みであっても、以下の画面から VLAN の設定を行う必要があります。 設定 > アクセスポイント > プロファイル > 設定 > マネジメント VLAN
VLAN	ネットワークの VLAN を有効にし、「VLAN モード」と「VLAN タグ」を指定します。 （「VLAN モード」と「VLAN タグ」は VLAN 有効時のみ表示されます。） 注意 「NAT モード」を有効にした場合、「VLAN」は表示されません。
SSID 内パーティション	有効にした場合、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。
NAS-ID	NAS-ID（ネットワークアクセスサーバ識別子）を入力します。（3-48 文字以内） NAS-ID により、RADIUS サーバはどの AP が要求を送信したかを判別します。

セキュリティモード設定

セキュリティモード「Enhanced Open」または「Enhanced Open + Open」を選択時	
暗号化	「AES」が自動的に選択されます。

セキュリティモード「WPA2」「WPA/WPA2」「WPA3」「WPA2/WPA3」のいずれかを選択時	
認証方式	認証方式を以下から選択します。 - 「PSK」「SAE」「PSK/SAE」「RADIUS」 選択したセキュリティモードによって表示される項目は異なります。 注意 WPA3 Enterprise 192-bit 暗号化には対応していません。
暗号化	暗号化方式を選択します。「AES」「AES/TKIP」から選択します。 セキュリティモードに「WPA3」を選択している場合は、「AES」が自動的に選択され、変更できません。
事前共有鍵（PSK）	「認証方式」で「PSK」または「SAE」を選択した場合に表示されます。 PSK（Pre-Shared Key/ 事前共有鍵）を以下のルールに従い入力します。 ・ 入力可能文字数：8-63 文字 ・ 入力可能な文字：ASCII 印字可能文字表（https://ja.wikipedia.org/wiki/ASCII）の『ASCII 印字可能文字』に記載されている文字 目のアイコンをクリックすると、入力した文字が表示されます。
グループキー更新間隔	グループキーの更新間隔を 3600-84600 秒の範囲で指定します。

セキュリティモード「WPA2」「WPA/WPA2」「WPA3」「WPA2/WPA3」のいずれかを選択時	
プライマリ RADIUS サーバ セカンダリ RADIUS サーバ	「認証方式」で「RADIUS」を選択した場合に表示されます。プルダウンメニューから RADIUS サーバを選択します。 RADIUS サーバの追加 「RADIUS サーバの追加」をクリックし、RADIUS サーバを追加することもできます。追加する場合は以下の項目を入力します。 - 「サーバ名」「IP アドレス」「ポート」「シークレット」「認証方法」「RADIUS アカウンティング」 注意 RADIUS サーバ設定における「認証方法」項目には以下の制限があります。 ・DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 ・DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。

入力後、「保存」をクリックします。

DHCP プールの追加

DHCPプールの追加

DHCPプールを有効にする

DHCPプール名*

リースタイム

リースIPレンジ

サブネットマスク

ゲートウェイ*

DNSサーバ

プライマリ*

セカンダリ*

ドメインを検索

キャンセル

保存

図 8-10 DHCP プールの追加

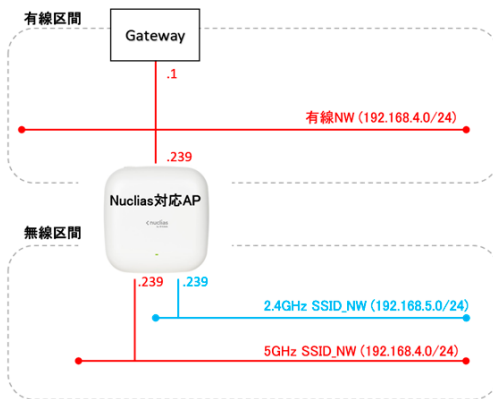
項目	説明
DHCP プールを有効にする	
DHCP プール名	DHCP プール名を入力します。(1-64 文字以内)
リースタイム	IP をリースする期間を設定します。 リース期間が終了すると、クライアントにはプールから新しい IP アドレスが割り当てられます。
リース IP レンジ	
開始 IP	プールの開始 IP アドレスを入力します。開始 IP/ 終了 IP の範囲内の IP アドレスのみがクライアントに割り当てられます。
終了 IP	プールの終了 IP アドレスを入力します。開始 IP/ 終了 IP の範囲内の IP アドレスのみがクライアントに割り当てられます。
サブネットマスク	サブネットマスクを表示します。
ゲートウェイ	ゲートウェイを入力します。
DNS サーバ	
プライマリ	プライマリ DNS サーバを入力します。
セカンダリ	セカンダリ DNS サーバを入力します。
ドメインを検索	DNS 検索ドメインを入力します。

入力後、「保存」をクリックします。

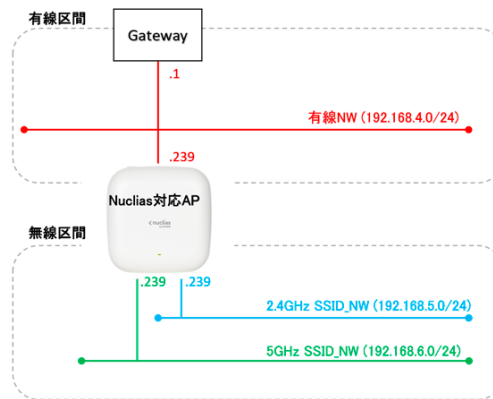
■ DHCP プール設定時の注意事項

DHCP プールを設定する場合、AP の有線区間のネットワークアドレスと、無線区間のネットワークアドレスが重複しないように設定してください。有線区間と無線区間でネットワークアドレスが重複していると、NAT (NAPT) 機能が正しく動作せず、無線区間から有線区間への通信ができなくなる可能性があります。

NG設定



OK設定



NG 設定の例：有線区間と無線区間 (5GHz SSID) のネットワークアドレスが重複しています。

OK 設定の例：有線区間と無線区間のネットワークアドレスが重複していません。

プロフィール - SSID - キャプティブポータルタブ

「キャプティブポータル」は、無線クライアントのユーザが Nuclias 管理アクセスポイントの SSID へ接続する際に、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、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入力した場合のみ、クライアントのトラフィックが許可されます。キャプティブポータルの設定と追加により、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、スプラッシュページに自動的にリダイレクトされます。

ただし、利用ブラウザ、利用 OS 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場合があるため、非 SSL サイト（http サイト）へのアクセスを推奨します。

注意

AP のマネジメント VLAN と VAP VLAN が異なっている場合、以下の機能が動作しません。

- ・外部キャプティブポータル
- ・サードパーティー資格情報でサインオン
- ・ウォールドガーデン

「キャプティブポータル」タブを選択し、キャプティブポータルの設定を行います。



図 8-11 プロファイル - SSID - キャプティブポータルタブ

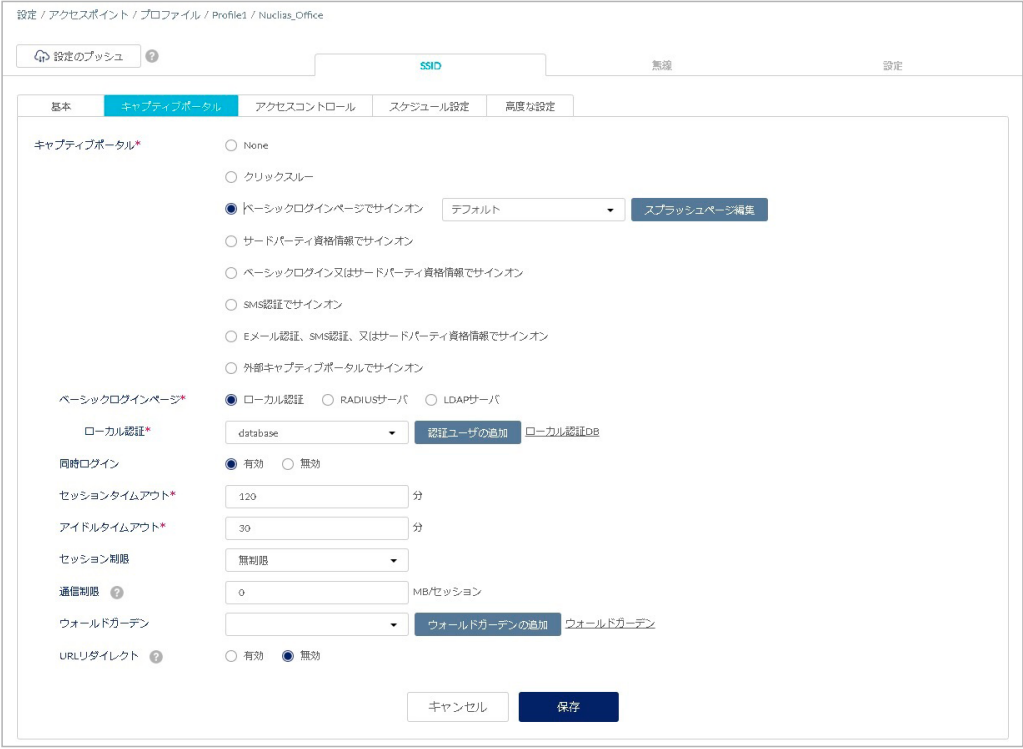


図 8-12 キャプティブポータルタブ（ベーシックログインページでサインオン）

キャプティブポータルのタイプを選択すると、それに適応したスプラッシュページをプルダウンから選択できるようになります。新しくスプラッシュページを作成する場合は、「スプラッシュページ編集」をクリックします。スプラッシュページの詳細については「スプラッシュページ」を参照ください。

■ キャプティブポータルのタイプ

キャプティブポータルのタイプを以下から選択します。

項目	説明
クリックスルー	Nuclias で設定するスプラッシュページ上のボタンを押下することで、上位ネットワークとの通信が許可されます。
ベーシックログインページでサインオン	スプラッシュページ上でユーザ ID とパスワードを入力します。 ユーザ ID とパスワードのリストは下記から選択します。 「ローカル認証」：Nuclias 上 で設定する ID ・パスワードでユーザ認証を行います。 「RADIUS サーバ」：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。 「LDAP サーバ」：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。 ● ローカル認証選択時は下記の設定をします。 「ローカル認証」：認証ユーザを選択します。 「認証ユーザの追加」をクリックすると追加ウィンドウが表示され、新規 DB を作成することができます。 「ローカル認証 DB」のリンクをクリックすると登録されている認証 DB が表示されます。 ● RADIUS サーバ選択時は下記の設定をします。 「プライマリ RADIUS サーバ」「セカンダリ RADIUS サーバ」：サーバを指定します。 「RADIUS サーバの追加」をクリックすると追加ウィンドウが表示され、新規サーバを追加することができます。 「RADIUS サーバ」のリンクをクリックすると登録されているサーバリストが表示されます。 注意 RADIUS サーバ設定における「認証方法」項目には以下の制限があります。 - DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 - DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。 ● LDAP サーバ選択時は下記の設定をします。 「プライマリ LDAP サーバ」「セカンダリ LDAP サーバ」：サーバを指定します。 「LDAP サーバの追加」をクリックすると追加ウィンドウが表示され、新規サーバを追加することができます。 「LDAP サーバ」のリンクをクリックすると登録されているサーバリストが表示されます。

項目	説明
サードパーティ資格情報でサインオン	スプラッシュページ上で使用する SNS を、「Facebook」「Google」「LINE」「Weibo」から 1 つ以上指定します。全て指定することも可能です。 無線クライアントは、いずれかの SNS で認証を実施すると上位ネットワークとの通信が許可されます。 注意 SNS 認証機能（Facebook、Google、LINE、Weibo）の場合、「同時ログイン」項目の設定に関わらず同時ログインが有効になっています。
ベーシックログイン又はサードパーティ資格情報でサインオン	上記の「ベーシックログイン」と「サードパーティ資格情報」の両方をスプラッシュページに表示します。 無線クライアントは、いずれかの認証を実施すると上位ネットワークとの通信が許可されます。 注意 SNS 認証機能（Facebook、Google、LINE、Weibo）の場合、「同時ログイン」項目の設定に関わらず同時ログインが有効になっています。
SMS 認証でサインオン	SMS 認証を有効にするには、SMS アカウントの設定が必要です。Nucias は、Twilio サービスを使用して SMS テキストメッセージを受信します。設定内容の詳細は「アドバンスド設定 > SMS 設定」を参照してください。
E メール認証、SMS 認証、又はサードパーティ資格情報でサインオン	スプラッシュページ上に「E メール認証」「SMS 認証」「サードパーティ資格情報」を表示します。 無線クライアントは、いずれかの認証を実施すると、上位ネットワークとの通信が許可されます。 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。 メール認証を有効にするために以下の設定をします。 ・「許容時間」：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。 ・「認証回数」：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。 ・「拒否時間」：無線利用者が認証用メールを要求後、「許容時間」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。 注意 SNS 認証機能（Facebook、Google、LINE、Weibo）の場合、「同時ログイン」項目の設定に関わらず同時ログインが有効になっています。
外部キャプティブポータルでサインオン	認証に外部キャプティブポータルを使用します。 ・「オプション」：「カスタム外部キャプティブポータル」が選択されます。 ・「スプラッシュページ URL」：スプラッシュページの URL を入力します。 ● RADIUS サーバ ・「プライマリ RADIUS サーバ」「セカンダリ RADIUS サーバ」：サーバを指定します。 ・「RADIUS サーバの追加」をクリックすると追加ウィンドウが表示され、新規サーバを作成することができます。 ・「RADIUS サーバ」のリンクをクリックすると登録されているサーバリストが表示されます。 注意 RADIUS サーバ設定における「認証方法」項目には以下の制限があります。 ・DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 ・DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。

■ キャプティブポータル画面の設定項目

選択したキャプティブポータルのタイプに応じて、以下の項目を設定します。

「同時ログイン」の設定を行います。本項目は「外部キャプティブポータルでサインオン」「クリックスルー」を選択した場合は表示されません。

項目	説明
同時ログイン	同一 ID 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。

「MAC 認証」の設定を行います。本項目は「外部キャプティブポータルでサインオン」を選択した場合に表示されます。

項目	説明
MAC 認証	MAC 認証の有効 / 無効を設定します。

「セッションタイムアウト」「アイドルタイムアウト」の項目では、全ての認証タイプにおいて、どのくらいの時間接続を許可するかを指定します。

項目	説明
セッションタイムアウト	無線クライアントがログイン成功後、何分間接続できるかを指定します。 セッションタイムアウトが過ぎると、再度ログインが必要になります。

第8章 デバイス設定

項目	説明
アイドルタイムアウト	無線クライアントが指定した時間（分）連続して通信しない場合、自動的にログアウトの状態にします。 セッションタイムアウトより短い時間を入力してください。

「セッション制限」の項目では、セッション数の制限を行います。
本項目は「SMS 認証でサインオン」を選択した場合は表示されません。

項目	説明
セッション制限	1 日の中で許容する、同一クライアントによるネットワークへの接続回数を選択します。 セッション制限を以下から選択して設定します。 ・ 選択肢：「無制限」「1」「2」「3」「4」「5」 注意 本項目は、DBA-1210P、DBA-X1230P のみでサポートされます。

「通信制限」の項目では、各クライアントが 1 セッションで送受信できるデータ量を制限します。
本項目は、「外部キャプティブポータルでサインオン」を選択した場合は表示されません。

項目	説明
通信制限	1 セッションで送受信できるデータ量を以下から選択します。 「0」を選択した場合は、送受信できるデータ量は無制限になります。 ・ 設定可能範囲：0-100000（MB） 注意 本項目は、DBA-2520P、DBA-2620P、DBA-2720P では未サポートです。

ワールドガーデンの設定を行います。本項目は「クリックスルー」を選択した場合は表示されません。

項目	説明
ワールドガーデン	ワールドガーデンを選択します。 ワールドガーデンを追加する場合は「ワールドガーデンの追加」をクリックし、設定を行います。 詳細は「 ワールドガーデン 」を参照してください。 注意 ワールドガーデンでは、「http」のページにはアクセスできません。 「https」でアクセスできるページを指定してください。

URL リダイレクトを行う場合は、以下の設定を行います。本項目は「外部キャプティブポータルでサインオン」を選択した場合は表示されません。

項目	説明
URL リダイレクト	本機能を有効にするとクライアントが無線 LAN に接続し、ブラウザを表示すると指定された 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。 ・ 「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」： 強制再リダイレクトを行う間隔（単位：分）を指定します。 指定できる間隔は「15」「30」「60」「120」「180」分です。「アイドルタイムアウト」で設定した値を超過しない値の選択肢のみ表示されます。 「15」分を選択した場合、15 分おきに指定した URL へ強制的にリダイレクトされます。 「1 回目のリダイレクトのみ」を選択した場合は、再リダイレクトは行いません。一度 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ことができます。 注意 URL リダイレクトが有効に設定されている場合、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。 注意 無線クライアントの OS やバージョンにより、動作が異なる場合があります。

プロファイル - SSID - アクセスコントロールタブ

「アクセスコントロール」タブでは、MAC フィルタリングと IP フィルタリングの設定を行います。

設定 / アクセスポイント / プロファイル / DBA-2820P / Nuclias_Office

設定のプッシュ ?

SSID 無線 設定

基本 キャプティブポータル **アクセスコントロール** スケジュール設定 高度な設定

MACフィルタリング ?

MACフィルタリング ☐ 有効 ☒ 無効

フィルタ ☐ RADIUSサーバ ☐ MAC ACL

MAC ACLポリシー ☐ 許可 ☒ 拒否

IPフィルタリング ?

IPフィルタリング ☐ 有効 ☒ 無効

IP ACLポリシー ☐ 許可 ☒ 拒否

IP ACL名 IP ACLの追加 IP ACL

キャンセル 保存

図 8-13 プロファイル - SSID - アクセスコントロールタブ

第8章 デバイス設定

■ MAC フィルタリング

「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。

項目	説明
MAC フィルタリング	MAC フィルタリングを使用する場合は「有効」を選択します。
フィルタ	使用する MAC アドレスリストを、Nuclias 上で設定する「MAC ACL」と、RADIUS サーバを使用する「RADIUS サーバ」から選択します。
MAC ACL ポリシ	「フィルタ」で「MAC ACL」を選択した場合に表示されます。 ・「許可」: AC 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」: 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。
MAC ACL 名	「フィルタ」で「MAC ACL」を選択した場合に使用するリストを指定します。「 <u>MAC ACL</u> 」のリンクをクリックすると、MAC ACL のリストが表示されます。 「MAC ACL の追加」については「 MAC ACL の追加 」を参照してください。
プライマリ RADIUS サーバ セカンダリ RADIUS サーバ	「フィルタ」で「RADIUS サーバ」を選択した場合に表示されます。プルダウンメニューから RADIUS サーバを選択します。「 <u>RADIUS サーバ</u> 」のリンクをクリックすると、RADIUS サーバのリストが表示されます。 RADIUS サーバの追加 「RADIUS サーバの追加」をクリックし、RADIUS サーバを追加することもできます。 RADIUS サーバの追加については「認証 - 認証サーバ - RADIUS サーバの追加」を参照してください。 注意 RADIUS サーバ設定における「認証方法」項目には以下の制限があります。 ・DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 ・DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。

■ IP フィルタリング

「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 アドレスまたはネットワーク宛ての通信を、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 アドレス宛ての通信の動作設定を行います。

項目	説明
IP フィルタリング	IP フィルタリングを使用する場合は「有効」を選択します。
IP ACL ポリシ	・「許可」: IP ACL リストに登録された IP アドレス（グループ）宛の通信を許可し、それ以外は破棄します。 ・「拒否」: IP ACL リストに登録された IP アドレス（グループ）宛の通信を破棄し、それ以外は許可します。
IP ACL 名	使用する IP アドレスリストを指定します。「 <u>IP ACL</u> 」のリンクをクリックすると、IP ACL のリストが表示されます。 「IP ACL の追加」については「 IP ACL の追加 」参照してください。

設定後、ページ下部の「保存」をクリックします。
デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

プロファイル - SSID - スケジュール設定タブ

「スケジュール設定」タブでは、SSID のスケジュール設定を行います。指定した曜日、時刻に SSID が有効になります。初期設定は全曜日終日有効です。

注意 2019 年 7 月 23 日以前にサイトを作成していた場合、スケジュール設定の内容が 1 時間遅れで実行されます。
正しい時刻で実行するには、再度サイトを作り直してください。

「スケジュールポリシー」のドロップダウンリストで、適用するスケジュールを選択します。
「スケジュールポリシー」のリンクをクリックすると、**設定>スケジュールポリシー**画面に移動します。

図 8-14 プロファイル - SSID - スケジュール設定タブ

スケジュールを選択後、ページ下部の「保存」をクリックします。
デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

■ スケジュールポリシーの追加

1. 「スケジュールポリシーの追加」をクリックし、以下の画面を表示します。

図 8-15 スケジュールポリシーの追加

2. 「名前」を入力し、各曜日のスケジュールを設定します。
「テンプレート」のドロップダウンリストでスケジュールテンプレートを選択することもできます。

注意 「再起動」項目は未サポートです。

注意 スケジュールが「オフ」の間中は、対象の SSID を Hidden で広告（接続は不可）、または停波します。

3. 「保存」をクリックし、スケジュールポリシーを追加します。

プロファイル - SSID - 高度な設定タブ

「高度な設定」タブでは、SSID プロファイルの詳細設定を行います。

設定 / アクセスポイント / プロファイル / DBA-2820P / Nuclias_Office

設定のプッシュ SSID 無線 設定

基本 キャプティブポータル アクセスコントロール スケジュール設定 高度な設定

クライアント制限 ☒ 有効 ☐ 無効

最大クライアント数* 64

クライアントからの最大接続リトライ数* 5

最大上り帯域* 0 Kbps

最大下り帯域* 0 Kbps

最大クライアント上り帯域* 0 Kbps

最大クライアント下り帯域* 0 Kbps

フォワードBonjourパケット ☐ 有効 ☒ 無効

IGMPスヌーピング ☐ 有効 ☒ 無効

最大マルチキャスト帯域* 0 Kbps

RTS閾値* 2347 bytes

強制ローミング* ☒ 有効 ☐ 無効

電波強度しきい値* -70 dBm

低電波強度を許可 ☒ 有効 ☐ 無効

弱いRSSI値のクライアントを許可* 1 - 10

キャンセル 保存

図 8-16 プロファイル - SSID - 高度な設定タブ

本画面には以下の項目があります。

項目	説明
クライアント制限	接続するクライアント数の制限を有効または無効にします。
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 0-10 (回) の間で指定します。 「0」にした場合、接続しているクライアント数が「最大クライアント数」に達している状態では、それ以上クライアントは SSID に接続できません。
最大上り帯域	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。 本項目に「0」を指定した場合、最大値は設定されず無制限となります。
最大下り帯域	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。 本項目に「0」を指定した場合、最大値は設定されず無制限となります。
最大クライアント上り帯域	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。 本項目に「0」を指定した場合、最大値は設定されず無制限となります。 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、本項目を 0 に設定する必要があります。
最大クライアント下り帯域	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。 本項目に「0」を指定した場合、最大値は設定されず無制限となります。 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、本項目を 0 に設定する必要があります。
フォワード Bonjour パケット	クライアントからの Bonjour パケットフォワーディングの有効 / 無効を設定します。
IGMP スヌーピング	マルチキャスト接続を構築する IGMP スヌーピングの有効 / 無効を設定します。
最大マルチキャスト帯域	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。 本項目に「0」を指定した場合、最大値は設定されず無制限となります。

項目	説明
RTS 閾値	デバイスがパケットを送信する際の RTS しきい値を指定します。この設定値を超えるパケットを送信する場合、RTS 信号が送信されます。主に隠れ端末問題などを解決します。256 - 2347 (bytes) から指定できます。
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 から拒否されます。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。
電波強度しきい値	「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拒否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が一定の回数以上 AP への接続を試みた場合に、クライアントと AP 間の接続を許可します。回数の設定は「弱い RSSI 値のクライアントを許可」で行います。
弱い RSSI 値のクライアントを許可	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 (回) の間で指定します。

注意 「最大上り/下り帯域」「最大クライアント上り/下り帯域」について、IPv6 トラフィックを対象とした制御は未サポートです。

設定後、ページ下部の「保存」をクリックします。
デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

プロファイル - 無線

設定 > アクセスポイント > プロファイル画面で「アクション」欄の「無線」をクリックすると、無線の設定画面が表示されます。
以下のタブについて設定を行います。

- 基本：詳細は「[プロファイル - 無線 - 基本タブ](#)」を参照してください。
- チャンネル：詳細は「[プロファイル - 無線 - チャンネルタブ](#)」を参照してください。
- 高度な設定：詳細は「[プロファイル - 無線 - 高度な設定タブ](#)」を参照してください。

図 8-17 プロファイル - 無線

プロファイル - 無線 - 基本タブ

「無線」の「基本」タブ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。
アクセスポイントでサポートされる周波数帯に応じて、2.4GHz/5GHz/6GHz の各帯域に対して無線モードなどを設定することができます。

図 8-18 プロファイル - 無線 - 基本タブ

DBA-2720P の場合は、本画面で「5GHz」のかわりに「5GHz1」「5GHz2」の 2 つの項目が表示されます。
DBA-X5480P の場合は、本画面で「2.4GHz」「5GHz」「6GHz」の 3 つの項目が表示されます。

第8章 デバイス設定

本画面には以下の項目があります。

項目	説明
無線バンドの有効	各帯域を有効または無効にします。
無線モード	各帯域の無線モードを選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2720P/DBA-2820P/DBA-3621P の場合： - 2.4GHz - 「N only」 「B/G」 「B/G/N」 - 5GHz - 「N only」 「A only」 「A/N」 「A/N/AC」 ● DBA-X2830P/DBA-X1230P の場合： - 2.4GHz - 「N only」 「B/G」 「B/G/N」 「B/G/N/AX」 - 5GHz - 「N only」 「A only」 「A/N」 「A/N/AC」 「A/N/AC/AX」 ● DBA-X5480P の場合： - 2.4GHz - 「N only」 「B/G」 「B/G/N」 「B/G/N/AX」 - 5GHz - 「N only」 「A only」 「A/N」 「A/N/AC」 「A/N/AC/AX」 - 6GHz - 「AX」
チャンネル帯域	チャンネル帯域を選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2720P/DBA-3621P/DBA-X1230P の場合： - 2.4GHz - 「20MHz」 「20/40MHz(Auto)」 - 5GHz - 「20MHz」 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 ● DBA-2820P の場合： - 2.4GHz - 「20MHz」 「20/40MHz(Auto)」 - 5GHz - 「20MHz」 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80+80MHz(Auto)」 「20/40/80/160MHz(Auto)」 ● DBA-X2830P の場合： - 2.4GHz - 「20MHz」 「20/40MHz(Auto)」 - 5GHz - 「20MHz」 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 ● DBA-X5480P の場合： - 2.4GHz - 「20MHz」 「20/40MHz(Auto)」 - 5GHz - 「20MHz」 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 - 6GHz - 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 注意 DBA-2820P では、80+80MHz または 160MHz を選択した場合ストリームが 2x2 になります。 注意 DBA-X2830P では、160MHz を選択した場合ストリームが 2x2 になります。
送信電波出力	各帯域の送信電波出力をそれぞれ 2-100（%）で指定します。
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。

設定後、ページ下部の「保存」をクリックします。

デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

プロファイル - 無線 - チャンネルタブ

「チャンネル」タブでは 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します。
「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。

図 8-19 プロファイル - 無線 - チャンネルタブ

DBA-2720P の場合は、本画面で「5GHz」のかわりに「5GHz1」「5GHz2」の 2 つの項目が表示されます。
DBA-X5480P の場合は、本画面で「2.4GHz」「5GHz」「6GHz」の 3 つの項目が表示されます。

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	オートチャンネルを有効または無効に設定します。 オートチャンネルを無効にすると、各帯域（2.4GHz/5GHz/6GHz）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」が有効でない場合に手動でチャンネルを選択します。 5GHz 帯については、日本で使用不可なチャンネル（149, 153, 157, 161）を選択した場合、設定プッシュ時にエラーとなります。
有効チャンネル	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。ただし 5GHz 帯は、日本で使用不可なチャンネル（149, 153, 157, 161）には切り替わりません。オートチャンネルで利用するチャンネルは「青地に白色の文字」、利用しないチャンネルは「白地に黒色の文字」で表示されます。数字のマスをクリックすることにより、利用する / しないを切り替えることができます。
強制オートチャネルスキャン	オートチャンネルを強制的に実行する機能を有効または無効にします。 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。
オートチャネル間隔	オートチャンネルの実行間隔を指定します。 ・ 設定可能範囲：6-24（時間）
オートチャネル実行	AP がオートチャンネル有効の状態で作動している状態で「今すぐオートチャネル実行」をクリックするとオートチャンネルを開始します。 本項目をクリックすると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一時的な停止を考慮し、実行してください。

設定後、ページ下部の「保存」をクリックします。
デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

- 注意** 6GHz 帯の「有効チャンネル」では PSC チャンネルが選択可能です。
- 注意** DFS 検知により使用可能なチャンネルがないと判断された場合は、30 分間停波、または W52 に遷移します。
- 注意** DBA-2620P と DBA-2720P において、「有効チャンネル」の設定をアクセスポイントに反映するには以下の手順を実行してください。
 - ①「有効チャンネル」を選択し、「保存」をクリックします。
 - ②「設定のプッシュ」をクリックします。
 - ③「今すぐオートチャネル実行」をクリックします。

プロファイル - 無線 - 高度な設定タブ

「高度な設定」タブでは 2.4GHz/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。

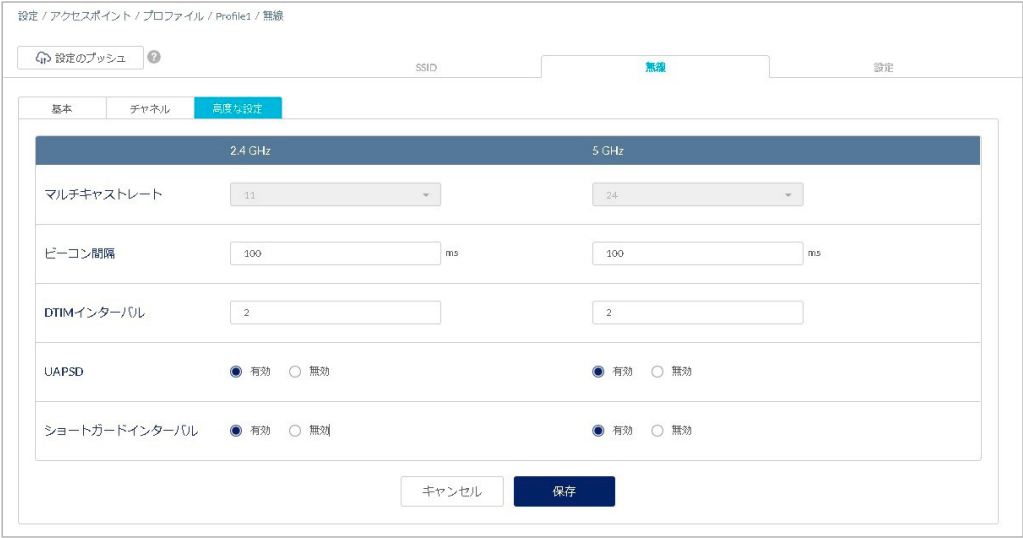


図 8-20 プロファイル - 無線 - 高度な設定タブ

DBA-2720P の場合は、本画面で「5GHz」のかわりに「5GHz1」「5GHz2」の 2 つの項目が表示されます。
DBA-X5480P の場合は、本画面で「2.4GHz」「5GHz」「6GHz」の 3 つの項目が表示されます。（6Ghz 帯における本画面の設定はサポートされていません。）

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。100 - 3500 (ms) の範囲で設定可能です。
DTIM インターバル	DTIM インターバルは TIM（Traffic Indication Map）を使用して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 の範囲で設定可能です。
UAPSD	U-APSD を有効または無効に設定します。 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	ショートガードインターバルを有効または無効に設定します。 有効にした場合、データとデータの間に挿入される時間（ガードインターバル）を短くし、データの送信時間が短縮されます。データの干渉がおこりやすくなるため、無効にすることで通信が安定する場合があります。

設定後、ページ下部の「保存」をクリックします。
デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

プロファイル - 設定

設定 > アクセスポイント > プロファイル画面で「アクション」欄の「設定」をクリックすると、プロキシと IPv6 の設定画面が表示されます。

設定 / アクセスポイント / プロファイル / Profile1 / SSID

設定のプッシュ ? SSID 無線 設定

プロキシ ☐ 有効 ☒ 無効

IPv6 ☒ 有効 ☐ 無効

ファストローミング ☐ 有効 ☒ 無効

マネジメント VLAN ☐ 有効 ☒ 無効

再起動スケジュール ☐ 有効 ☒ 無効

デバイス設置環境のVLANやプロキシ設定が変更されていることを確認してください。そうでない場合、デバイスはNucliasから切断されます。
デバイスがローカル設定になっている場合、IPアドレス、マネジメントVLAN、プロキシ設定は、このページからの変更されません。

キャンセル 保存

図 8-21 プロファイル - 設定

本画面には以下の項目があります。

項目	説明
プロキシ	アクセスポイントを Nuclias サーバに接続する際、プロキシ経由で接続する場合は有効にします。有効にした場合は、プロキシホストとプロキシポートを入力します。 注意 デバイスで使用するプロキシサーバは WebSocket をサポートしている必要があります。 注意 本設定は無線 LAN クライアントのインターネット接続には影響を与えません。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 DBA-X5480P は Cloud サーバとの接続に IPv4 または IPv6 アドレスを使用しますが、プロキシサーバは IPv4 アドレスのみ指定可能です。
IPv6	アクセスポイントで IPv6 によるローカル設定の有効 / 無効を切り替えます。
ファストローミング	ファストローミング（高速ローミング）を有効 / 無効にします。 本機能は、NAT モードが有効、または WPA3 セキュリティが設定されている SSID では有効にできません。
マネジメント VLAN	マネジメント VLAN を有効 / 無効に設定します。 有効にした場合、VLAN モードと VLAN タグを設定します。
再起動スケジュール	再起動スケジュールを有効 / 無効に設定します。有効を選択した場合、再起動のスケジュールを指定します。 注意 本機能は未サポートです。

設定後、ページ下部の「保存」をクリックします。

デバイスへの設定の適用には「設定のプッシュ」を行う必要があります。

注意 デバイス設置環境の VLAN やプロキシ設定が変更されていることを確認してください。そうでない場合、デバイスは Nuclias から切断されます。

注意 デバイスがローカル設定になっている場合、IP アドレス、マネジメント VLAN、プロキシ設定は、このページからの変更されません。

アクセスポイント - デバイス

設定 > アクセスポイント > デバイス を選択し、デバイスに関する設定を実施します。



図 8-22 デバイス

本画面には以下の項目があります。

項目	説明
チェックボックス	デバイスを選択し「削除」をクリックすると、Nuclias からそのデバイスが削除されます。 注意 デバイスを削除しても、そのデバイスに紐づけられているフリーライセンスは元の組織に残ります。そのため該当デバイスを別の組織に登録する場合、別途ライセンスを用意いただく必要があります。 注意 デバイスを Nuclias から削除すると、そのデバイスに関するイベントログは全て削除されます。そのためイベントログを残しておく必要がある場合は、事前にイベントログをダウンロードしてください。詳細は、第 7 章 モニタ「 アクセスポイント - イベントログ 」を確認してください。
状態	各機器のステータスを以下の色で表示します。 ・ 緑色：オンライン / 赤色：オフライン / 灰色：休止（デバイスが登録済だが、Nuclias に未接続である状態）
デバイス名	Nuclias 上でのデバイス名を表示します。本項目をクリックすると、各デバイスの設定画面へ移行します。
MAC アドレス	デバイスの MAC アドレスを表示します。
グローバル IP アドレス	デバイスのグローバル IP アドレスを表示します。
ローカル IP アドレス	デバイス本体に割り振られているローカル IP アドレスを表示します。
モデル名	デバイスのモデル名を表示します。
接続	デバイスの直近のステータスを表示します。緑色がオンライン、赤色がオフラインを表示します。時間帯は、「タイムフレーム」で設定できます。四角形の左端はタイムフレームで設定した日時のうち最も古いときを、右端は現在を指しています。
同期ステータス	デバイスに Nuclias 上の最新の設定が同期されているかを表示します。
デバイス UID	デバイスの UID を表示します。
プロファイル	デバイスが紐づいているプロファイルを表示します。
サイト	デバイスが紐づいているサイトを表示します。
サイトタグ	上記のサイトにサイトタグが紐づいている場合、サイトタグを表示します。
シリアル番号	デバイスのシリアル番号を表示します。
ファームウェアバージョン	デバイスのファームウェアバージョンを表示します。
ハードウェアバージョン	デバイスハードウェアバージョンを表示します。
最終閲覧	最終接続日時を表示します。デバイスがオンライン状態の場合は「オンライン」と表示されます。
ライセンス状態	デバイスに紐づけられているライセンスのステータスを表示します。
登録日	デバイスを Nuclias に登録した日を表示します。
期限日	ライセンスの期限日を表示します。
現在のクライアント	現在デバイスに接続しているクライアント数を表示します。
使用量	デバイスの通信容量を表示します。
チャンネル	デバイス（AP）に設定されているチャンネルを表示します。「2.4GHz/5GHz/6GHz のチャンネル」が表示されます。表示される帯域は製品により異なります。
送信電波出力	2.4GHz/5GHz/6GHz の電波出力を表示します。表示される帯域は製品により異なります。
LACP	デバイスの LACP の状態を表示します。

■ デバイスの追加

1. 設定 > アクセスポイント > デバイス画面の「デバイスの追加」をクリックし、以下の画面で設定を行います。

デバイスの追加

デバイスUID*

UIDを選択してください

デバイス名

1-64文字

登録するデバイスのUIDを入力してください

UIDフォーマットはXXXXXXXXXXXXまたはXXXXXXXXXXXXXXXXです。

サイト*

?

プロファイル*

更にライセンスを追加する

?

キャンセル

保存

図 8-23 デバイスの追加

本画面には以下の項目があります。

項目	説明
デバイス UID	デバイス UID を入力します。
デバイス名	Nuclias 上で管理するためのデバイス名を入力します。
サイト	デバイスに適用するサイトをプルダウンで選択します。
プロファイル	デバイスに適用するプロファイルをプルダウンで選択します。
ライセンスキー	「更にライセンスを追加する」をクリックし、ライセンスキーを紐づけます。 枠をクリックすると、そのデバイスで使用可能なライセンスキーがプルダウンで表示されますので、選択することができます。使用可能なライセンスキーとは、デバイスに初期状態で紐づけられているライセンスキー、または既に組織に登録されているライセンスキーです。これらとは異なるライセンスキーを使用する場合は、枠に直接入力してください。 選択可能なライセンスキーが複数ある場合の詳細については、巻末の「付録A ライセンスの適用や開始等に関する詳細」をご確認ください。 ライセンスキー #1* ライセンスキーを選択してください 123.100.244.123.100.244.234(363 日) 123.100.244.123.100.244.234(361 日) 123.100.244.123.100.244.234(195 日) 注意 デバイスに紐づけられているフリーライセンスは最初にデバイスを登録した組織に保存され、他の組織で使うことはできません。該当デバイスを本組織から削除し、他の組織へ登録し直す場合、別途ライセンスを用意頂く必要があります。

2. 設定後、「保存」をクリックします。

■ 表示する期間の変更

「タイムフレーム」で表内の「接続」欄に表示する期間を設定します。

■ デバイス情報の検索

特定の文字列を含む情報を検索する場合は、検索ウィンドウに文字を入力します。

■ 表示する項目の選択

をクリックすると表示できる項目の一覧が表示されます。表示する項目にチェックをいれます。

■ デバイス情報のダウンロード

をクリックし、デバイスの情報を CSV 形式でダウンロードします。

デバイス - 基本

設定 > アクセスポイント > デバイス 画面でデバイス名をクリックすると、デバイスごとの設定画面に移行します。
「基本」タブでは以下の画面が表示されます。

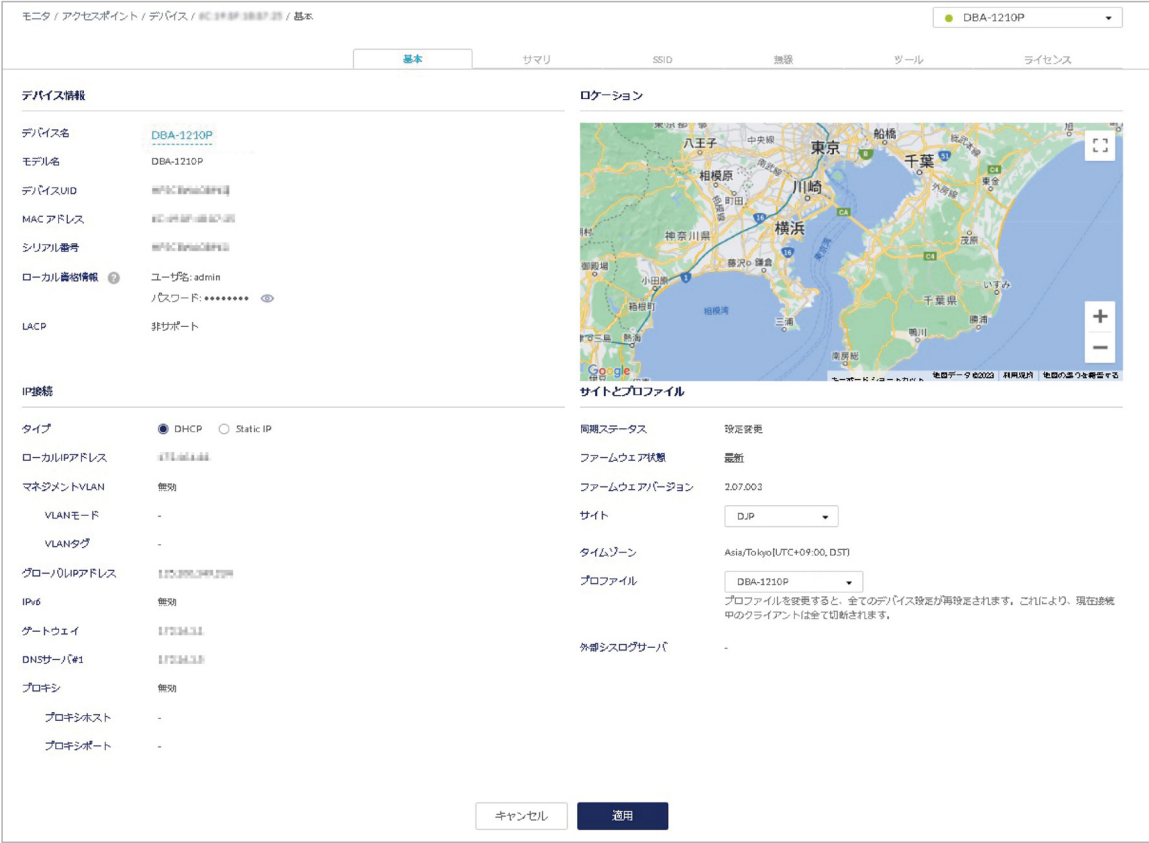


図 8-24 デバイス - 基本

■ デバイス情報

デバイス名、モデル名、デバイス UID、MAC アドレス、シリアル番号、ローカル資格情報、LACP を表示します。
デバイス名は変更可能です。

■ サイトとプロファイル

同期ステータス、ファームウェア状態、ファームウェアバージョン、サイト、タイムゾーン、プロファイル、外部シスログサーバが表示されます。
サイトとプロファイルはドロップダウンリストから変更できます。

■ IP 接続

IP 接続には以下の項目があります。

項目	説明
タイプ	IP 設定を「DHCP」「Static IP」から選択します。 「DHCP」：デバイスは DHCP クライアントとなります。 「Static IP」：スタティック IP 設定を行います。以降に表示される項目が設定できるようになります。
ローカル IP アドレス	デバイスの IP アドレスです。
マネジメント VLAN	デバイスのマネジメント VLAN 設定です。
グローバル IP アドレス	デバイスのグローバル IP 設定です。
IPv6	IPv6 の有効 / 無効を表示します。
ゲートウェイ	デバイスのゲートウェイ設定です。
DNS サーバ	デバイスの DNS サーバ設定です。
プロキシ	デバイスのプロキシ設定です。

設定後、「適用」をクリックします。Nuclias 上に設定が保存され、当該デバイスにも即時に設定が反映されます。

デバイス - サマリ

設定 > アクセスポイント > デバイス 画面でデバイスを選択 → 「サマリ」タブを選択します。

「サマリ」タブでは以下の画面が表示されます。

注意 「サマリ」タブは、DBA-2620P および DBA-2720P では未サポートの為表示されません。

注意 DBA-2520P では、「サマリ」タブは表示されますが未サポートです。



図 8-25 デバイス - サマリ

■ クライアント

接続クライアントの数とクライアントの使用量をグラフで表示します。

表示の対象とする期間を「タイムフレーム」、表示の対象とする SSID を「SSID's」、表示の対象とする帯域を「帯域」のプルダウンメニューから選択します。

- ・ **接続クライアント**
接続しているクライアントの数を、時間または日別に棒グラフで表示します。グラフ上にカーソルをあてると数値が表示されます。
 - ・ **クライアント使用量**
「タイムフレーム」で指定した期間のクライアントの使用量を、クライアント名または MAC アドレス別、かつデバイス別に曲線グラフで表示します。グラフの線上にカーソルをあてると数値が表示されます。以下の項目を設定します。
 - 「表示タイプ」：表示の種類を、プルダウンメニューの「クライアント名」、または「MAC アドレス」から選択します。
 - 「デバイス」：表示の対象とするデバイスをプルダウンメニューから選択します。
- 🔄 アイコンをクリックすると、情報を最新の状態に更新できます。 ⬇️ アイコンをクリックすると、表示している情報を CSV 形式でダウンロードできます。

■ **ワイヤレス**

電波の強度、チャンネルの使用率、およびデータレートを曲線グラフで表示します。
表示の対象とする時間の範囲を「タイムフレーム」、表示の対象とする SSID を「SSIDs」、表示の対象とする帯域を「帯域」のプルダウンメニューから選択します。

- ・ **電波強度**
対象とする電波の質の強度を曲線グラフで表示します。グラフの線上にカーソルをあてると数値が表示されます。
以下の項目を設定します。
 - 「電波の質の指標」：表示の対象とする電波品質の種類をプルダウンメニューから選択します。
- ・ **チャンネル使用率**
チャンネルの使用率を曲線グラフで表示します。グラフの線上にカーソルをあてると数値が表示されます。
- ・ **データレート**
選択したタイムフレームにおけるデータレートを、パケットの種別ごとに曲線グラフで表示します。グラフの線上にカーソルをあてると数値が表示されます。以下の項目を設定します。
 - 「パケットタイプ」：表示の対象とするパケットの種別をプルダウンメニューから選択します。

🔄 アイコンをクリックすると、情報を最新の状態に更新できます。 ⬇️ アイコンをクリックすると、表示している情報を CSV 形式でダウンロードできます。

デバイス - SSID

「ユーザプロファイル設定」を「有効」または「無効」に設定し、プロファイルの SSID 設定をデバイスに適用するかどうか選択できます。

- 「有効」を選択した場合：
設定 > アクセスポイント > プロファイル画面で設定したプロファイルの SSID をデバイスに適用します。
画面右の「プロファイル設定の閲覧」をクリックすると、設定 > アクセスポイント > プロファイルの SSID 設定画面に移行します。
プロファイルの SSID 設定については、「[プロファイル - SSID](#)」を参照してください。
- 「無効」を選択した場合：
設定 > アクセスポイント > プロファイル画面で設定したプロファイルの SSID を使用しません。本画面で各デバイス専用の SSID を作成できます。
本画面で作成するデバイス専用の SSID は、設定 > アクセスポイント > プロファイル画面で設定した SSID と比較して機能が制限されます。

モニタ / アクセスポイント / デバイス / DBA-2820P / SSID

DBA-2820P

基本 サマリ SSID 無線 ツール ライセンス

ユーザプロファイル設定 ☒ 有効 ☐ 無効 [プロファイル設定の閲覧](#)

#	SSID	2.4 GHz	5 GHz	ブロードキャストSSID	セキュリティ
1	_DUP_Garven	✓	✓	✓	WPA / WPA2
2	_DUP_Garven_2	✓	✓	✓	WPA / WPA2
3	TEST3	✓	✓	✓	WPA / WPA2
4	TEST4	✓			Open
5	TEST5		✓		Open
6	TEST6	✓	✓	✓	WPA / WPA2
7	TEST7	✓	✓		Open
8	TEST8	✓	✓		Open
9	TEST9	✓			Open

1 10

適用

図 8-26 デバイス - SSID

■ デバイス固有の SSID を追加する

1. 「ユーザプロファイル設定」を「無効」にします。



図 8-27 デバイス - SSID（ユーザプロファイル設定無効）

2. 「SSID の追加」をクリックします。
3. SSID 名を入力し、「バンド選択」で使用する帯域を選択 → 「保存」をクリックします。



図 8-28 SSID の追加

4. 作成した SSID が表示されるので、SSID 名をクリックして設定を行います。

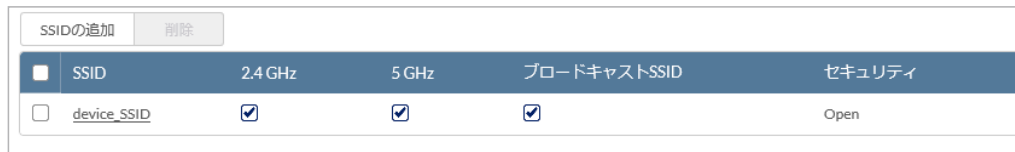


図 8-29 デバイス - SSID 一覧

SSID 設定内容については「[デバイス固有の SSID 設定](#)」を参照してください。

デバイス固有の SSID 設定

デバイス固有の SSID のリンクをクリックすると、SSID の設定画面が表示されます。



図 8-30 デバイス - SSID- 基本タブ

各タブの設定項目はプロファイルの SSID 設定と同じです。詳細は以下を参照してください。

- ・「[プロファイル - SSID - 基本タブ](#)」
- ・「[プロファイル - SSID - キャプティブポータルタブ](#)」
- ・「[プロファイル - SSID - アクセスコントロールタブ](#)」
- ・「[プロファイル - SSID - スケジュール設定タブ](#)」
- ・「[プロファイル - SSID - 高度な設定タブ](#)」

デバイス - 無線

「ユーザプロファイル設定」を「有効」または「無効」に設定し、プロファイルの無線設定をデバイスに適用するかどうかを選択できます。

■ 「ユーザプロファイル設定」を「有効」にした場合：

設定 > アクセスポイント > プロファイル画面で設定したプロファイルの無線設定をデバイスに適用します。
画面右端の「プロファイル設定の閲覧」をクリックすると、設定 > アクセスポイント > プロファイルの無線設定画面に移行します。
プロファイルの無線設定については、「[プロファイル - 無線](#)」を参照してください。

■ 「ユーザプロファイル設定」を「無効」にした場合：

設定 > アクセスポイント > プロファイル画面で設定したプロファイルの無線設定を使用しません。
本画面でデバイスごとに無線設定を行います。

モニタ / アクセスポイント / デバイス / DBA-2820P / 無線 DBA-2820P

基本 サマリ SSID 無線 ツール ライセンス

ユーザプロファイル設定 ☐ 有効 ☒ 無効 [プロファイル設定の閲覧](#)

2.4 GHz	5 GHz
無線 ☒ 有効 ☐ 無効	無線 ☒ 有効 ☐ 無効
無線モード B / G / N	無線モード A / N / AC
チャネル帯域 20/40 MHz (Auto)	チャネル帯域 20/40/80 MHz (Auto)
送信電波出力 100 %	送信電波出力 100 %
オートチャネル ☒ 有効 ☐ 無効	オートチャネル ☒ 有効 ☐ 無効
チャネル オート	チャネル オート
有効チャネル 1 2 3 4 5 6 7 8 9 10 11 12 13 ☐ 未選択 ☒ 選択済	有効チャネル 36 40 44 48 52 56 60 64 100 104 108 112 116 120 124 128 132 136 140 ☐ 未選択 ☒ 選択済
サイト Japan	サイト Japan
強制オートチャネルスキャン ☐ 有効 ☒ 無効	強制オートチャネルスキャン ☐ 有効 ☒ 無効
オートチャネル間隔 6 時間	オートチャネル間隔 6 時間
オートチャネル実行 今すぐオートチャネル実行	オートチャネル実行 今すぐオートチャネル実行
SSID隠蔽バージョン ☐ 有効 ☒ 無効	

キャンセル

適用

図 8-31 デバイス - 無線

DBA-2720P の場合は、本画面で「5GHz」のかわりに「5GHz1」「5GHz2」の 2 つの項目が表示されます。
DBA-X5480P の場合は、本画面で「2.4GHz」「5GHz」「6GHz」の 3 つの項目が表示されます。

本画面には以下の項目があります。

項目	説明
無線バンドの有効	各帯域を「有効」または「無効」にします。
無線モード	各帯域の無線モードを選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2720P/DBA-2820P/DBA-3621P の場合： - 2.4GHz - 「N only」「B/G」「B/G/N」 - 5GHz - 「N only」「A only」「A/N」「A/N/AC」 ● DBA-X2830P/DBA-X1230P の場合： - 2.4GHz - 「N only」「B/G」「B/G/N」「B/G/N/AX」 - 5GHz - 「N only」「A only」「A/N」「A/N/AC」「A/N/AC/AX」 ● DBA-X5480P の場合： - 2.4GHz - 「N only」「B/G」「B/G/N」「B/G/N/AX」 - 5GHz - 「N only」「A only」「A/N」「A/N/AC」「A/N/AC/AX」 - 6GHz - 「AX」
チャンネル帯域	チャンネル帯域を選択します。 ● DBA-1210P/DBA-2520P/DBA-2620P/DBA-2720P/DBA-3621P/DBA-X1230P の場合： - 2.4GHz - 「20MHz」「20/40MHz(Auto)」 - 5GHz - 「20MHz」「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 ● DBA-2820P の場合： - 2.4GHz - 「20MHz」「20/40MHz(Auto)」 - 5GHz - 「20MHz」「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80+80MHz(Auto)」 「20/40/80/160MHz(Auto)」 ● DBA-X2830P の場合： - 2.4GHz - 「20MHz」「20/40MHz(Auto)」 - 5GHz - 「20MHz」「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 ● DBA-X5480P の場合： - 2.4GHz - 「20MHz」「20/40MHz(Auto)」 - 5GHz - 「20MHz」「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 - 6GHz - 「20/40MHz(Auto)」 「20/40/80MHz(Auto)」 「20/40/80/160MHz(Auto)」 注意 DBA-2820P では、80+80MHz または 160MHz を選択した場合ストリームが 2x2 になります。 注意 DBA-X2830P では、160MHz を選択した場合ストリームが 2x2 になります。
送信電波出力	各帯域の送信電波出力をそれぞれ「2-100」(%) で指定します。
オートチャンネル	オートチャンネルの有効 / 無効を切り替えます。 オートチャンネルを無効にすると、各帯域 (2.4GHz/5GHz/6GHz) 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	オートチャンネルが無効の場合に手動でチャンネルを選択します。 5GHz 帯について日本で使用不可なチャンネル (149, 153, 157, 161) を選択すると、設定適用時にエラーとなります。
有効チャンネル	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。ただし 5GHz 帯は、日本で使用不可なチャンネル (149,153,157,161) には切り替わりません。 オートチャンネルで利用するチャンネルは「青地に白色の文字」、利用しないチャンネルは「白地に黒色の文字」で表示されます。数字のマスをクリックすることにより、利用する / しないを切り替えることができます。 注意 6GHz 帯の「有効チャンネル」では PSC チャンネルが選択可能です。
サイト	サイトを表示します。
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または無効にします。 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。1 時間単位で、6-24 (時間) の範囲で設定できます。
オートチャンネル実行	AP がオートチャンネル有効の状態で作動している状態で「今すぐオートチャンネル実行」をクリックするとオートチャンネルを開始します。 本項目をクリックすると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一時的な停止を考慮し、実行してください。
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。

設定後、「適用」をクリックします。

Nuclias 上に設定が保存され、当該デバイスへも即時に設定が反映されます。

注意 DFS 検知により使用可能なチャンネルがないと判断された場合は、30 分間停波、または W52 に遷移します。

デバイス - ツール

本項目ではデバイスと Nuclias の接続の確認と、デバイスの再起動を行います。

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できます。
また、LED の点滅により、デバイスが Nuclias からの操作に対応しているか確認できます。

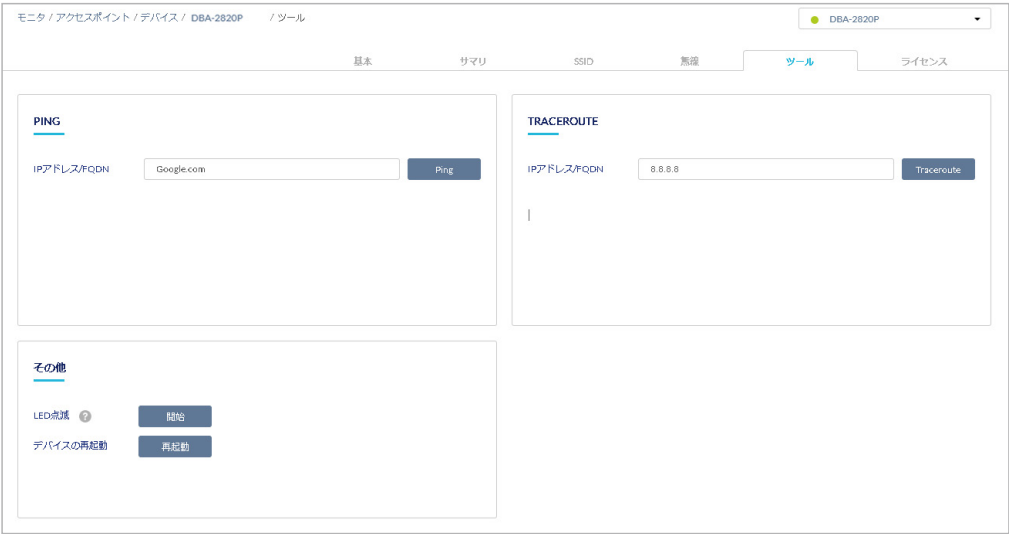


図 8-32 デバイス - ツール

本画面には以下の項目があります。

項目	説明
PING	「IP アドレス /FQDN」に、接続性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ます。 「Ping」をクリックし、Ping を実行します。Ping により、指定のデバイスに対する接続性を確認できます。 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。
TRACEROUTE	「IP アドレス /FQDN」に、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ます。 「Traceroute」をクリックし、トレースルートを実行します。 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。
その他	● LED 点滅 「開始」をクリックすると当該デバイスの LED が赤色で点滅を開始します。 「停止」をクリックすると当該デバイスの LED の点滅が停止します。 点滅する LED は以下の通りです。 • DBA-1210P：ステータス LED • DBA-2520P：Power/Cloud LED • DBA-2620P：Power/Cloud LED • DBA-2720P：Power/Cloud LED • DBA-2820P：Power/Cloud LED • DBA-3621P：Power/Cloud LED • DBA-X2830P：Power/Cloud LED • DBA-X1230P：Power/Cloud LED • DBA-X5480P：Power/Cloud LED ● デバイスの再起動 「再起動」をクリックし、確認ウィンドウで再度「再起動」をクリックするとデバイスは再起動します。

デバイス - ライセンス

デバイスに紐づけられているライセンスの情報を表示します。
ライセンスを追加し、使用期間を延長することもできます。

図 8-33 デバイス - ライセンス

本画面には以下の項目があります。

項目	説明
ライセンス状態	ライセンスが有効状態かを表示します。
ライセンス開始日	ライセンスが有効になった日付を表示します。
ライセンス期限日	ライセンスの有効期限と、残りの有効期間を表示します。
ライセンス表	紐づけられているライセンスの状態とライセンスキーを表示します。 「ライセンスの追加」をクリックし、表示されるウィンドウからライセンスの追加ができます。

■ ライセンスの追加

デバイスにライセンスを追加します。

1. 「ライセンスの追加」をクリックします。

図 8-34 ライセンスの追加

2. ライセンスキーを入力し、「保存」をクリックします。

■ ライセンスの削除

デバイスのライセンスを削除します。

ライセンスの削除は、1 台の AP に 2 つ以上のライセンスが紐づけられている場合に実行できます。

1 台の AP に 2 つ以上のライセンスが紐づけられている場合、1 つのライセンスが使用中となり、それ以外のライセンスは未使用の状態となります。
未使用のライセンスを AP から除外し、別の AP に紐づけたい場合などに使用します。

1. 「アクション」欄で「削除」アイコンをクリックします。
2. 確認画面で「はい」をクリックします。

アクセスポイント - IP ACL

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 設定内で使用）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、ネットワーク宛での通信を、許可・拒否する事が可能になります。

設定 > アクセスポイント > IP ACL をクリックし、以下の画面を表示します。



図 8-35 アクセスポイント - IP ACL

■ IP ACL の追加

1. 「IP ACL の追加」をクリックし、以下の画面を表示します。

IP ACLの追加

IP ACL名*

1-64文字

アクセス権限

アクセスレベル

組織

☒ IP ACLの追加

IPアドレス1*

0.0.0.1

サブネットマスク1*

255.255.255.0

+ 追加

☐ 一括インポート

キャンセル

保存

図 8-36 IP アドレスの追加

2. 以下の項目を設定します。

項目	説明
IP ACL 名	リスト名を入力します。
アクセスレベル	アクセスレベルを「組織」「サイトタグ」「サイト」から選択します。 設定 > アクセスポイント > プロファイル画面の SSID > アクセスコントロールタブで IP ACL を追加する場合は、本項目は表示されません。アクセスレベルは自動的に「組織」になります。
IP アドレスの追加	「IP アドレス」と「サブネットマスク」を設定します。複数入力する場合は「+追加」アイコンをクリックし、枠を増やします。
一括インポート	CSV ファイルで複数の IP アドレスをインポートする場合は、「一括インポート」をクリックし、ファイルを読み込みます。 記載方法の参考のために、CSV ファイルのサンプルをダウンロードすることもできます。 ☒ 一括インポート このデータベースに追加する情報を記載したCSVファイルをアップロードしてください。 リストの最大レコード数は255です。 閲覧 テンプレートファイルのサンプルをダウンロードすることができます。 こちら

3. 「保存」をクリックし、IP ACL を追加します。

■ IP ACL の編集

1. 登録済みの IP アドレスを変更する場合は右側の鉛筆アイコンをクリックします。
2. 以下の画面で「IP アドレス」「サブネットマスク」を設定します。削除する場合は「アクション」欄のごみ箱アイコンをクリックします。

IP ACLの更新 - IP_ACL

アクセス権限

アクセスレベル
組織

検索

#	IP アドレス	サブネットマスク	アクション
1	10.0.0.0	255.0.0.0	

+ 追加

キャンセル 保存

図 8-37 IP ACL の更新

3. 設定後、保存をクリックします。

■ IP ACL のエクスポート

1. 設定 > アクセスポイント > IP ACL 画面で、「アクション」欄の「エクスポート」をクリックします。
2. 登録されている IP アドレス一覧が CSV ファイルでエクスポートされます。

■ IP ACL の削除

IP ACL をリストごと削除します。

1. 設定 > アクセスポイント > IP ACL 画面で、「アクション」欄の「削除」をクリックします。
2. 表示される確認メッセージで「はい」をクリックします。
SSID に紐づけられているリストは削除できません。

認証 - 認証サーバ

認証サーバの追加と設定を行います。
認証サーバは「RADIUS」「LDAP」「POP3」「アクティブディレクトリ」「NT ドメイン」から選択できます。

設定 > 認証 > 認証サーバを選択します。



図 8-38 認証 - 認証サーバ

本画面には以下の項目があります。

項目	説明
認証サーバ	追加する認証サーバをドロップダウンリストで選択します。 「RADIUS」「LDAP」「POP3」「アクティブディレクトリ」「NT ドメイン」から選択できます。
サーバ名	認証サーバの名前を表示します。
タイプ	認証サーバのタイプを表示します。
アクセスレベル	アクセスレベルを表示します。
IP アドレス	認証サーバの IP アドレスを表示します。
ポート	RADIUS サーバ、LDAP サーバ、POP3 サーバ、アクティブディレクトリのポート番号を表示します。
暗号化	LDAP サーバ、POP3 サーバの暗号化の設定を表示します。
関連デバイス	認証サーバを使用しているデバイスの数を表示します。 リンクをクリックするとデバイスのリストが表示されます。
関連プロファイル	認証サーバを使用しているプロファイルの数を表示します。 リンクをクリックするとプロファイルのリストが表示されます。
アクション	認証サーバの編集、削除を行います。 プロファイルやデバイスが関連付けられている認証サーバは削除できません。

■ 認証サーバの追加

- 「認証サーバ」のドロップダウンリストで認証サーバを選択し、「追加」をクリックします。
- 表示される画面で認証サーバの設定を行います。
画面は選択したサーバのタイプによって異なります。詳細は以下の項目を参照してください。
[「認証 - 認証サーバ - RADIUS サーバの追加」](#)
[「認証 - 認証サーバ - LDAP サーバの追加」](#)
[「認証 - 認証サーバ - POP3 サーバの追加」](#)
[「認証 - 認証サーバ - アクティブディレクトリの追加」](#)
[「認証 - 認証サーバ - NT ドメインサーバの追加」](#)
- 「保存」をクリックし、サーバを追加します。

■ 認証サーバの検索

画面右端の「検索」で、表示する認証サーバを検索できます。
以下の画面で「タイプ」「サーバ名」「IP アドレス」を指定します。

タイプ:

全て

サーバ名:

IP アドレス:

図 8-39 認証サーバの検索

認証 - 認証サーバ - RADIUS サーバの追加

認証に使用する RADIUS サーバを追加します。

1. 設定 > 認証 > 認証サーバ画面の「認証サーバ」ドロップダウンリストで「RADIUS サーバ」を選択し、「追加」をクリックします。
2. 以下の画面で設定を行います。

RADIUSサーバの追加

サーバ名 *
1-64文字

IP アドレス *
例 10.90.90.90

ポート *
1812

シークレット *
2-32 文字

認証方法 ?
CHAP

RADIUS アカウンティング *
☒ Enable ☐ Disable

IP アドレス *
例 10.90.90.90

ポート *
1813

シークレット *
2-32 文字

Accounting interim interval *
300 秒

アクセス権限
アクセスレベル
組織

キャンセル保存

図 8-40 RADIUS サーバの追加

本画面には以下の項目があります。

項目	説明
サーバ名	RADIUS サーバの名前を入力します。
IP アドレス	RADIUS サーバの IP アドレスを入力します。
ポート	RADIUS 認証に使用するポート番号を入力します。初期値は 1812 です。
シークレット	シークレットを 2-32 文字の範囲で入力します。
認証方法	認証方法を以下から選択します。 ・ 選択肢：「PAP」「CHAP」「MS-CHAP」「MS-CHAPv2」「EAP-MD5」 注意 「認証方法」の設定には以下の制限があります。 ・ DBG シリーズのキャプティブポータル、または MAC フィルタリングでのみ有効です。 ・ DBA シリーズ、DBS シリーズでは未サポートのため、設定しても反映されません。
RADIUS アカウンティング	
RADIUS アカウンティング	RADIUS アカウンティングを有効 / 無効に設定します。 RADIUS アカウンティングを有効にすると、接続時間や送受信したパケットの量などをユーザごとに記録できます。
IP アドレス	RADIUS アカウンティングに使用する IP アドレスを入力します。
ポート	RADIUS アカウンティングに使用するポート番号を入力します。初期値は 1813 です。
シークレット	シークレットを 2-32 文字の範囲で入力します。
Accounting interim interval	RADIUS アカウンティングサーバへ Interim パケットを送信する間隔を、300-3600（秒）の範囲で指定します。 Interim パケットの送信により、AP は RADIUS サーバに対しアカウンティング情報をアップデートします。
アクセス権限	
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。 設定 > アクセスポイント > プロファイル画面の SSID > アクセスコントロールタブで RADIUS サーバを追加する場合は、本項目は表示されません。アクセスレベルは自動的に「組織」になります。

3. 「保存」をクリックし、サーバを追加します。

認証 - 認証サーバ - LDAP サーバの追加

認証に使用する LDAP サーバを追加します。

- 1. 設定 > 認証 > 認証サーバ画面の「認証サーバ」ドロップダウンリストで「LDAP サーバ」を選択し、「追加」をクリックします。
- 2. 以下の画面で設定を行います。

LDAPサーバの追加

サーバ名*

1-64 文字

IP アドレス*

例 10.90.90.90

ポート* ?

389

Base DN*

例 ou=dlink,dc=nuclias,dc=com

暗号化

無効

アクセス権限

アクセスレベル

組織

キャンセル

保存

図 8-41 LDAP サーバの追加

本画面には以下の項目があります。

項目	説明
サーバ名	LDAP サーバの名前を入力します。
IP アドレス	LDAP サーバの IP アドレスを入力します。
ポート	LDAP 認証に使用するポート番号を入力します。 LDAP リスニングポートは通常 389、SSL 経由の場合は 636 です。
Base DN	Base DN を入力します。
暗号化	暗号化の設定を「無効」「SSL」「TLS」から選択します。
アクセス権限	
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。

- 3. 「保存」をクリックし、LDAP サーバを追加します。

認証 - 認証サーバ - POP3 サーバの追加

認証に使用する POP3 サーバを追加します。

注意 本機能は未サポートです。

- 1. 設定 > 認証 > 認証サーバ画面の「認証サーバ」ドロップダウンリストで「POP3 サーバ」を選択し、「追加」をクリックします。
- 2. 以下の画面で設定を行います。

POP3サーバの追加

サーバ名*

1-64文字

IPアドレス*

例 10.90.90.90

ポート*

110

暗号化

無効

アクセス権限

アクセスレベル

組織

キャンセル

保存

図 8-42 POP3 サーバの追加

本画面には以下の項目があります。

項目	説明
サーバ名	POP3 サーバの名前を入力します。
IP アドレス	POP3 サーバの IP アドレスを入力します。
ポート	POP3 サーバ認証に使用するポート番号を入力します。初期値は 110 です。
暗号化	暗号化の設定を「無効」「SSL」から選択します。
証明書	「SSL」を選択した場合は、証明書を選択します。
アクセス権限	
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。

- 3. 「保存」をクリックし、POP3 サーバを追加します。

認証 - 認証サーバ - アクティブディレクトリの追加

認証に使用するアクティブディレクトリサーバを追加します。

注意 本機能は未サポートです。

- 1. 設定 > 認証 > 認証サーバ画面の「認証サーバ」ドロップダウンリストで「アクティブディレクトリ」を選択し、「追加」をクリックします。
- 2. 以下の画面で設定を行います。

アクティブディレクトリの追加

サーバ名*

1-64 文字

IP アドレス*

例 10.90.90.90

ポート*

1-65535

AD ドメイン*

例 Dlink.com

ホスト名*

1-128 文字

アクセス権限

アクセスレベル

組織

キャンセル

保存

図 8-43 アクティブディレクトリの追加

本画面には以下の項目があります。

項目	説明
サーバ名	アクティブディレクトリサーバの名前を入力します。
IP アドレス	アクティブディレクトリサーバの IP アドレスを入力します。
ポート	アクティブディレクトリサーバ認証に使用するポート番号を 1-65535 の範囲で入力します。
AD ドメイン	アクティブディレクトリのドメインを入力します。
ホスト名	ホスト名を 1-128 文字で入力します。
アクセス権限	
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。

- 3. 「保存」をクリックし、アクティブディレクトリサーバを追加します。

認証 - 認証サーバ-NT ドメインサーバの追加

認証に使用する NT ドメインサーバを追加します。

注意 本機能は未サポートです。

- 1. 設定 > 認証 > 認証サーバ画面の「認証サーバ」ドロップダウンリストで「NT ドメインサーバ」を選択し、「追加」をクリックします。
- 2. 以下の画面で設定を行います。

NTドメインサーバの追加

サーバ名*

1-64 文字

IP アドレス*

例 10.90.90.90

ワークグループ*

例 DlinkGroup

アクセス権限

アクセスレベル

組織

キャンセル

保存

図 8-44 NT ドメインサーバの追加

本画面には以下の項目があります。

項目	説明
サーバ名	NT ドメインサーバの名前を入力します。
IP アドレス	NT ドメインサーバの IP アドレスを入力します。
ワークグループ	NT ドメインサーバ認証に使用するワークグループを入力します。
アクセス権限	
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。

- 3. 「保存」をクリックし、NT ドメインサーバを追加します。

認証 - ローカル認証 DB

本項目は、キャプティブポータル ローカルデータベース 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「ユーザ名」「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「ユーザ名」「パスワード」は AP に転送され、AP がローカルでユーザ認証を行うため Nuclias 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。

設定 > 認証 > ローカル認証 DB を選択します。



図 8-45 認証 - ローカル認証 DB

本画面には以下の項目があります。

項目	説明
名前	ローカル認証データベースの名前を表示します。
アクセスレベル	アクセスレベルを表示します。
エントリ	データベースに登録されているエントリの数を表示します。
関連デバイス	ローカル認証データベースを使用しているデバイスの数を表示します。 リンクをクリックするとデバイスのリストが表示されます。
関連プロファイル	ローカル認証データベースを使用しているプロファイルの数を表示します。 リンクをクリックするとプロファイルのリストが表示されます。
アクション	ローカル認証データベースの編集、エクスポート、削除を行います。 プロファイルやデバイスが関連付けられているデータベースは削除できません。

■ ローカル認証データベースの追加

1. 「ローカル認証 DB の追加」をクリックし、以下の画面を表示します。

ローカル認証DBの追加

ローカル認証名*

1-64文字

アクセス権限

アクセスレベル

組織

☒ ローカル認証DBの追加

ユーザ名*

パスワード*

1-63文字

追加

☐ 一括インポート

キャンセル

保存

図 8-46 ローカル認証 DB の追加

2. 以下の項目を設定します。

項目	説明
ローカル認証名	ローカル認証データベースの名前を 1-64 文字で入力します。
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。
ユーザ名	ローカル認証に使用するユーザ名を入力します。「追加」をクリックすると複数のエントリを追加できます。
パスワード	ローカル認証に使用するパスワードを入力します。「追加」をクリックすると複数のエントリを追加できます。
一括インポート	CSV ファイルで複数のローカルユーザ情報をインポートする場合は、「一括インポート」をクリックし、ファイルを読み込みます。記載方法の参考のために、CSV ファイルのサンプルをダウンロードすることもできます。

3. 「保存」をクリックし、ローカル認証データベースを保存します。

■ ローカル認証 DB リストのエクスポート

1. **設定 > 認証 > ローカル認証 DB** 画面で「アクション」欄の「エクスポート」をクリックします。
2. 登録されているローカル認証 DB リストが CSV ファイルでエクスポートされます。

■ ローカル認証データベースの編集

1. 「アクション」欄の「編集」をクリックします。
2. 以下の画面で「ユーザ名」「パスワード」を編集します。

ローカル認証DBの編集 - database

アクセス権限

アクセスレベル

組織

追加

検索

#	ユーザ名	パスワード	アクション
1	user		

前 1 次 10

キャンセル 保存

図 8-47 ローカル認証 DB の更新

3. 「保存」をクリックします。

■ ローカル認証データベースの削除

1. **設定 > 認証 > ローカル認証 DB** 画面で「アクション」欄の「削除」をクリックします。
2. 表示される確認メッセージで「はい」をクリックします。

注意 プロファイルやデバイスが関連付けられているデータベースは削除できません。

MAC ACL

本項目は、MAC アドレス フィルタリング機能で使用する MAC アドレスの作成・管理のために使用します。
MAC フィルタリング機能（SSID 設定内で使用）を有効にすることで、MAC アドレスデータベースに登録した MAC アドレスからの通信を、許可・拒否する事が可能になります。

設定 > MAC ACL をクリックし、以下の画面を表示します。



図 8-48 MAC ACL

■ MAC ACL の追加

1. 「MAC ACL の追加」をクリックし、以下の画面を表示します。



図 8-49 MAC ACL の追加

2. 以下の項目を設定します。

項目	説明
MAC ACL 名	リスト名を入力します。
アクセスレベル	アクセスレベルを「組織」「サイトタグ」「サイト」から選択します。 設定 > アクセスポイント > プロファイル画面の SSID > アクセスコントロールタブで MAC ACL を追加する場合は、本項目は表示されません。アクセスレベルは自動的に「組織」になります。
MAC アドレスの追加	「MAC アドレス」と「ユーザ名」を入力します。 複数入力する場合は「+追加」アイコンをクリックし、枠を増やします。
一括インポート	CSV ファイルで複数の IP アドレスをインポートする場合は、「一括インポート」をクリックし、ファイルを読み込みます。 記載方法の参考のために、CSV ファイルのサンプルをダウンロードすることもできます。 一括インポート このデータベースに追加する情報を記載したCSVファイルをアップロードしてください。 リストの最大レコード数は2000です。 閲覧 テンプレートファイルのサンプルをダウンロードすることができます。 こちら

3. 「保存」をクリックし、MAC ACL を追加します。

■ MAC ACL の編集

登録済みの MAC ACL を編集します。

1. 「アクション」欄の「編集」をクリックします。
2. 以下の画面で「MAC アドレス」「ユーザ名」を設定します。削除する場合は「アクション」欄のゴミ箱アイコンをクリックします。

MAC ACLの更新 - MAC_ACL

アクセス権限

アクセスレベル

組織

追加

検索

#	MAC アドレス	ユーザ名	アクション
1	01:23:45:67:89:AB	1-64文字	🗑️
2	AB:CD:AB:CD:AB:CD	1-64文字	🗑️

前 1 次 10

キャンセル 保存

図 8-50 MAC ACL の更新

3. 設定後、「保存」をクリックします。

■ MAC ACL のエクスポート

1. 設定>アクセスポイント>MAC ACL 画面で、「アクション」欄の「エクスポート」をクリックします。
2. 登録されている IP アドレス一覧が CSV ファイルでエクスポートされます。

■ MAC ACL の削除

MAC ACL をリストごと削除します。

1. 設定>アクセスポイント>MAC ACL 画面で、「アクション」欄の「削除」をクリックします。
2. 表示される確認メッセージで「はい」をクリックします。
但し SSID に紐づけられているリストは削除できません。

ウォールドガーデン

ウォールドガーデンでは、" キャプティブポータルが設定された SSID " にアクセスしたユーザが、キャプティブポータルの認証なしでアクセスできるホスト名または IP アドレスを指定します。キャプティブポータルでの認証が完了していないユーザは、指定したホスト名または IP アドレスにのみアクセス可能となるため、認証されていないユーザのインターネットへのアクセスを制限できます。

注意 ウォールドガーデンでは、「http」のページにはアクセスできません。
「https」でアクセスできるページを指定してください。

注意 AP の管理 VLAN と SSID VLAN が異なっている場合、ウォールドガーデンが動作しません。

ウォールドガーデンを使用するには、以下の設定を行います。

- ①**設定 > ウォールドガーデン**画面で、ユーザが認証なしでアクセスできるページのホスト名または IP アドレスを設定します。
- ②キャプティブポータルでウォールドガーデンを有効にします。
キャプティブポータルで「クリックスルー」を選択した場合はウォールドガーデンを使用できません。

参照 キャプティブポータルの設定については、「[プロファイル-SSID-キャプティブポータルタブ](#)」を参照してください。

設定 > ウォールドガーデンを選択します。
以下の画面に設定したウォールドガーデンが表示されます。

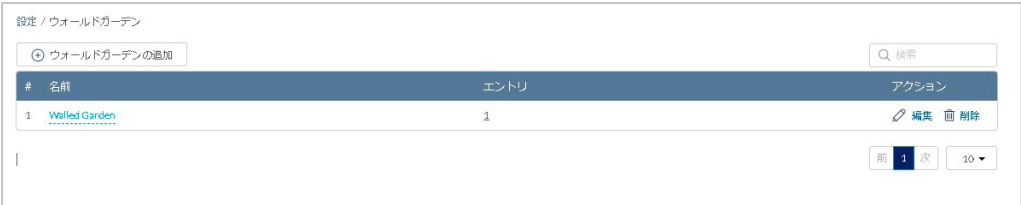


図 8-51 ウォールドガーデン

■ ウォールドガーデンの追加

1. 「ウォールドガーデンの追加」をクリックし、以下の画面を表示します。

図 8-52 ウォールドガーデンの追加

2. 以下の項目を設定します。

項目	説明
ウォールドガーデン名	ウォールドガーデンの名前を 1-64 文字で入力します。
レンジ	ウォールドガーデンの範囲をホスト名または IP アドレスで入力します。 最大 20 までのホスト名または IP アドレスを入力できます。 欄を追加する場合は「追加」をクリックします。

3. 「保存」をクリックし、ウォールドガーデンを追加します。

■ ウォールドガーデンの編集

1. 「アクション」欄の「編集」をクリックし、編集を行います。
削除する場合は「アクション」欄の「削除」をクリックします。



図 8-53 ウォールドガーデンの更新

2. 設定後、「適用」をクリックします。

■ ウォールドガーデンの削除

1. 設定 > アクセスポイント > ウォールドガーデン画面で「アクション」欄の「削除」をクリックします。
2. 確認画面で「はい」をクリックします。
但し SSID に紐づけられているウォールドガーデンは削除できません。

スケジュールポリシー

本画面では、プロファイルおよびデバイスに適用するスケジュールポリシーを作成できます。

設定 > スケジュールポリシーを選択します。



図 8-54 設定 - スケジュールポリシー

本画面には以下の項目があります。

項目	説明
スケジュール名	スケジュールポリシーの名前を表示します。
アクセスレベル	スケジュールポリシーのアクセスレベルを表示します。
タイプ	スケジュールの種類を表示します。
スケジュール	「View」のリンクをクリックすると、各スケジュールの詳細が表示されます。
関連デバイス	スケジュールを使用しているデバイスの数を表示します。 リンクをクリックするとデバイスのリストが表示されます。
関連プロファイル	スケジュールを使用しているプロファイルの数を表示します。 リンクをクリックするとプロファイルのリストが表示されます。
アクション	スケジュールポリシーの編集と削除を行います。 プロファイルやデバイスが関連付けられているスケジュールは削除できません。 デフォルトのスケジュールの編集と削除はできません。

■ スケジュールポリシーの追加

1. 設定 > スケジュールポリシー画面で「スケジュールポリシーの追加」をクリックし、以下の画面を表示します。

スケジュールポリシーの追加

名前
1-64文字

アクセス権限
アクセスレベル
組織

スケジュール
タイプ
☒ スケジュール ☐ 再起動

テンプレート
常にオン

24時間 AM/PM

曜日	利用可能状態	から	まで	時刻表示
日曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
月曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
火曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
水曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
木曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
金曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00
土曜日	☒ オン ☐ オフ	00:00	- 24:00	00:00 24:00

キャンセル 保存

図 8-55 スケジュールポリシーの追加

2. 「名前」「アクセス権限」を設定し、各曜日のスケジュールを設定します。

「アクセスレベル」は「組織」「サイト」「サイトタグ」から選択します。「サイト」「サイトタグ」を選択した場合は、「管理サイト」と「管理サイトタグ」を選択します。

「テンプレート」のドロップダウンリストでスケジュールテンプレートを選択することもできます。

注意 「再起動」項目は未サポートです。

3. 「保存」をクリックし、スケジュールポリシーを保存します。

■ スケジュールポリシーの削除

1. 設定 > スケジュールポリシー画面で「アクション」欄の「削除」をクリックします。
2. 確認画面で「はい」をクリックします。

注意 プロファイルやデバイスが関連付けられているスケジュールポリシーは削除できません。

■ スケジュールポリシーの編集

1. 設定 > スケジュールポリシー画面で「アクション」欄の「編集」をクリックします。
2. スケジュールを編集し、「保存」をクリックします。

注意 デフォルトのスケジュールポリシーは編集できません。

スプラッシュページ

キャプティブポータルで使用するスプラッシュページの作成、編集を行います。
クライアントがインターネットに接続する際に、ここで作成したスプラッシュページが表示されます。

設定 > スプラッシュページを選択します。



図 8-56 スプラッシュページ

■ スプラッシュページの追加

1. 設定 > スプラッシュページ画面で「スプラッシュページの追加」をクリックし、以下の画面を表示します。

×

スプラッシュページの追加

スプラッシュ名*

My new splash page template

スタイル

テンプレート

アクセス権限

アクセスレベル

組織

ベース

デフォルト

キャンセル

次

図 8-57 スプラッシュページの追加

2. 以下の項目を設定します。

項目	説明
スプラッシュ名	スプラッシュページの名前（1-64 文字）を入力します。
スタイル	スプラッシュページを作成する方法を選択します。 ・「テンプレート」：テンプレートを使用してスプラッシュページを作成します。
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」 から選択します。
ベース	作成済みのスプラッシュページをベースとする場合は、ドロップダウンリストから選択します。 「デフォルト」を選択するとデフォルトのスプラッシュページがベースになります。

3. 「次」をクリックし、スプラッシュページを編集します。
編集方法については「[スプラッシュページの編集（テンプレート）](#)」を参照してください。
4. 「保存」をクリックし、スプラッシュページを保存します。

■ スプラッシュページの削除

設定 > スプラッシュページ画面で、アクション欄のごみ箱アイコンをクリックします。

■ スプラッシュページの編集（テンプレート）

テンプレートを使用してスプラッシュページの編集を行います。



図 8-58 スプラッシュページ編集（テンプレート）

本画面には以下の項目があります。

項目	説明
スプラッシュ名	スプラッシュページの名前（1-64 文字）を入力します。
ユースケースでのプレビューと編集	ドロップダウンからスプラッシュページのユースケースを選択します。 詳細は「 スプラッシュページのユースケースの選択 」を参照してください。
	アイコンをクリックし、画面サイズを選択します。 アイコンは左から順に「PC」「タブレット」「スマートフォン」です。
	「プレビュー」を選択すると、プレビューモードに切り替わり、実際に表示される画面を確認できます。 「編集」を選択すると、編集モードに切り替わります。
ログイン	「ログイン」タブを選択すると、ログイン画面の編集を行うことができます。
メッセージ	「メッセージ」タブを選択すると、スプラッシュページに表示するメッセージを編集できます。
規約	無線クライアントがキャプティブポータルの SSID に接続した際に閲覧する利用規約を編集できます。
複数の言語	スプラッシュページに使用する言語を追加できます。 詳細は「 スプラッシュページに複数言語を追加 」を参照してください。
	表示言語を切り替えます。「複数の言語」で選択した言語が選択肢として表示されます。

● スプラッシュページ（テンプレート）の編集方法

編集したい箇所にカーソルをあてると鉛筆のアイコンが表示されます。
表示される内容に従い、テキストの編集や画像の変更を行います。



図 8-59 スプラッシュページ編集（テンプレート）の例

第8章 デバイス設定

● スプラッシュページのユースケースの選択

スプラッシュページの使用例（ユースケース）を選択します。
サインオン方法のほかに、セッション制限の警告ページ、Web コンテンツフィルタの警告ページも選択できます。



図 8-60 ユースケースの選択

● スプラッシュページに複数言語を追加

「複数の言語」をクリックし、スプラッシュページを表示する言語を追加できます。



図 8-61 複数言語の追加

本画面には以下の項目があります。

項目	説明
複数言語に対応	チェックをいれると、複数言語に対応したスプラッシュページを作成できます。
デフォルト言語	スプラッシュページを表示した際、最初に表示される言語を選択します。
対応言語の追加	スプラッシュページに表示する言語を追加します。 ドロップダウンリストから言語を選択し、「追加」をクリックします。
対応言語	スプラッシュページに表示できる言語が表示されます。 また、言語のアイコンをクリックし、対応言語を削除できます。グレーアウトしているアイコンの言語は削除できません。

設定後「はい」をクリックし、設定を保存します。

第9章 レポート

- 変更ログ
- サマリレポート
- アラート
- ライセンス (レポート)

変更ログ

設定変更のログを表示します。

レポート>変更ログを選択してください。

レポート / 変更ログ

タイムフレーム: 最近24時間

検索

#	時間	アカウント	サイト	プロファイル	SSID	ページ	デバイス名	ラベル	古い値
1	2022/05/30 15:49:56	huykhtaiquykhetai1@gmail.com						Login successful	
2	2022/05/30 13:28:59	huykhtaiquykhetai1@gmail.com						Login successful	
3	2022/05/30 10:41:41	huykhtaiquykhetai1@gmail.com						Login successful	
4	2022/05/30 09:18:00	huykhtaiquykhetai1@gmail.com	2520P	DBA-1210P			huykhtaiquykhetai1 (huykhtaiquykhetai1)	Configuration Pushed	
5	2022/05/30 09:17:57	huykhtaiquykhetai1@gmail.com		DBA-1210P	5GHz	SSID		SSID Captive Portal change	["captivePortal": {"enable": true, "aut
6	2022/05/30 09:09:38	huykhtaiquykhetai1@gmail.com	2520P	DBA-1210P			huykhtaiquykhetai1 (huykhtaiquykhetai1)	Configuration Pushed	
7	2022/05/30 09:09:34	huykhtaiquykhetai1@gmail.com		DBA-1210P	5GHz	SSID		SSID Captive Portal change	["captivePortal": {"e
8	2022/05/30 09:05:35	huykhtaiquykhetai1@gmail.com						Login successful	

8 エントリ 検索開始日: 2022/05/29

前

1

次

10

図 9-1 変更ログ

■ 表示する期間の変更

「タイムフレーム」で表示する期間を設定します。

■ ログのダウンロード



をクリックし、ログを CSV 形式でダウンロードします。

■ ログの検索

特定の文字列を含むログを検索する場合は、検索ウィンドウに文字を入力します。

検索ウィンドウ右側の▼をクリックして詳細な検索ウィンドウを表示させ、より精度の高い検索を行うこともできます。

本画面には以下の項目が表示されます。

項目	説明
時間	設定変更を実施した時間を表示します。
アカウント	使用されたアカウント（メールアドレス表示）を表示します。
サイト	サイトに関係する設定変更の場合、そのサイトを表示します。
プロファイル	プロファイルに関係する設定変更の場合、そのプロファイルを表示します。
SSID	SSID に関係する設定変更の場合、その SSID を表示します。
ページ	設定項目を表示します。
デバイス名	デバイスに関係する設定変更の場合、そのデバイスを表示します。
ラベル	変更内容を表示します。
古い値	更新箇所における、更新前の設定値を表示します。
新しい値	更新箇所における、更新後の設定値を表示します。

サマリレポート

サイトごと、デバイスごとなどにレポートを表示できます。
レポート>サマリレポートを選択してください。

レポート / サマリレポート

サイト:

製品カテゴリ:

カスタマイズ:

上位結果の表示:

タイムフレーム:

全てのサイト

全て

全て

5

最近24時間

プレビュー

Eメール

ダウンロード

図 9-2 サマリレポート

本画面には以下の項目があります。

項目	説明
サイト	表示するサイトを「全てのサイト」「単独のサイト」「サイトタグ付きのサイト」から検索します。
製品カテゴリ	レポートを表示する製品のカテゴリを「アクセスポイント」「スイッチ」「ゲートウェイ」から選択します。
カスタマイズ	サマリレポートに表示する項目を選択します。
上位結果の表示	上位何番目までをサマリレポートに表示するかを指定します。
タイムフレーム	直近のどのくらいの期間の情報を表示、閲覧するかを指定します。
プレビュー	設定した対象のレポートを表示します。
Eメール	メールアドレスを入力し、レポートをメール送信します。HTML形式で送信されます。
ダウンロード	レポートをエクセル (xlsx) ファイルでダウンロードします。

「プレビュー」をクリックすると、以下のようにサマリレポートが表示されます。

レポート / サマリレポート

最近24時間からのサマリレポート

サイト:

製品カテゴリ:

カスタマイズ:

上位結果の表示:

タイムフレーム:

全てのサイト

1 選択済

全て

5

最近24時間

プレビュー

Eメール

ダウンロード

アクセスポイント

上位アクティブアクセスポイント

#	モデル	デバイス名	UID	MAC アドレス	使用量	使用量(%)
データがありません						

上位アクティブSSID

#	SSID	使用量	使用量(%)
データがありません			

上位アクティブWi-Fiクライアント

#	MAC アドレス	ベンダー	使用量	使用量(%)
データがありません				

図 9-3 サマリレポート（プレビュー） - アクセスポイント

アラート

検知したアラートを表示します。

レポート>アラートを選択、または画面右上部の  「アラート」を選択してください。

注意 本ページでアラートとして表示されるイベントは、事前に**管理>アラート設定**で設定されている必要があります。詳細は「[アラート設定](#)」をご確認ください。



図 9-4 アラート

本画面には以下の項目が表示されます。

項目	説明
重大性	アラートの重大性を「重大」「警告」「情報」で表示します。
時間	アラートが発生した日時を表示します。
デバイスタイプ	デバイスタイプを表示します。
デバイス名	事象の発生したデバイスの名前を表示します。
MAC アドレス	デバイスの MAC アドレスを表示します。
内容	発生した事象の詳細を表示します。

■ アラートの処理

アラート画面は「未確認」と「確認済」の2つのタブから構成されています。

最初、全てのアラートは「未確認」に表示されています。

「未確認」タブで左側のチェックボックスにチェックを入れ、「確認」をクリックすると、アラートは「確認済」タブに移動します。

「確認済」タブで同様にチェックボックスにチェックを入れ、「削除」をクリックすると、アラートは Nuclias 上から削除されます。

「未確認」タブにアラートがある場合は、アラートマークに「！」が表示されます。



アラートマーク

■ アラートの検索

検索ウィンドウ右側の  をクリックして詳細な検索ウィンドウを表示させ、精度の高い検索を行うことができます。

ライセンス（レポート）

ライセンスの使用状況を確認することができます。
レポート>ライセンスを選択します。



図 9-5 ライセンス

本画面には以下の項目が表示されます。

項目	説明
組織名	組織名を表示します。
デバイス名	デバイス名を表示します。
MAC アドレス	デバイスの MAC アドレスを表示します。
デバイス UID	デバイスの UID を表示します。
シリアル番号	デバイスのシリアル番号を表示します。
モデル名	デバイスのモデル名を表示します。
プロファイル名	デバイスが紐づいているプロファイルを表示します。
登録ステータス	Nuclias への登録状況を表示します。
ライセンス状態	ライセンスのステータスを表示します。
ライセンス数量	ライセンスの数を表示します。
ライセンスキー	ライセンスキーを表示します。
登録日	ライセンスの登録日を表示します。
期限日	ライセンスの期限日を表示します。
最終閲覧	デバイスの最終オンライン接続日時を表示します。
ファームウェア	デバイスのファームウェアバージョンを表示します。

■ ライセンスレポートの検索

特定の文字列を含むライセンスのレポートを検索する場合は、検索ウィンドウに文字を入力します。

■ ライセンス情報のダウンロード

をクリックすると、ライセンスの情報を CSV 形式でダウンロードできます。

第 10 章 管理

- アカウント管理
- 組織管理
- ライセンス管理
- インベントリ
- ファームウェア
- アラート設定
- 証明書の管理
- アドバンスト設定 > SAML 設定
- アドバンスト設定 > SMS 設定
- アドバンスト設定 > シスログサーバ 設定
- デバイスの追加
- デバイス一括インポート

アカウント管理

ユーザ情報の管理ができます。
管理 > アカウント管理を選択してください。



図 10-1 アカウント管理

本画面には以下の項目があります。

項目	説明
名前	ユーザ名を表示します。ユーザ名をクリックすると、「ユーザ名」「アクセス権限」「管理サイト」を変更できます。ログインしているユーザ自身の権限は変更できません。
E メール	使用しているメールアドレスを表示します。
アクセスレベル	アクセスレベルと、閲覧できる組織、サイトを表示します。
役割	アカウントの権限を表示します。
管理サイト	アクセス可能な組織やサイトの数を表示します。
状態	ユーザアカウントのステータスを表示します。 招待メール送信後、有効化前の場合は「未確認」と表示され、メールアドレスの変更やメールの再送を行うことができます。
最終接続日時	最後にログインした日時を表示します。

■ アカウントの検索

右上の検索ウィンドウで、「名前」「E メール」「役割」からアカウントを検索できます。

■ ユーザの招待

「ユーザを招待する」をクリックし、管理下の組織に新たなユーザを作成、招待します。特定のサイトタグやサイトのみに閲覧権限を持たせたユーザを作成することも可能です。

名前、E メールアドレス、アクセス可能なサイトタグやサイト、並びに役割を設定します。
ユーザ名は、アクティベーション後にユーザ自身で変更できます。

注意 既に Nuclias アカウントで使用中のメールアドレスを招待することはできません。

ユーザを招待する

名前*

1-64文字

Eメールアドレス*

1-128文字

このメールアドレスはNucliasへのログインや、各種情報を受け取るために使用されます。

アクセス権限

役割*

管理者

アクセスレベル*

組織

DJP_画面確認用

管理サイト

全てのサイト

全て

閉じる

送信

図 10-2 ユーザを招待する

アクセス権限の説明は以下のとおりです。

項目	説明
管理者	全ての設定の閲覧、追加、編集、削除が可能です。
編集者	ほぼ全ての設定の閲覧、編集が可能です。 ただしユーザやデバイス、設定情報などの追加または削除の作業を行うことはできません。
モニタ	Wi-Fi ポリシーなどの設定を確認することはできません。 また、ユーザやライセンスなどの管理設定は、閲覧のみが可能です。変更することはできません。
モニタ閲覧者	デバイスやサイトの使用状況やステータスのみ閲覧することができます。

入力後「送信」をクリックし、記載したE メールアドレスへ招待メールを送信します。

■ ユーザの削除

削除するユーザアカウントのチェックボックスにチェックを入れ、「削除」をクリックします。
パスワード入力画面が表示されるので、作業者自身のパスワードを入力し、「はい」をクリックします。

ユーザが正常に削除されると、画面はログイン画面に移行し、削除アカウントのメールアドレスに削除された旨の通知が送付されます。

注意 ユーザを削除した場合、そのユーザに関連する情報もあわせて削除されます。

組織管理

組織、サイト、サイトタグの管理と、ユーザの招待を行うことができます。

管理 > 組織管理を選択し、以下の画面を表示します。



図 10-3 組織管理

項目	説明
組織	組織名を表示します。 クリックすると、組織、サイト、サイトタグがツリー表示されます。 ツリー表示の画面からサイトやサイトタグを作成、編集できます。
タイプ	組織の属性を表示します。
サイト	登録されているサイトの数を表示します。 マウスカーソルを合わせると、登録されているサイトが表示されます。
サイトタグ	登録されているサイトタグの数が表示されます。
デバイス	登録されているデバイスの状況と数を表示します。
アクセスポイント	登録されているアクセスポイントの状況と数を表示します。
スイッチ	登録されているスイッチの状況と数を表示します。
ゲートウェイ	登録されているゲートウェイの状況と数を表示します。
アクション	以下の項目をクリックし、設定を行います。 「編集」：組織の編集を行います。 「サイトの作成」：サイトの作成を行います。 「サイトタグの作成」：サイトタグの作成を行います。 「ユーザを招待する」：ユーザを招待します。

■ ツリー表示画面

管理 > 組織管理画面で「組織」欄の組織名をクリックすると、サイトやサイトタグがツリー表示された画面が表示されます。
ページ右上から「サイトの作成」「サイトタグの作成」を選択できます。
また、サイト名とサイトタグ名を入力し、検索を行うことができます。

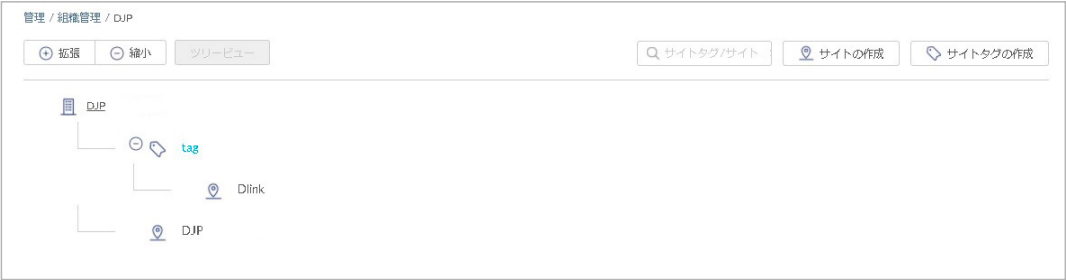


図 10-4 組織管理 - ツリー表示

サイト名とサイトタグ名で検索を行った場合は、以下の画面が表示されます。
検索後、ツリー表示に戻す場合は「ツリービュー」をクリックします。



図 10-5 組織管理 - 検索

■ 組織の編集

1. 管理 > 組織管理 画面でアクション欄の「編集」をクリックし、以下の画面を表示します。

組織の編集

組織画像のアップロード

組織名*

Nuclias_Manual

画像をここにドラッグ&ドロップ
してください

または

ファイルの閲覧

最大1MBの、PNGまたはJPGのファイル
をアップロードできます。

連絡先情報

名前

1-64文字

電話

1-32文字

Eメールアドレス

1-128文字

閉じる

保存

図 10-6 組織の編集

2. 「組織名」と「連絡先情報」を編集します。
また、「組織画像のアップロード」では、画像ファイルをアップロードできます。
「ファイルの閲覧」をクリックし、アップロードするファイルを選択します。（ファイル形式：PNG または JPEG、サイズ：最大 1 MB）
3. 「保存」をクリックし、設定を保存します。

■ サイトの作成

1. 「サイトの作成」をクリックし、以下の画面を表示します。

サイトの作成

サイト名*

1-64文字

サイトタグ

None

国・地域のタイムゾーン*

Japan

Asia/Tokyo(UTC+09:00, ...)

選択したタイムゾーンによって、ファームウェアのアップグレードやログの時間が決まります
のでご注意ください。また、選択した国のWi-Fi規制（6GHz帯など）にもご注意ください。

住所

デバイス資格情報

デバイス資格情報のユーザ名とパスワードは、ローカルのWebページからログインする際
に使用されます。パスワードの長さは8～64文字に設定する必要があります。

ユーザ名

admin

パスワード*

NTP情報

NTPサーバ 1*

ntp.nuclias.com

NTPサーバ 2

連絡先情報

名前

1-64文字

電話

1-32文字

Eメールアドレス

1-128文字

閉じる

適用

図 10-7 サイトの作成

2. 以下の項目を入力、選択します。

- 「サイト名」を入力
- 「国・地域のタイムゾーン」から「Japan」を選択

NTP サーバ、連絡先情報は初期状態で問題ありません（必要に応じて変更、入力してください）。

注意 NTP サーバの設定が正しくない場合、イベントログが正常に取得できません。

「ユーザ名」と「パスワード」は、デバイスに Web GUI でローカル接続する際のユーザ名 / パスワード情報です。

ユーザ名は「管理者」(admin) で固定されており、変更できません。

パスワードは変更可能です。初期状態ではサイトごとにランダムな 8 文字が設定されています。パスワードを変更する場合は、パスワード欄に文字を入力します。目のアイコンをクリックするとパスワードの表示 / 非表示を切り替えられます。

3. 「適用」をクリックし、設定を保存します。

■ サイトタグの作成

「サイトタグ」を使うと、複数のサイトをまとめて管理することができます。またタグ同士で親子関係の設定を行うことができます。

1. 「サイトタグの作成」をクリックし、以下の画面を表示します。

図 10-8 サイトタグの作成

2. タグの名前、並びに親タグを紐づける場合は親タグをプルダウンから選択します。
直接サイトが紐づけられているタグを親タグにすることはできません。
3. 「保存」をクリックし、設定を保存します。

■ ユーザの招待

管理 > 組織管理 画面の「ユーザを招待する」をクリックすると、ユーザを招待することができます。

詳細は「[ユーザの招待](#)」をご確認ください。

■ サイト、サイトタグの編集

1. ツリー表示画面でサイト、サイトタグをクリックし、表示される画面右上の鉛筆マークをクリックします。



図 10-9 サイトの編集

ツリー表示画面では、サイト / サイトタグと同様に組織の編集を行うこともできます。

2. 以下の画面で設定を行います。設定項目は「[サイトの作成](#)」「[サイトタグの作成](#)」を参照してください。

サイトの編集

サイト名 *

Gotanda

サイトタグ

None

国・地域のタイムゾーン *

Japan

Asia/Tokyo(UTC+09:00, ...)

住所

デバイス資格情報

デバイス資格情報のユーザ名とパスワードは、ローカルのWebページからログインする際に使用されます。パスワードの長さは8~64文字に設定する必要があります。

ユーザ名

admin

パスワード *

.....

NTP情報

NTPサーバ 1 *

ntp.nuclias.com

NTPサーバ 2

連絡先情報

名前

1-64文字

電話

1-32文字

Eメールアドレス

1-128文字

閉じる

適用

サイトタグの編集

タグ名 *

Japan

親タグ

None

作成するタグは、選択した親タグのサブタグとなります。どのサイトとも関連していないタグが表示されます。

閉じる

保存

図 10-11 サイトタグの編集

3. 設定後、「適用」または「保存」をクリックします。
変更した設定は Nuclias サーバに保存され、同時にデバイスへプッシュ配信されます。

ライセンス管理

ライセンス管理画面では、Nuclias に登録しているライセンス情報の確認と管理を行います。

注意 ライセンス切れとなった機器の動作については、動作保証外になります。

注意 「ライセンス管理」の項目は、1 つのサイトのみを管理するアカウントでは表示されません。

管理 > ライセンス管理を選択します。



図 10-12 ライセンス管理（概要）

本画面には「オーバービュー」「デバイス」「ライセンス」「期限日の統一化」「ライセンスログ」のタブがあります。各画面の詳細については以下を参照してください。

[「ライセンス管理 - オーバービュー」](#)

[「ライセンス管理 - デバイス」](#)

[「ライセンス管理 - ライセンス」](#)

[「ライセンス管理 - 期限日の統一化」](#)

[「ライセンス管理 - ライセンスログ」](#)

■ ライセンスの使用状況について

ライセンスの使用状況は、Nuclias 上で以下のように表示されます。

項目	説明
ライセンスタイプ (デバイスに割り当てられているか、割り当てられていないかを表します)	
使用中	ライセンスはデバイスに割り当てられています。
未使用	ライセンスはデバイスに割り当てられていません。
状態 (稼働を開始したか、稼働を開始していないかを表します)	
稼働中	稼働を開始したライセンスです。ライセンスの有効期間は消費されます。 「使用中・稼働中」 デバイスに割り当てられ、稼働中のライセンスです。 「未使用・稼働中」 デバイスに割り当てて稼働を開始した後、デバイスの削除などによりデバイスに割り当てられていない状態になったライセンスです。デバイスに割り当てられていない「未使用」の状態でも、「稼働中」であればライセンスの有効期間は消費されます。
休止中	稼働を開始していないライセンスです。ライセンスの有効期間は消費されません。 「未使用・休止中」 デバイスに割り当てられておらず、稼働も開始していないライセンスです。 「使用中・休止中」 デバイスに割り当てられていますが、稼働を開始していないライセンスです。 デバイスに割り当てられた 2 つ目のライセンスの場合や、デバイスに割り当て済みでもデバイスがまだオンラインになっていない場合などは「使用中・休止中」となります。

ライセンス管理 - オーバービュー

Nuclias に登録されているライセンスの概要を表示します。
登録されているライセンスの数と使用状況、60 日以内に期限切れになるライセンスを確認できます。



図 10-13 ライセンス管理（オーバービュー）

ライセンス管理 - デバイス

ライセンスを使用しているデバイスの情報を確認できます。
また、デバイスの追加と削除、ライセンスやプロファイルの割り当てを実行できます。

注意 本画面は、**管理 > インベントリ**をクリックした場合に表示される画面と同一です。



図 10-14 ライセンス管理（デバイス）

画面には以下の項目が表示されます。

項目	説明
状態	各機器のステータスを以下の色で表示します。 ・ 緑色：オンライン / 赤色：オフライン / 灰色：休止状態
MAC アドレス	デバイスの MAC アドレスを表示します。
デバイス UID	デバイスの UID を表示します。
シリアル番号	デバイスのシリアル番号を表示します。
モデル名	デバイスのモデル名を表示します。
デバイス名	デバイス名を表示します。
サイト	デバイスが登録されているサイトを表示します。
プロファイル	デバイスが紐づいているプロファイルを表示します。
ライセンス状態	ライセンスのステータスを表示します。
登録日	ライセンスの登録日を表示します。
期限日	ライセンスの期限日を表示します。

■ デバイスの追加

1. 管理 > ライセンス管理画面の「デバイス」タブで「デバイスの追加」をクリックし、以下の画面を表示します。



図 10-15 インベントリへデバイスを追加

2. 「デバイス UID」を入力します。

CSV ファイルを用いてまとめてデバイスを登録する場合は、「一括インポート」をクリック → ファイルを選択してアップロードします。
CSV ファイルのサンプルが必要な場合は、指定のメッセージをクリックします。

3. 設定後、「保存」をクリックします。

■ デバイスの削除

1. 管理 > ライセンス管理画面の「デバイス」タブで、削除するデバイスのチェックボックスを選択します。
2. 「削除」をクリックし、以下の画面を表示します。

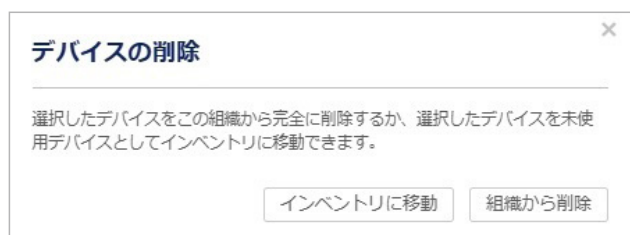


図 10-16 デバイスの削除

3. 「インベントリに移動」または「組織から削除」をクリックします。
 - ・「インベントリに移動」：デバイスに割り当てたサイト、プロファイル、ライセンスが削除されます。「割り当て」から再度サイト、プロファイル、ライセンスを割り当てることができます。
 - ・「組織から削除」：デバイスは組織から削除されます。

注意 デバイスを削除した場合、そのデバイスに割り当てられていたライセンスは削除されず、元の組織に残ります。
削除したデバイスを別の組織に登録する場合、別途ライセンスを用意いただく必要があります。

注意 デバイスを Nuclias から削除すると、削除したデバイスに関するイベントログは全て削除されます。
イベントログを残しておく必要がある場合は、事前にイベントログをダウンロードしてください。
詳細は、第 7 章 モニタ「[アクセスポイント - イベントログ](#)」を確認してください。

■ 組織 / サイトとプロファイルの割り当て

新しく一括登録したデバイス（ライセンスは割り当てられていない状態）を、既存の組織または新規組織に割り当てることができます。組織のほか、サイト / プロファイル / ライセンスの割り当てが可能です。ライセンスは「割り当て」の実行前に組織へ登録しておく必要があります。

- 1. 管理 > ライセンス管理画面の「デバイス」タブで、デバイスのチェックボックスにチェックを入れ、「割り当て」をクリックします。
- 2. 以下の画面で「既存サイトとプロファイル」または「新しいサイトとプロファイル」を選択します。

組織にアサインする

● 既存の組織、サイト、プロファイル

組織*
DJP_2

サイト*
Gotanda

プロファイル*
DBA-1510P

オートアサインライセンス

ライセンス期間
未使用 1年

○ 新しい組織、サイト、プロファイル

キャンセル

既存へ追加

組織にアサインする

○ 既存の組織、サイト、プロファイル

● 新しい組織、サイト、プロファイル

組織*

サイト*

国・地域のタイムゾーン
Afghanistan Asia/Kabul(UTC +04:30, DST)

住所

プロファイル
デフォルトコンフィグを使用する

オートアサインライセンス

ライセンス期間
未使用 1月

キャンセル

組織の作成と追加

図 10-17 組織にアサインする

- ・「既存の組織、サイト、プロファイル」：
すでに設定済みの組織、サイト、プロファイルを選択し、デバイスに割り当てます。
- ・「新しい組織、サイト、プロファイル」：
新しい組織、サイトを設定し、デバイスに割り当てます。プロファイルはデフォルトプロファイルが割り当てられます。
プロファイルは後から編集可能です。
- ・「オートアサインライセンス」：
利用可能な既存のライセンスキーが、選択したデバイスに対して自動的に割り振られます。
ただし、選択したデバイスに適用するライセンスキーが条件を満たしていない場合、割り当てが失敗する可能性があります。

注意 複数のデバイスを選択して「割り当て」を行う場合、「オートアサインライセンス」で使用できるのは「休止中」（稼働を開始していない）状態のライセンスのみです。
1つのデバイスのみを選択して「割り当て」を行う場合は、「稼働中 / 未使用」（稼働を開始したが、現在はデバイスに割り当てられていない）状態のライセンスも使用できます。

- 3. 設定後、「既存へ追加」または「組織の作成と追加」をクリックします。

136

■ ライセンスの割り当て

使用中のデバイスにライセンスを割り当てます。
本機能は、「休止中」（まだ稼働を開始していない）状態のライセンスが組織内にある場合のみ使用できます。

以下の手順の例では、有効期限 1 年のライセンス 5 つを組織に登録し、デバイスに割り当てます。

1. 管理 > ライセンス管理画面の「デバイス」タブで、デバイスのチェックボックスにチェックを入れます。
以下の画面では 2 つのデバイスを選択しています。

デバイスの追加 削除 割り当て... ライセンスの割り当て				
☐	#	状態	MAC アドレス	デバイスUID
☒	1	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	2	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	3	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	4	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	5	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	6	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	7	●	0800D04F49809A8B5	0800D04F49809A8B5
☒	8	●	0800D04F49809A8B5	0800D04F49809A8B5
☐	9	●	0800D04F49809A8B5	0800D04F49809A8B5

図 10-18 ライセンス管理（デバイス選択）

2. 「ライセンスの割り当て」をクリックし、以下の画面を表示します。

5 つのライセンスのうち 2 つをデバイスに割り当てる場合、「残り 3」と表示されます。

ライセンス割り当て

選択された数 2 AP, 0 switch, 0 gateway.

アクセスポイント

1年

+ 追加

残り 3

スイッチ

1年

+ 追加

残り 0

ゲートウェイ

1年

+ 追加

残り 0

キャンセル

割り当て

図 10-19 ライセンス割り当て

注意 ドロップダウンリストで「2 年」を選択しても、「1 年ライセンス × 2」とは判定されません。

「+ 追加」をクリックするとライセンスの枠が追加されます。割り当て可能なライセンスキーがある場合は入力します。

ライセンス割り当て

選択された数 2 AP, 0 switch, 0 gateway.

アクセスポイント

1年

+ 追加

残り 3

1年

×

残り 1

スイッチ

1年

+ 追加

残り 0

ゲートウェイ

1年

+ 追加

残り 0

キャンセル

割り当て

図 10-20 ライセンス割り当て（追加）

3. 「割り当て」をクリックし、ライセンスの割り当てを実行します。

4. ライセンスの割り当ての結果が表示されます。



図 10-21 ライセンス割り当て（結果）

注意 デバイスに割り当てられているライセンスの情報を確認するには、**モニタ** > **アクセスポイント** > **デバイス**画面、または**設定** > **アクセスポイント** > **デバイス**画面でデバイスを選択し、「ライセンス」タブを選択してください。

ライセンス管理 - ライセンス

登録しているライセンスの情報と履歴を表示します。また、ライセンスを組織に登録できます。



図 10-22 ライセンス管理（ライセンス）

本画面には以下の項目が表示されます。

項目	説明
ライセンスタイプ	ライセンスがデバイスに割り当てられているか、割り当てられていないかを表示します。 「使用中」：ライセンスがデバイスに割り当てられています。 「未使用」：ライセンスがデバイスに割り当てられていません。
状態	ライセンスの稼働状態を表示します。 「稼働中」：稼働しているライセンスです。有効期間が消費されます。 「休止中」：稼働を開始していないライセンスです。有効期間は消費されません。
ライセンスキー	ライセンスキーを表示します。
期間	ライセンスの期間を表示します。
ライセンスデバイスタイプ	ライセンスのデバイスタイプを表示します。
登録日	デバイスの登録日を表示します。
デバイス UID	デバイスの UID を表示します。
モデル名	デバイスのモデル名を表示します。
MAC アドレス	デバイスの MAC アドレスを表示します。
開始日	ライセンスの使用開始日を表示します。
期限日	ライセンスの期限日を表示します。
残り時間	ライセンスの残りの有効期間を表示します。

■ ライセンス履歴の表示

「ライセンス履歴」をクリックすると、1年以内に失効したライセンスの情報を確認できます。
「タイムフレーム」で期間を選択→「ダウンロード」をクリックして csv ファイルをダウンロードします。

■ ライセンスの検索

特定の文字列を含むライセンス情報を検索する場合は、検索ウィンドウに文字を入力します。

検索ウィンドウ右側の  をクリックして詳細な検索ウィンドウを表示させ、より精度の高い検索を行うこともできます。

■ ライセンス一覧表のダウンロード

 をクリックすると、ライセンス一覧表を csv ファイルでダウンロードします。

■ ライセンスの追加

ライセンスを組織に登録します。

1. 管理 > ライセンス管理画面の「ライセンス」タブで、「ライセンスの追加」をクリックします。
2. ライセンスキーを入力し、「追加」をクリックします。



ライセンスキーの追加

☒ ライセンスキーの追加
ライセンスキー #1*

☐ 一括インポート

キャンセル 追加

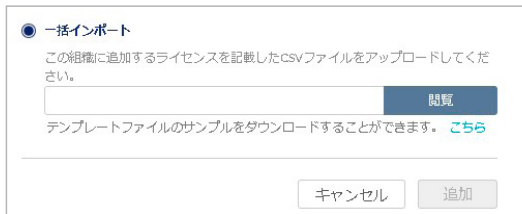
図 10-23 ライセンスキーの追加

注意 登録したライセンスキーは、他の組織で使用することはできません。

■ ライセンスの一括インポート

CSV ファイルからまとめてライセンスを登録する場合は、「一括インポート」を選択します。

以下の画面でファイルを選択し、CSV ファイルをアップロードします。



☒ 一括インポート

この組織に追加するライセンスを記載したCSVファイルをアップロードしてください。

閲覧

テンプレートファイルのサンプルをダウンロードすることができます。 [こちら](#)

キャンセル 追加

図 10-24 ライセンスの一括インポート

CSV ファイルのサンプルが必要な場合は、指定のメッセージをクリックします。

ライセンス管理 - 期限日の統一化

「期限日の統一化」タブでは、登録しているライセンスの期限日を統一できます。

Nuclias に複数のライセンスを登録している場合、登録した日によってそれぞれのライセンスの有効期限が異なります。この場合、ライセンスごとに有効期限を確認し、期限が切れる前にそれぞれのライセンスの更新を個別に行う必要があります。

ライセンスの期限日を統一することによって、ライセンスの更新作業をまとめて実行できるため、ライセンスの管理が容易になります。

「期限日の統一化」を実行すると、登録済みのライセンスを終了し、新しいライセンスが生成されます。

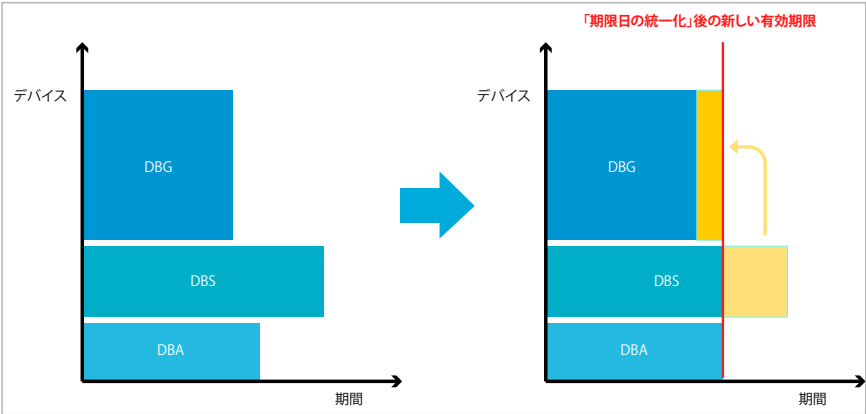


図 10-25 「期限日の統一化」の仕組み

注意 本機能は、実行後に取り消すことはできません。

「期限日の統一化」実行前のライセンスを復元することはできませんので、ご注意ください。

「期限日の統一化」は、組織ごとに実行できます。実行できるデバイスとライセンスの条件は以下のとおりです。

- 同一の組織に登録されている以下のデバイス
 - ・「稼働中」のライセンスが割り当てられているデバイス
 - ・期限切れのライセンスが割り当てられているデバイス
- 同一の組織に登録されている以下のライセンス
 - ・「使用中」で「稼働中」のライセンス（デバイスに割り当てられていて、有効期間を消費中のライセンス）
 - ・「使用中」で「休止中」のライセンス（デバイスに割り当てられているが、有効期間の消費は開始されていないライセンス）
 - ・「未使用」で「稼働中」のライセンス（現在はデバイスに割り当てられていないが、有効期間を消費中のライセンス）

注意 ライセンスの「使用中」「未使用」「稼働中」「休止中」の説明については「[ライセンスの使用状況について](#)」を参照してください。

「期限日の統一化」の手順は以下の通りです。

1. 管理 > ライセンス管理画面で「期限日の統一化」タブを選択します。



図 10-26 ライセンス管理 - 期限日の統一化

2. 「ライセンス期限の計算」をクリックし、期限を統一化した場合のライセンス有効期限を確認します。



図 10-27 ライセンス期限の計算

- 注意** 「ライセンス期限の計算」の結果、ライセンスの有効期間が残り 30 日未満の場合は、「ライセンス期限日の統一化」を実行できません。
3. 「ライセンスの期限日の統一化」をクリックします。
4. 確認画面の内容を確認後、同意する場合はチェックボックスを選択し、「確認」をクリックします。
本機能は、実行後に取り消すことはできませんのでご注意ください。

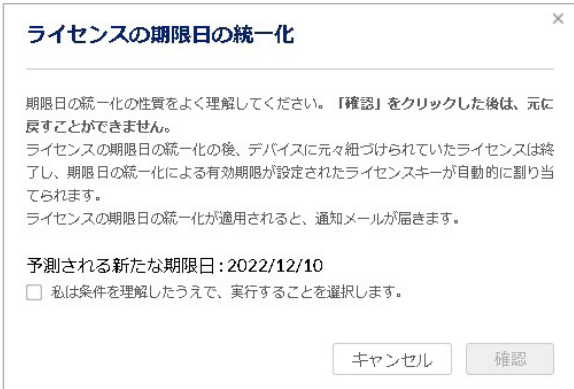


図 10-28 ライセンス期限の計算

注意 関係するライセンスやデバイスに変更があった場合、期限日の統一化の動作は中断します。最初からやり直してください。

■ ライセンスの有効期限の計算方法について

「ライセンス期限日の統一化」を行う場合、統一化後の有効期限は、デバイスタイプの比重と残りの有効期間をもとに計算されます。ライセンスの価格が異なるため、計算の際の比重はデバイスタイプによって異なります。

デバイスタイプ	DBS-2000	DBA シリーズ	DBG シリーズ
比重	1	2	5

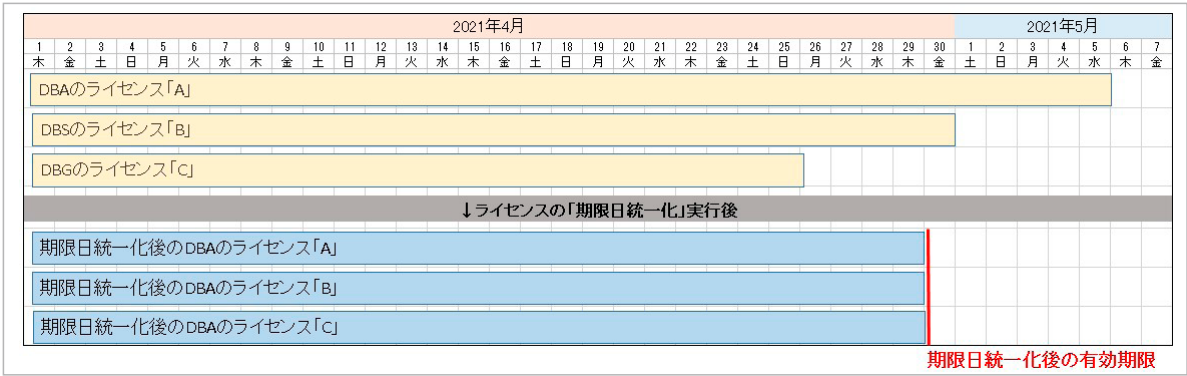


図 10-29 ライセンス期限統一化の例

計算手順

期限日統一化後の有効期限は、以下の方法で計算されます。

- (1) 統一化するライセンスを収集します。
- (2) ライセンス有効期間の残存日数を収集します。
- (3) 残存日数とデバイスの比重を乗算します。
- (4) 統一化するすべてのライセンスの「残存日数×デバイスの比重」値を合計します。
- (5) 統一化するすべてのデバイスの比重を合計します。
- (6) 手順 4 の値を手順 5 の値で割ります。
- (7) 手順 6 で出した値の小数点以下を切り上げて、統一化後の残存日数とします。

$$\frac{\sum_{i=1}^n \text{デバイスの比重} \times \text{ライセンス有効期間の残存日数}_i}{\text{デバイスの比重の合計}} = \text{統一化後の有効残存日数}$$

計算例

以下にライセンスの有効期限の計算例を記載します。

2021/1/14 に、DBA-1210P の 1 年間ライセンスを購入し、有効化。(2 台分)
2021/10/20 に、DBG-2000 の 1 年間ライセンスを購入し、有効化。(1 台分)
2021/11/5 に「ライセンスの期限日の統一化」を実行。

統一化前のライセンスの有効期間残存日数：

- DBA-1210P (2021/11/5 – 2022/1/14 = 70 日)
- DBG-2000 (2021/11/5 – 2022/10/20 = 349 日)

残存日数と比重の計算式（計算手順の 3、4）：

70（日）× 2（DBA の数）× 2（DBA の比重）= 280
349（日）× 1（DBG-2000 の数）× 5（DBG の比重）= 1745

デバイスの比重の合計（計算手順の 5）：

(2 DBA × 2) + (1 DBG × 5) = 9

統一化後の残存日数（計算手順の 6）：

(280 + 1745) / 9 = 225（日）

統一化後の有効期限：

2021/11/5 + 225（日）= 2022/6/18
全てのデバイスには、期限日が 2022 年 6 月 18 日のライセンスが付与されます。

ライセンス管理 - ライセンスログ

ライセンスに関するログを表示します。

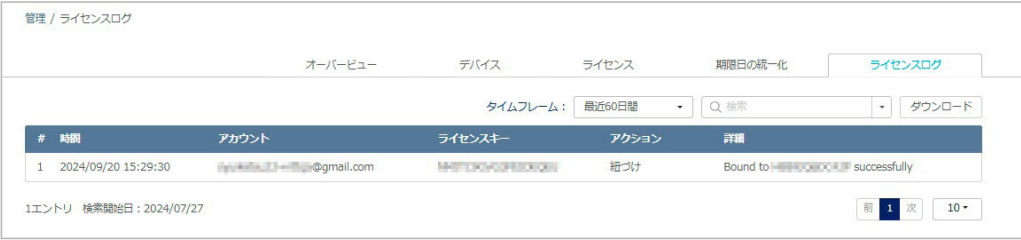


図 10-30 ライセンス管理（ライセンスログ）

本画面には以下の項目が表示されます。

項目	説明
時間	ログが記録された時間を表示します。
アカウント	アクションを行ったユーザのアカウントを表示します。
ライセンスキー	ライセンスキーを表示します。
アクション	ライセンスのアクション（追加、紐づけなど）を表示します。
詳細	アクションの詳細を表示します。

■ 表示する期間の変更

「タイムフレーム」で表示する期間を設定します。

■ ライセンスログの検索

特定の文字列を含むライセンス情報を検索する場合は、検索ウィンドウに文字を入力します。

検索ウィンドウ右側の「▼」をクリックして詳細な検索ウィンドウを表示させ、より精度の高い検索を行うこともできます。

■ ライセンスログのダウンロード

「ダウンロード」をクリックすると、ライセンスログを csv ファイルでダウンロードします。

インベントリ

デバイスの登録と削除、組織 / プロファイル / ライセンスの割り当てを行います。

本画面は、管理 > ライセンス管理画面で「デバイス」タブを選択した場合に表示される画面と同一です。

設定内容については「ライセンス管理 - デバイス」を参照してください。

注意 「インベントリ」の項目は、1 つのサイトのみを管理するアカウントでは表示されません。

管理 > インベントリを選択し、以下の画面を表示します。



図 10-31 インベントリ画面

ファームウェア

管理 > ファームウェア画面では、ファームウェアの管理を行います。
本画面には以下のタブがあります。

- ・「ニューリリース」
- ・「サイトのファームウェアアップグレード」
- ・「デバイスのファームウェア管理」

ファームウェア - ニューリリースタブ

各デバイスごとにファームウェアのリリース状況を表示します。
「バージョン」欄のリンクをクリックするとリリースノート（英語版）が表示されます。
日本で販売されている製品については、弊社のホームページでリリースノートをご確認ください。

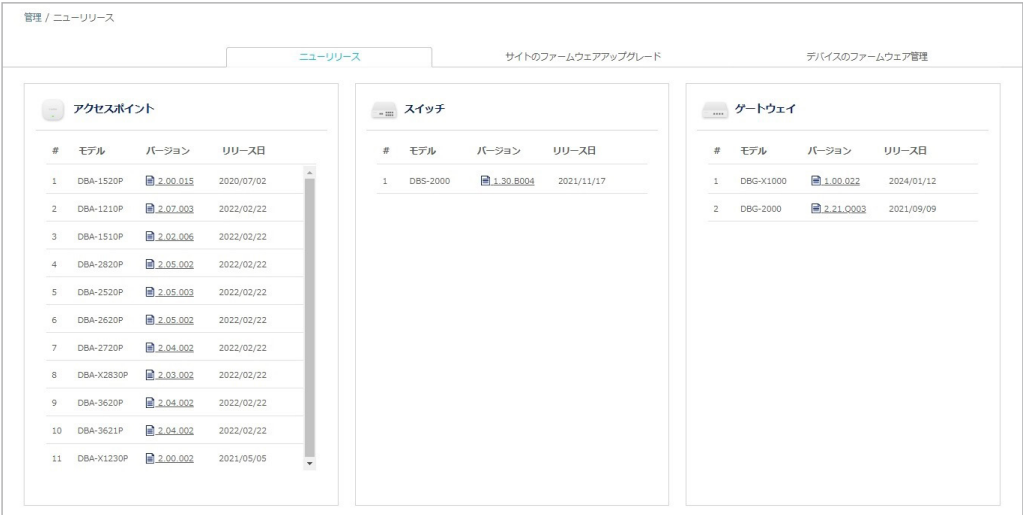


図 10-32 ファームウェア

ファームウェア - サイトのファームウェアアップグレードタブ

ファームウェアのスケジュールアップグレードを設定します。



図 10-33 ファームウェア - サイトのファームウェアアップグレード

本画面には以下の項目があります。

項目	説明
チェックボックス	チェックボックスにチェックを入れて「スケジュールアップグレード」をクリックすると、ファームウェアアップグレードのスケジュールを設定できます。
サイト	製品が登録されているサイトを表示します。
製品カテゴリ	製品のカテゴリ（スイッチ、アクセスポイント、ゲートウェイ）を表示します。
モデル名	製品のモデル名を表示します。
デバイス	デバイスの数を表示します。数字をクリックするとデバイスの情報が表示されます。
適用ファームウェア	現在デバイスに適用しているファームウェアの状態を表示します。 最新のバージョンを適用している場合は「最新」と表示されます。
現在のファームウェアバージョン	現在 Nuclias 上で設定されているファームウェアバージョンです。
対象のファームウェアバージョン	アップグレード時に適用するファームウェアのバージョンを表示します。
アップグレードポリシー	ファームウェアのアップグレードポリシー（手動/スケジュール）を表示します。
アップグレードスケジュール（現地時間）	ファームウェアのアップグレードを行うスケジュールを表示します。
最終アップグレード日時（現地時間）	最後にファームウェアアップグレードを実行した日時を表示します。
対象ファームウェアのリリースノート	アップグレード時に適用するファームウェアバージョンのリリースノート（英語版）を表示します。

■ スケジュールアップグレード

ファームウェアアップグレードのスケジュールを設定します。

- 1. 管理＞ファームウェア画面の「サイトのファームウェアアップグレード」タブでスケジュール設定を行うデバイスを選択します。
- 2. 「スケジュールアップグレード」を選択し、以下の画面でスケジュールを設定します。

スケジュールファームウェア変更

ファームウェアを変更するデバイスの数によっては、アップグレード時間にずれが生じる場合があります。

自動アップグレードのスケジュール (曜日/時刻指定)

日曜日00:00(サイトの現地時間)

アップグレードのスケジュール (日付/時刻指定)

02/27/202511:00(サイトの現地時間)

今すぐアップグレード実行 (手動で実行)

閉じる

次

図 10-34 スケジュールファームウェア変更

本画面には以下の項目があります。

項目	説明
自動アップグレードのスケジュール	指定した曜日と時刻になった場合、自動的にファームウェアアップグレードを行います。
アップグレードのスケジュール	指定した日時にファームウェアアップグレードを行います。
今すぐアップグレード実行	今すぐファームウェアアップグレードを行います。

- 3. 「次」をクリックします。
- 4. 「対象のファームウェアバージョン」のドロップダウンリストでファームウェアバージョンを選択します。
手順2で「自動アップグレードのスケジュール」を選択した場合はファームウェアバージョンを選択できません。

ファームウェアバージョンの一括編集

#	サイト	製品カテゴリ	モデル名	現在のファームウェアバージョン	対象のファームウェアバージョン
1	DJP_画面確認用	アクセスポイント	DBA-1210P	2.07.003	2.07.003(最新)

前

1

次

10

Back

スケジュール変更

図 10-35 ファームウェアバージョンの一括編集

- 5. 「スケジュール変更」をクリックします。

注意 手順3で「今すぐアップグレード実行」を選択した場合は、ファームウェアアップグレードが開始されます。

■ ファームウェアアップグレード対象の検索

検索ウィンドウでファームウェアアップグレードを行うデバイスを検索できます。
「モデル名」「ファームウェア状態」を指定して検索することも可能です。

145

ファームウェア - デバイスのファームウェア管理タブ

デバイスのファームウェア管理タブでは、デバイスとファームウェア情報のプレビューとダウンロードを実行できます。



図 10-36 ファームウェア - デバイスのファームウェア管理

本画面には以下の項目があります。

項目	説明
デバイスモデル	プレビューに表示するデバイスをドロップダウンリストから選択します。
適用ファームウェア	プレビューに表示するファームウェアを「全て」「更新可能分」「最新」から選択します。
プレビュー	「プレビュー」をクリックすると、画面下部にデバイスとファームウェアの情報が表示されます。
ダウンロード	「ダウンロード」をクリックすると、プレビューで表示した情報を CSV ファイルでダウンロードできます。

アラート設定

管理 > アラート設定を選択し、アラート設定するイベントを指定します。
指定したイベントは、図 9-4 「アラート」画面に表示、並びに管理用メールアドレスにメール送信されます。
アラートを発報する項目が表示されます。「E メール」にチェックをいれた場合、アラートが管理用メールアドレスに送信されます。

管理 / アラート設定

一般

デバイスが登録されました

☐

Eメール

デバイスのファームウェアは正常にアップグレードしました

☐

ファームウェアアップグレードは失敗しました

☐

サイト並びにプロファイルは正常に更新されました

☐

デバイスはNucliasに正常に接続されました

☐

プロファイル設定の適用に成功しました

☐

プロファイル設定の更新に失敗しました

☐

アクセスポイント

APオフラインを何分間継続して検知したらアラートを送るか

60

分

☒

Eメール

スイッチ

Switchオフラインを何分間継続して検知したらアラートを送るか

60

分

☒

Eメール

Anyポート

ダウン状態の時間

60

分

☒

Eメール

ゲートウェイ

ゲートウェイオフライン状態

60

分

☒

Eメール

DHCPリースプールが残り10%を切りました

☐

IPsecトンネルが接続されました

☐

IPsecトンネルが切断されました

☐

WANポートが接続されました

☐

WANポートが切断されました

☐

ネットワーク使用量超過

100

GB

in

30分

☐

Eメール

図 10-37 アラート設定

本画面には以下の項目があります。

項目	説明
デバイスが登録されました	デバイスが Nuclias に登録された際にアラートを発報します。
デバイスのファームウェアは正常にアップグレードしました	ファームウェアアップグレード実施時にアラートを発報します。
ファームウェアアップグレードは失敗しました	ファームウェアアップグレードに失敗したときにアラートを発報します。
サイト並びにプロファイルは正常に更新されました	サイトおよびプロファイルが正常に更新されたときにアラートを発報します。
デバイスは Nuclias に正常に接続されました	オフライン状態のデバイスが正常に Nuclias に接続（オンライン）状態になったときにアラートを発報します。
プロファイル設定の適用に成功しました	デバイスへ「設定のプッシュ」を実施した際にアラートを発報します。
プロファイル設定の更新に失敗しました	デバイスへの「設定のプッシュ」が失敗した際にアラートを発報します。

項目	説明
AP オフラインを何分間継続して検知したらアラートを送るか	Nuclias でオフライン状態と判断したタイミングを起点とし、引き続き指定した時間オフラインが継続した場合にアラートを発報します。プルダウンで「5」「10」「15」「30」「60」(単位：分) から指定できます。 AP が実際に Nuclias から切断された後、オフライン状態と判断されるためには、5 分間オフラインを継続している必要があります。上記は 5 分後の状態を起点とします。 そのため、例えば本項目で「10 分」と設定した場合、実際に AP が Nuclias から切断されてからアラートメールが送付されるためにはおよそ 15 分以上かかります。

注意 上記以外にも、デバイスに紐づけられたライセンスの期限日が近くなった場合にアラートメールが送信されます。
30 日前、7 日前、3 日前、1 日前に通知されますので、継続してデバイスを使用する場合は新しいライセンスを適用してください。
設定後、「保存」をクリックします。

証明書とキーの管理

管理 > 証明書とキーの管理を選択し、証明書とキーの設定、管理を行う画面を表示します。

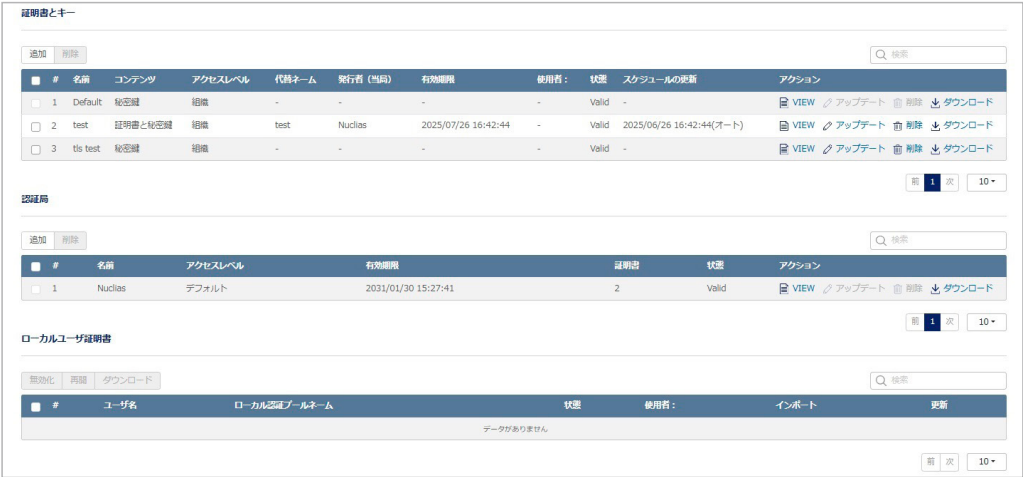


図 10-38 証明書とキーの管理

本画面には以下の項目が表示されます。

項目	説明
証明書とキー	
チェックボックス	チェックボックスにチェックを入れ、「削除」をクリックすると証明書とキーを削除できます。デフォルトで設定されている証明書とキーは削除できません。
名前	証明書とキーの名前を表示します。
コンテンツ	証明書とキーのコンテンツを表示します。
アクセスレベル	証明書とキーに設定されたアクセスレベルを表示します。
代替ネーム	証明書とキーの代替ネームを表示します。
発行者（当局）	証明書とキーの発行者を表示します。
有効期限	証明書とキーの有効期限を表示します。
使用者	証明書の使用者について表示します。
状態	証明書とキーの状態を表示します。
スケジュールの更新	証明書とキーの更新スケジュールを表示します。
アクション	「VIEW」：証明書とキーの詳細情報を表示します。 「アップデート」：証明書とキーをアップデートします。デフォルトの証明書とキーはアップデートできません。 「削除」：証明書とキーを削除します。デフォルトの証明書とキーは削除できません。 「ダウンロード」：証明書とキーを PEM 形式のファイルでダウンロードします。
認証局	
チェックボックス	チェックボックスにチェックを入れ、「削除」をクリックすると認証局を削除できます。デフォルトで設定されている認証局は削除できません。
名前	認証局の名前を表示します。
アクセスレベル	認証局に設定されたアクセスレベルを表示します。
有効期限	認証局の有効期限を表示します。
証明書	証明書の数を表示します。
状態	認証局の状態を表示します。
アクション	「VIEW」：認証局の詳細情報が表示されます。 「アップデート」：認証局の設定をアップデートします。デフォルトの認証局はアップデートできません。 「削除」：認証局を削除します。デフォルトの認証局は削除できません。 「ダウンロード」：認証局の情報を PEM 形式のファイルでダウンロードします。
ローカルユーザ証明書	
チェックボックス	チェックボックスにチェックを入れ、「無効化」「再開」「ダウンロード」を実行できます。
ユーザ名	ユーザ名を表示します。
ローカル認証プールネーム	ローカル認証のプール名を表示します。
状態	ローカルユーザ証明書の状態を表示します。
使用者	証明書の使用者について表示します。
インポート	ローカルユーザ証明書のインポート日時を表示します。
更新	ローカルユーザ証明書の更新日時を表示します。

■ 証明書とキーの追加

1. 管理 > 証明書管理画面の「証明書とキー」エリアで「追加」をクリックし、以下の画面を表示します。

証明書またはキーの追加

● 証明書署名要求の発行

コモン名

代替ネーム

Signed by

Nuclias (期限日 2031/01/30 15:27:41)

☐ CSRのアップロード

☐ 証明書のインポート

☐ 秘密鍵の生成(DH, TLS)

☐ 秘密鍵のインポート(DH, TLS)

アクセス権限

アクセスレベル

組織

閉じる

保存

図 10-39 証明書要求

2. 作成する証明書を以下から選択後、表示される項目を入力、またはファイルをアップロード/インポートします。
- 証明書署名要求の発行：「コモン名」「代替ネーム」を入力し、「Signed by」で認証局を設定します。
 - CSR のアップロード：「Signed by」で認証局を設定し、CSR（certificate signed request）をアップロードします。
 - 証明書のインポート：証明書をインポートします。
 - 秘密鍵の作成 (DH, TLS):「キーネーム」「キータイプ」「キーサイズ」を設定します。キータイプは「DH キー」「TLS キー」から選択できます。
 - 秘密鍵のインポート (DH, TLS)：「キーネーム」を設定し、秘密鍵をインポートします。
3. 「証明書のインポート」「秘密鍵の作成 (DH, TLS)」「秘密鍵のインポート (DH, TLS)」を選択した場合、アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。
4. 「保存」をクリックします。

■ 認証局の追加

1. 管理 > 証明書管理画面の「認証局」エリアで「追加」をクリックします。

認証局の追加

アクセス権限

アクセスレベル

組織

CAのアップロード

認証局（CA）の暗号化されていないPEM形式のRSA秘密鍵をアップロードします*

閲覧

認証局（CA）のPEM形式のX.509証明書をアップロードします*

閲覧

閉じる

保存

図 10-40 認証局の追加

2. アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。
3. 「CA のアップロード」の「閲覧」をクリックし、認証局（CA / Certification Authority）をアップロードします。
4. 「保存」をクリックします。

アドバンスト設定 > SAML 設定

管理 > アドバンスト設定 > SAML 設定を選択し、以下の画面で SAML の設定を行います。

管理 / アドバンスト設定 / SAML設定

1つ以上のTrusted Identity Provider (IdP) to enable SAML SSOを追加してください。

SAML設定

SAML SSO

☒ 有効 ☐ 無効

エンティティID

124365.sp.saml.nucias.com

URL

https://portal.nucias.com/oauth/124365/samlLogin

TRUSTED IDENTITY PROVIDER (IDP)

追加

削除

☐

名前

URL

Issuer

証明書

ログアウトURL

X.509 cert SHA1 fingerprint

アクション

SAMLロール

追加

削除

☐

#

名前

役割

管理サイト

アクション

前

次

10

図 10-41 SAML 設定

本画面には以下の項目があります。

項目	説明
SAML SSO	SAML SSO を有効または無効に設定します。
エンティティ ID	エンティティ ID が表示されます。設定作業には使用しません。
URL	URL が表示されます。IdP サーバに設定する Assertion Consumer URL です。
TRUSTED IDENTITY PROVIDER (IDP)	TRUSTED IDENTITY PROVIDER (IDP) が表示されます。「追加」をクリックし、SAML IDP を追加することも可能です。
SAML ロール	SAML ロールが表示されます。「追加」をクリックし、SAML ロールを追加することも可能です。

■ TRUSTED IDENTITY PROVIDER (IDP) の追加

1. TRUSTED IDENTITY PROVIDER (IDP) の「追加」をクリックし、以下の画面を表示します。

SAML IdPの追加

名前*

1-64文字

☒ IdPの追加

URL

認証に使用されるURL

Issuer

発行者のIDまたは発行者の詳細のURL

証明書*

PEM形式の証明書のアップロード

閲覧

ログアウトURL

ユーザがログアウトした際のリダイレクト先URL

X.509 cert SHA1 fingerprint

☐ IdPメタデータのインポート

閉じる

保存

図 10-42 SAML Idp の追加

2. 以下の項目を設定します。
- 「名前」：SAML IDP の名前を入力します。
 - 「IdP の追加」：「URL」「Issuer」「証明書」「ログアウト URL」「X.509 cert SHA1 fingerprint」を入力します。
 - 「IdP メタデータのインポート」：詳細な情報を含んだ metadata XML ファイルをインポートします。
3. 設定後、「保存」をクリックします。

■ SAML ロールの追加

1. SAML ロールの「追加」をクリックし、以下の画面を表示します。

SAMLルールを追加

名前*

1-64文字

アクセス権限

役割*

管理者

アクセスレベル

組織

Nuclias_Manual

管理サイト*

全てのサイト

全て

閉じる

保存

図 10-43 SAML ロールを追加

2. 以下の項目を設定します。
- ・「名前」：SAML ロールの名前を入力します。
 - ・「役割」：「管理者」「編集者」「モニタ」「モニタ閲覧者」から選択します。
 - ・「アクセスレベル」：アクセスレベルが表示されます。
 - ・「管理サイト」：サイトおよびサイトタグを選択します。
3. 設定後、「保存」をクリックします。

■ IdP サーバからのログイン

IdP サーバから Nuclias にログインを実施する場合は、IdP サーバ側に以下の情報を入力する必要があります。
IdP サーバの設定方法等につきましては、各サーバの説明書等をご確認ください。

項目	説明
Assertion Consumer URL	Nuclias の 管理 > アドバンスド設定 > SAML 設定 画面の「URL」に記載されている URL を入力します。
SAML Attributes	以下のとおり記載します。 ・ userName：任意のユーザ名を入力します。 ・ roleName：Nuclias の 管理 > アドバンスド設定 > SAML 設定画面の「SAML ロール」に作成されている「名前」を入力します。 ・ email：任意のメールアドレスを入力します。

アドバンスト設定 > SMS 設定

認証に使用する SMS アカウントの設定を行います。
SMS 認証を行う場合は「Twilio」のアカウントが必要です。別途 Twilio のサービスをご契約ください。

管理 > アドバンスト設定 > SMS 設定を選択し、以下の画面で SMS の設定を行います。



図 10-44 SMS 設定

■ Twilio SMS 設定の追加

1. 「Twilio SMS 設定の追加」をクリックし、以下の画面を表示します。

Twilio SMS設定の追加

名前*

1-64文字

TwilioアカウントSID*

1-64文字

Twilio認証トークン*

1-128文字

Twilio番号*

+1234567890

再送 (分)* ?

2

最大再送 (回)* ?

3

最大リクエスト (回)* ?

3

拒否時間 (分)* ?

120

ワンタイムパスワード有効期限 (分)* ?

10

許可済電話番号* ?

*

アクセス権限

アクセスレベル

組織

閉じる

保存

図 10-45 Twilio SMS 設定の追加

2. 以下の項目を設定します。

項目	説明
名前	SMS 設定の名前を 1-64 文字で入力します。
Twilio アカウント SID	Twilio アカウント SID を 1-64 文字で入力します。
Twilio 認証トークン	Twilio 認証トークンを 1-128 文字で入力します。
Twilio 番号	Twilio 番号を入力します。
再送 (分)	ワンタイムパスワードが記載された SMS を再送できるようになる時間 (単位: 分) を設定します。 「0」に設定した場合はすぐに再送できます。
最大再送 (回)	ワンタイムパスワードが記載された SMS を再送できる回数を設定します。 「0」に設定した場合は再送できません。
最大リクエスト (回)	ワンタイムパスワードを要求できる最大回数を設定します。 「0」に設定した場合は無制限に要求できます。
拒否時間 (分)	ワンタイムパスワードの再送または要求制限に達した後、再度要求ができるようになるまでにクライアントが待機しなければならない時間 (単位: 分) を設定します。 「0」に設定した場合はすぐに要求できます。
ワンタイムパスワード有効期限 (分)	ワンタイムパスワードが有効な時間 (単位: 分) を設定します。
許可済電話番号	ワンタイムパスワード SMS の要求が許可されている国の通話コードです。コードはカンマで区切る必要があります。 ワイルドカードは、すべてのコードが許可されていることを意味します。
アクセスレベル	アクセスレベルを「組織」「サイト」「サイトタグ」から選択します。

3. 設定後、「保存」をクリックします。

アドバンスト設定 > シスログサーバ 設定

シスログサーバの追加、設定、削除を実行できます。

管理 > アドバンスト設定 > シスログサーバ設定を選択します。

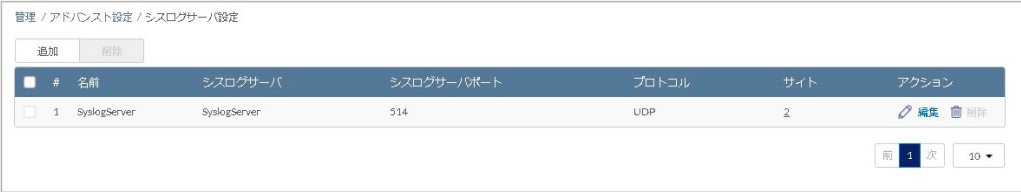


図 10-46 シスログサーバ設定

■ シスログサーバの追加

1. 管理 > アドバンスト設定 > シスログサーバ設定画面で「追加」をクリックし、以下の画面を表示します。

シスログサーバ設定の追加

名前 *

1-64文字

シスログサーバ *

192.168.200.1 or FQDN

シスログサーバポート *

514

プロトコル *

UDP

サイトの選択

0 選択済

閉じる

保存

図 10-47 シスログサーバ設定の追加

2. 以下の項目を設定します。

項目	説明
名前	設定名を 1-64 文字で入力します。
シスログサーバ	シスログサーバの IP アドレスまたはドメイン名を入力します。
シスログサーバポート	シスログサーバのポートを選択します。
プロトコル	プロトコルを「UDP」「TCP」から選択します。
サイトの選択	シスログサーバを紐づけるサイトを選択します。

3. 「保存」をクリックし、設定を保存します。

■ シスログサーバの編集

1. 管理 > アドバンスト設定 > シスログサーバ設定画面で、編集するシスログサーバのチェックボックスを選択します。
2. アクション欄の「編集」をクリックします。
3. 編集後、「保存」をクリックします。

■ シスログサーバの削除

1. 管理 > アドバンスト設定 > シスログサーバ設定画面で、削除するシスログサーバのチェックボックスを選択します。
2. 「削除」をクリックします。
3. 確認画面で「はい」をクリックします。

注意

サイトに紐づけられているシスログサーバは削除できません。
シスログサーバを削除する場合は、「編集」の「サイトの選択」でサイトが選択されていない状態にしてください。

注意

シスログサーバは DBA シリーズ、および DBG シリーズのみ対応しています。

デバイスの追加

デバイスを Nuclias に追加する方法について説明します。

1. 管理 > デバイスの追加をクリックし、以下の画面でデバイスの追加作業を行います。

デバイスの追加

デバイスUID *

Device UID

デバイス名

1-64文字

登録するデバイスのUIDを入力してください

UID フォーマットは XXXX-XXXX-XXXX または XXXXXXXXXXXX です。

サイト ?

プロファイル *

更にライセンスを追加する

キャンセル

保存

図 10-48 デバイスの追加

2. 以下の項目を設定します。

項目	説明
デバイス UID	デバイス UID を入力します。
デバイス名	Nuclias 上で管理するためのデバイス名を入力します。
サイト	デバイスに適用するサイトをプルダウンで選択します。
プロファイル	デバイスに適用するプロファイルをプルダウンで選択します。
ライセンスキー	「更にライセンスを追加する」をクリックし、ライセンスキーを紐づけます。 枠をクリックすると、そのデバイスで使用可能なライセンスキーがプルダウンで表示されますので、選択することができます。使用可能なライセンスキーとは、デバイスに初期状態で紐づけられているライセンスキー、または既に組織に登録されているライセンスキーです。これらとは異なるライセンスキーを使用する場合は、枠に直接入力してください。 選択可能なライセンスキーが複数ある場合の詳細については、巻末の「付録A ライセンスの適用や開始等に関する詳細」をご確認ください。 ライセンスキー #1 * ライセンスキーを選択してください 1123.1000.1234.1123.1000.1234(363 日) 1123.1000.1123.1000.1234.1234(361 日) 1123.1000.1123.1000.1234.1234 195 日) 注意 デバイスに紐づけられているフリーライセンスは最初にデバイスを登録した組織に保存され、他の組織で使用することはできません。該当デバイスを本組織から削除し、他の組織へ登録し直す場合、別途ライセンスを用意頂く必要があります。

3. 設定後、「保存」をクリックします。

デバイス一括インポート

複数のデバイスを Nuclias に一括で追加する方法について説明します。
一括インポートは xls 形式または xlsx 形式のファイルを使用して行います。

- 1. 管理> デバイス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 10-49 デバイス一括インポート

- 2. 「閲覧」をクリックし、xls 形式または xlsx 形式のファイルを選択します。
ファイルのサンプルが必要な場合は、指定のメッセージをクリックします。
- 3. 「アップロード」をクリックし、ファイルをアップロードします。

第 11 章 ヘルプ

- お知らせ
- 連絡をする
- リソース
- トラブルシューティング
- チュートリアル

お知らせ

ヘルプ> お知らせをクリックし、新機能サポートなどのお知らせを表示します。

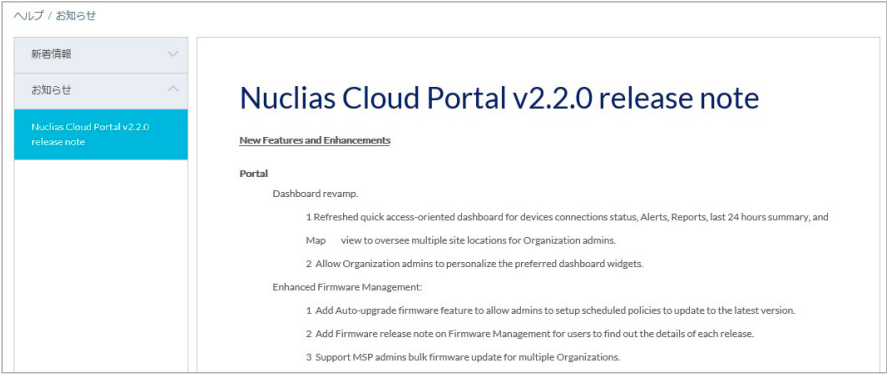


図 11-1 お知らせ

連絡をする

ヘルプ> 連絡をするをクリックし、情報を記入することにより Nuclias に関するお問い合わせができます。

図 11-2 連絡をする

本画面には以下の項目があります。

項目	説明
名前	自身の名前を入力します。
Eメール	連絡先のメールアドレスを入力します。
電話	必要に応じ、電話番号を入力できます。 ただし、Nuclias は電話による問い合わせや回答は実施していません。
問題種別	問い合わせ内容に最も近いカテゴリをプルダウンから選択します。 プルダウンメニューは「設定」「セットアップ」「デバイスの検出」「ライセンスの問題」「プライバシー関連」です。 「設定」「セットアップ」「デバイスの検出」「ライセンスの問題」を選択した場合、新たに「デバイスタイプ」「問題のあるデバイス」項目が表示されますので、該当するデバイスを選択してください。
内容	発生した事象の詳細を記述してください。
添付	画面キャプチャやシステム構築図など、事象をより詳細に把握できる資料がある場合は添付します。 1つのファイルにつき最大2MBまで対応できます。

入力後、「送信」をクリックします。

リソース

ヘルプ> リソースをクリックすると、Nuclias Cloud について説明する Web サイト（英語版）に移動します。

トラブルシューティング

ヘルプ> **トラブルシューティング**をクリックし、「Nuclias サポートの許可」を有効 / 無効に設定します。

有効にすると PIN コードが画面に表示されますので、その PIN コードをディーリンクサポートにお伝え頂くことにより、ディーリンクサポートはこの組織にアクセスできるようになります。

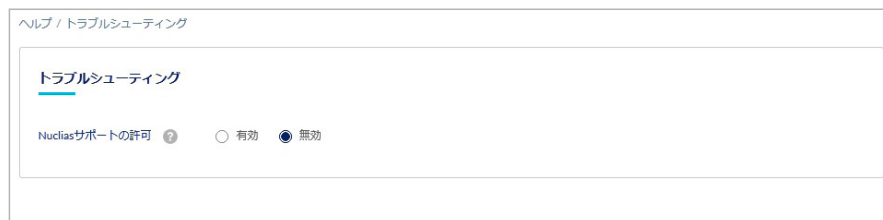


図 11-3 トラブルシューティング

チュートリアル

ヘルプ> チュートリアルをクリックすると、Nuclias の設定についてのチュートリアル（英語版）が表示されます。

第 12 章 Web GUI、CLI からの設定について

- Web GUI（Web ベース設定ユーティリティ）について
- コマンドラインインタフェース（CLI）の設定

Web GUI（Web ベース設定ユーティリティ）について

本章では、Nuclias を使用せず、PC から AP に直接アクセスし、ブラウザで設定を行う「Web GUI」について説明します。Web GUI から設定または実行できる主な項目は以下のとおりです。

- IP アドレスの設定
- NTP サーバの設定
- VLAN の設定
- 初期設定へのリセット
- ファームウェアアップグレード

上記以外の設定項目については、Nuclias Cloud から設定を行ってください。

注意 Nuclias 用 AP が LAN 内の DHCP サーバから IP アドレスを取得できる場合は、Web GUI から設定を行う必要はありません。

注意 以下の手順は Nuclias 用 AP で共通です。ここでは DBA-1210P の画面を例として記載しています。

Web GUI 設定画面へのログイン

ここでのアクセスポイントの設定は 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 ブラウザを開きます。
2. Web ブラウザのアドレス欄に Nuclias 用 AP のホスト名を入力し、Enter を押下します。
 - ホスト名の初期値：「DBA-XXXX-YYYY」
 - 「XXXX」は、Nuclias 用 AP の製品名です。
お使いの機種を確認し「1210P」「2520P」「2620P」「2720P」「2820P」「3621P」「X2830P」「X1230P」「X5480P」のいずれかを入力してください。
 - 「YYYY」は、Nuclias 用 AP 本体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 ケタです。
DBA-2820P の例：http://DBA-2820P-YYYY

既にアクセスポイントの IP アドレスが判明している場合は、IP アドレスを直接 URL 欄に入力します。

3. 接続に成功すると、以下のようなログイン画面が表示されます。

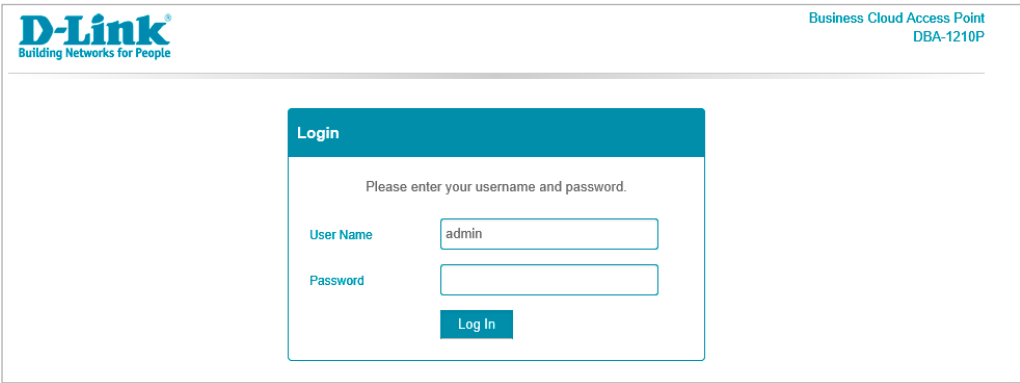


図 12-4 ログイン

4. 「User Name」と「Password」にユーザ名とパスワードを入力し、「Log In」をクリックします。
ユーザ名とパスワードの初期値は「admin」です。

アクセスポイントを Nuclias に登録後は、パスワードが変更されます。

変更済みのパスワードは、Nuclias の画面で確認できます。

- (1) モニタ > アクセスポイント > デバイス 画面でデバイス名をクリックします。
- (2) 「基本」タブの「ローカル資格情報」を確認します。

ステータス

ログインすると、下記の通りデバイスのステータス画面が表示されます。
ステータス画面では「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 Nuclias 用 AP についての様々な情報を参照できます。

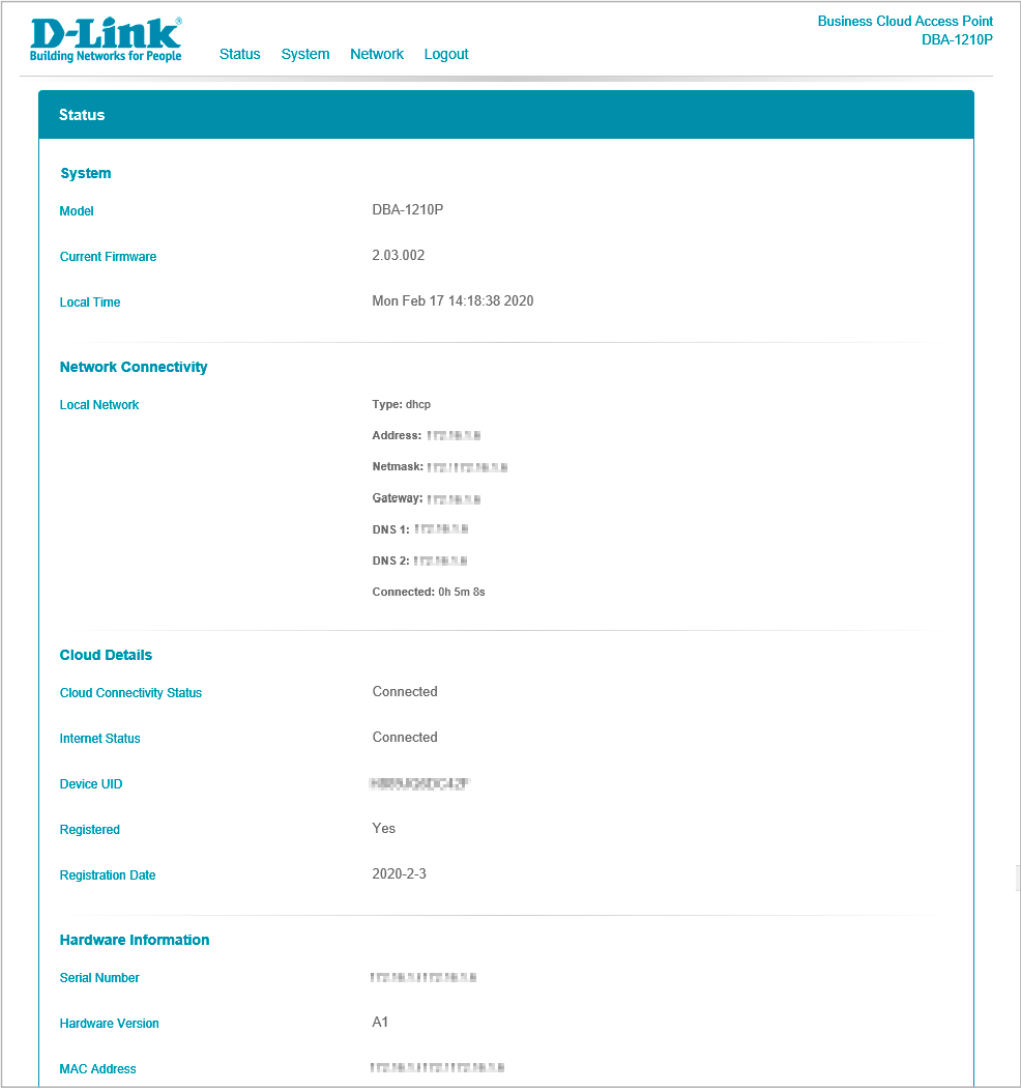


図 12-5 ステータス

本画面には以下の項目があります。

項目	説明
モデル	デバイスのモデル名（型番）を表示します。
現在のファームウェア	現在のファームウェアバージョンを表示します。
現地時刻	現地の時刻を表示します。 注意 Nuclias Cloud v2.0.x 以前に作成したサイトを、それ以降のバージョンで使用する場合、アクセスポイントの時間が UTC+8 になります。
ローカルネットワーク	ネットワーク設定を表示します。 - タイプ：DHCP、スタティック IP アドレスかを表示します。 - アドレス：IP アドレス（IPv4）を表示します。 - ネットマスク：サブネットマスクを表示します。 - ゲートウェイ：ゲートウェイの IP アドレスを表示します。 - DNS1（DNS2）：DNS サーバの IP アドレスを表示します。 - 接続時間：ローカルネットワーク接続後どのぐらい時間が経過したかを表示します。
クラウド接続ステータス	クラウドサーバ（Nuclias サーバ）に接続されているかを表示します。
インターネットステータス	デバイスがインターネット環境に接続されているかを表示します。
デバイス UID	本体のデバイス UID を表示します。
登録状況	UID が Nuclias に登録されている場合は「Yes」を表示します。Nuclias へ登録されていない場合は「No」です。
登録日	Nuclias に UID が登録され、デバイスがオンラインになった日を表示します。
シリアル番号	製品のシリアル番号を表示します。
ハードウェアバージョン	製品のハードウェアバージョンを表示します。
MAC アドレス	製品の LAN ポートの MAC アドレスを表示します。

システム > システム

システムでは、ホストネームの確認や NTP サーバの設定を行う事ができます。

D-Link®

Building Networks for People

StatusSystemNetworkLogout

Business Cloud Access Point
DBA-1210P

System

System Properties

Hostname

DBA-1210P-XXXX

Time Synchronization

NTP server candidates

ntp.nuclias.com

Apply

Cancel

図 12-6 システム

本画面には以下の項目があります。

項目	説明
ホスト名	本体のホスト名が記載されています。 命名規則は「DBA-XXXX- (MAC アドレス下 4 桁)」です。 ・「XXXX」は、Nuclias 用 AP の製品名です。
NTP サーバ	NTP サーバの情報を入力します。本製品には、初期状態で 3 つの NTP サーバが登録されています。 注意 NTP サーバで正常に時刻同期ができていない場合、Nuclias 上でデバイスに関するログが正常に収集されない場合があります。

「適用」をクリックし、設定を反映します。

システム > リセットとファームウェアアップグレード

本画面では、初期設定へのリセットとファームウェアアップグレードを行うことができます。

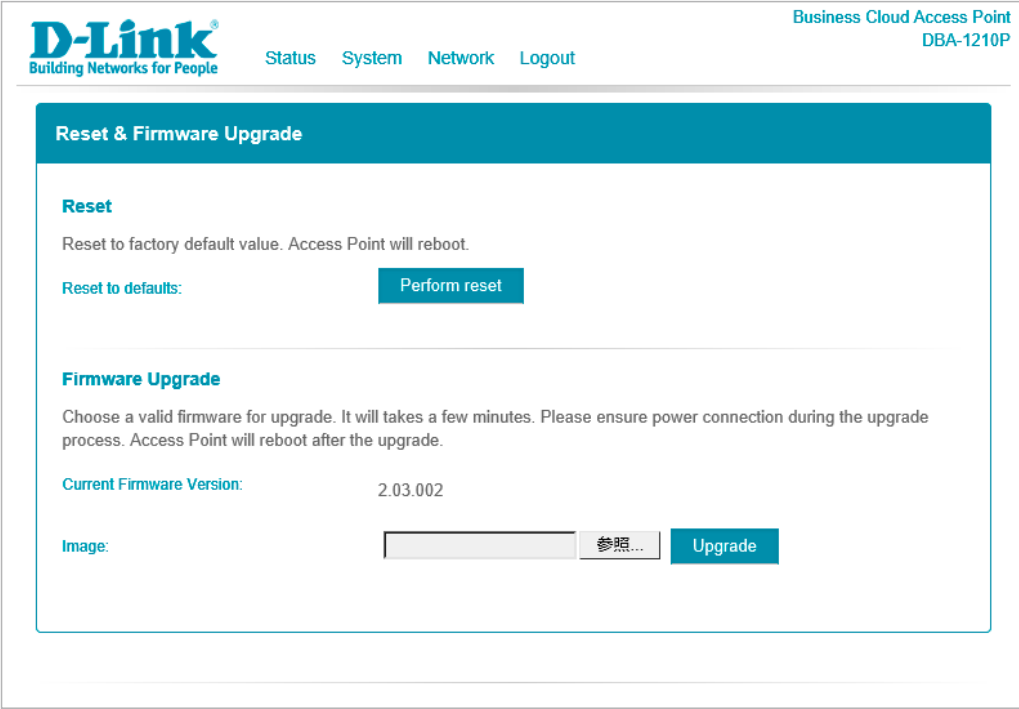


図 12-7 リセットとファームウェアアップグレード

本画面には以下の項目があります。

項目	説明
初期設定へのリセット	「リセットを実行する」をクリックし、本製品の設定を初期状態にリセットします。
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が表示されます。
イメージ	アップグレードするファームウェアを選択し、「アップグレード」をクリックします。

初期設定は「DHCP クライアント」です。スタティック IP を設定する場合は「接続タイプ」を「スタティック IP」に変更します。

図 12-8 ネットワーク - 基本設定

項目	説明
接続タイプ	DHCP クライアント、またはスタティック IP から選択します。 「DHCP client」: 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。 「Static IP」: 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。
DHCP が提供する DNS を使用	接続タイプで「DHCP client」を選択した場合のみ表示されます。 DHCP サーバが提供する DNS を使用する場合はチェックを入れます。DNS サーバの IP アドレスを指定する場合はチェックを外します。
カスタム DNS サーバ	DNS サーバの IP アドレスを入力します。接続タイプで「DHCP client」を選択した場合は、「DHCP が提供する DNS を使用」のチェックを外すと本項目が表示されます。
DHCP リクエスト時のホストネーム	接続タイプで「DHCP client」を選択した場合のみ表示されます。 ダイナミック DNS サーバを使用する際の、DHCP リクエスト時のホストネームを表示します。

「適用」をクリックし、設定を反映します。

ネットワーク > 高度な設定

IPv6、プロキシ、VLAN の設定を行います。

Business Cloud Access Point
DBA-1210P

StatusSystemNetworkLogout

Network

IPv6 Configuration

Enable IPv6☒

Proxy Configuration

Enable Proxy☐

Host

Port

VLAN Configuration

Enable VLAN☐

Management VLAN ID

VLAN Mode

Apply

Cancel

図 12-9 ネットワーク - 高度な設定

本画面には以下の項目があります。

項目	説明
IPv6 を有効にする	IPv6 経由でアクセスポイントの設定を行う機能を有効にします。
プロキシを有効にする	アクセスポイントをプロキシ経由で Nuclias サーバに接続する機能を有効にします。 注意 デバイスで使用するプロキシサーバは WebSocket をサポートしている必要があります。 注意 DBA-X5480P は Cloud サーバとの接続に IPv4 または IPv6 アドレスを使用しますが、プロキシサーバは IPv4 アドレスのみ指定可能です。
ホスト	プロキシサーバのホストを入力します。
ポート	プロキシサーバのポート番号を入力します。
VLAN を有効にする	VLAN 機能を有効にします。
マネジメント VLAN ID	マネジメント VLAN の ID を入力します。
VLAN モード	VLAN モードをタグ有 / タグ無から選択します。
リンクアグリゲーション (DBA-1210P/DBA-3621P/DBA-X1230P/DBA-X5480P を除く)	リンクアグリゲーションの設定を LACP、スタティック、無効から選択します。

「適用」をクリックし、設定を反映します。

注意

 DBA-X5480P の LAN(PoE) + LAN は同時利用できません。

注意

 DBA-X2830P には以下の制限があります。

Multi-Gigabit Ethernet Switch 対向で LACP を用いる場合、2.5Gbps (LAN1)、1Gbps (LAN2) の何れかが使用されます。再起動後の状態は通常 1Gbps (LAN2) 側が Bndl/Act になります。最後に Active だったリンクが継続して使用され、Preempt する事はありません。対向 Switch 側で 1Gbps 以下に落とす場合、LAN1/LAN2 bndl/bndl 運用が可能です。

ログアウト

Web GUI 上部の「Logout」をクリックすると Web GUI からログアウトし、ログイン画面が表示されます。

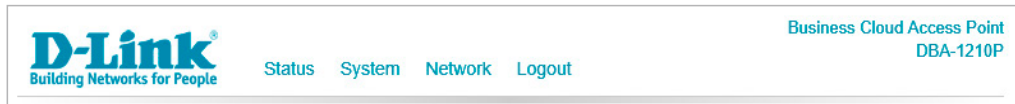


図 12-10 ログアウト

コマンドラインインタフェース (CLI) の設定

Nuclias を使用せずに AP へ直接接続し、設定を行うコマンドラインインタフェース (CLI) について説明します。

Nuclias AP の設定と管理は、基本的に「Nuclias」を使用して行いますが、一部の設定は CLI から行うことができます。DBA-1210P 以外の Nuclias AP は、CLI 設定に使用する 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して CLI から設定を行う場合、以下を準備してください。

- ・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

注意 DBA-1210P はコンソールポートを搭載していないため、CLI からの設定はできません。

注意 DBA-X5480P にはコンソールケーブルは同梱されていません。

端末をコンソールポートに接続する

ケーブルの接続

1. RJ-45/RS-232C 変換ケーブルの RS-232C コネクタを、シリアルポート搭載の端末またはコンピュータに接続します。
2. RJ-45/RS-232C 変換ケーブルの RJ-45 コネクタを、本製品のコンソールポートに接続します。

ターミナルソフトの設定

1. VT100 のエミュレーションが可能なターミナルソフトを起動します。
2. 「接続の設定」画面の「接続方法」で、適切なシリアルポート (COM 1 など) を選択します。
3. ターミナルソフトの設定を AP のシリアルポートの設定に合わせます。
AP のシリアルポートの設定は以下の通りです。
 - ・スピード: 「115200」
 - ・データ: 「8bit」
 - ・パリティ: 「なし (none)」
 - ・ストップビット: 「1bit」
 - ・フロー制御: 「なし (none)」

ログインとログアウト

1. ターミナルソフトの設定完了後、AP とシリアルポート搭載の端末またはコンピュータをケーブルで接続します。
2. AP の電源をいれます。ブートシーケンスが完了すると、ターミナルソフトにログイン画面が表示されます。
3. ユーザ名とパスワードを入力します。
ユーザ名とパスワードの初期値は「admin」です。
4. コマンドを入力して設定を行います。
5. CLI による設定を終了する場合は、「exit」コマンド使用するか、ターミナルソフトを終了します。

CLI コマンド一覧

DBA シリーズの CLI コマンドについて説明します。CLI コマンドを使用し、Nuclias AP の設定と設定情報の表示などを行うことができます。CLI から設定変更を行った場合、「apply」コマンドを実行して設定内容を適用してください。

■ ? コマンド

コマンド	動作
?	使用できるコマンドのリストを表示します。

■ set management コマンド

Nuclias AP の設定を行うコマンドです。

コマンド	動作
set management	
set management dhcp	IP アドレスを DHCP に設定します。
set management static static-ip <ip_address> mask <netmask> gateway <gateway>	IP アドレスをスタティックに設定します。「set management static」を実行すると <sub-config> モードになります。 <sub-config> モードで IP アドレス、サブネットマスク、ゲートウェイを指定してください。<sub-config> モードを終了するには「exit」を実行します。
set management vlan-id <UINT:vid>	VLAN ID を設定します。
set management vlan-enable [up down]	VLAN を有効または無効に設定します。
set management vlan-mode [tagged untagged]	VLAN モードを「タグ付き」または「タグなし」に設定します。
set management ipv6-enable [up down]	IPv6 を有効または無効に設定します。
set management proxy-enable [up down]	プロキシを有効または無効に設定します。 注意 デバイスで使用するプロキシサーバは WebSocket をサポートしている必要があります。
set management proxy-host <STRING:host>	プロキシホストを設定します。
set management proxy-port <UINT:port>	プロキシポートを設定します。
set management link-aggregation-mode [down lacp static]	リンクアグリゲーションモードを「無効」「LACP」「スタティック」に設定します。
set management link-aggregation-trunk-hash-mode [da sa da-sa dip sip dip-sip]	リンクアグリゲーションのトランクハッシュモードを設定します。
set host	
set host dns-via-dhcp [up down]	DHCP サーバが提供する DNS を使用します。
set host dns <IPv4ADDR:staticDns1>	DNS サーバの IP アドレスを設定します。
set ntp	
set ntp server <STRING:svrAddr1>	NTP サーバを設定します。

■ get management コマンド

Nuclias AP の設定内容を表示するコマンドです。

コマンド	動作
get management	
get management	AP のインタフェース情報を表示します。IP アドレス、MAC アドレス、VLAN 設定、プロキシ設定、リンクアグリゲーション設定を確認できます。
get management mac	MAC アドレスを表示します。
get management ip	IP アドレスを表示します。
get management static-ip	スタティック IP アドレスを表示します。
get management static-mask	IP アドレスがスタティックの場合のサブネットマスクを表示します。
get management static-gateway	IP アドレスがスタティックの場合のゲートウェイを表示します。
get management vlan-id	VLAN ID を表示します。
get management vlan-enable	VLAN の設定（有効または無効）を表示します。
get management vlan-mode	VLAN モード（「タグ付き」または「タグなし」）を表示します。
get management dhcp-status	DHCP の設定（有効または無効）を表示します。
get management ipv6-enable	IPv6 の設定（有効または無効）を表示します。
get management proxy-enable	プロキシの設定（有効または無効）を表示します。
get management proxy-host	プロキシホストの設定（ホスト名）を表示します。
get management proxy-port	プロキシポートの設定（ポート番号）を表示します。

第12章 Web GUI、CLIからの設定について

コマンド	動作
get management link-aggregation-mode	リンクアグリゲーションの設定 (LACP/ スタティック / 無効) を表示します。
get management link-aggregation-trunk-hash-mode	リンクアグリゲーションのトランクハッシュモードを表示します。
get system	
get system	製品名やシリアルナンバーなど、Nuclias AP のデバイス情報を表示します。
get system model	製品名を表示します。
get system serial-number	シリアルナンバーを表示します。
get system device-uid	デバイス UID を表示します。
get system version	ファームウェアバージョンを表示します。
get system cloud-registration	Nuclias クラウドへの登録状態を表示します。
get system date-of-registration	Nuclias クラウドに登録された日時を表示します。
get system local-network-status	ローカルネットワークへの接続状態を表示します。
get system internet-status	インターネットへの接続状態を表示します。
get system cloud-connect-status	Nuclias クラウドへの接続状態を表示します。
get host	
get host dns-via-dhcp	DHCP 経由の DNS ホストの設定を表示します。
get host dns	DNS ホストの情報を表示します。
get ntp server	
get ntp server	NTP サーバの情報を表示します。
get radio	
get radio [radio0 radio1] channel	指定帯域のチャンネルを表示します。 ※パラメータは製品により異なります。「?」オプションでヘルプ情報をご確認ください。
get vap	
get vap [vap0 vap1 vap2 vap3 vap4 vap5 vap6 vap7] radio [radio0 radio1] [ssid wpa-personal-key]	SSID 名と PSK を表示します。 ※パラメータは製品により異なります。「?」オプションでヘルプ情報をご確認ください。

■ firmware-upgrade コマンド

コマンド	動作
firmware-upgrade <STRING:url>	ファームウェアのアップグレードを行います。

■ reboot コマンド

コマンド	動作
reboot	再起動を行います。

■ apply コマンド

コマンド	動作
apply	設定を適用します。

■ exit コマンド

コマンド	動作
exit	CLI からログアウトします。 また、<sub-config> モードを終了する場合に使用します。

■ ライセンスの開始日と期限日について

ライセンスキーの「開始日」は、そのライセンスキーを適用させたデバイスが最初に Nuclias に接続され、オンラインになった日です。開始日が決まると自動的に期限日も決まり、この期限日は変更することはできません。
一度オンラインにすると、その後デバイスがオフラインになった場合やデバイスの登録が解除された場合でも、ライセンスは使用中の状態を継続しますのでご注意ください。

■ 機器交換時のライセンスの適用について

デバイスの故障などにより機器交換が必要になった際、Nuclias サイト上のデバイス削除や新デバイスの追加操作は、お客様自身（管理者権限のユーザ）にて実施頂きます。
新デバイスを登録する際は、故障デバイスが使用していたライセンスキーを適用することができます。
これによりデバイスが元々所有しているライセンスキーは未使用の状態になるため、別途有効に使用することができるようになります。

- 故障したデバイスの削除は、**設定 > アクセスポイント > デバイス**画面、または**管理 > インベントリ**画面から実行できます。
デバイスを削除すると、そのデバイスに紐づけられていたライセンスはどのデバイスにも紐づけられていない状態となり、他のデバイスに紐づけられるようになります。
- 新しいデバイスとライセンスの追加方法については、「[デバイスの追加](#)」を参照してください。

付録 B E メール認証時の画面

キャプティブポータルの E メール認証時に、サーバから入力されたメールアドレスに送付されるメールは以下の通りです。

タイトル	Verify your email to use Wi-Fi
送信元	D-Link Nuclias <verify@nuclias.com>
本文	Dear Wi-Fi guest user, Welcome. Please click the link to continue Wi-Fi use. https://mail.redirect.nuclias.com/email_url.ccp?tid=1234567890123456&email=XXXXXXxxxxXXXxxxxxXXXXxxxxxXXXXxxxxx ようこそ！ Wi-Fiの使用を続けるには、上記のリンクをクリックしてください。 환영합니다! Wi-Fi를 계속 사용하시려면 위의 링크를 클릭해 주십시오. 欢迎!请单击上面的链接继续使用Wi-Fi。 Bienvenue! Veuillez cliquer sur le lien ci-dessus pour continuer à utiliser le Wi-Fi. Benvenuto! Fare clic sul collegamento sopra per continuare a utilizzare il Wi-Fi. ¡Bienvenido! Haga clic en el enlace anterior para continuar con el uso de Wi-Fi. Herzlich willkommen! Bitte klicken Sie auf den obigen Link, um die Wi-Fi-Nutzung fortzusetzen. Powered by Nuclias Cloud

※記載される URL は、送付されるメールによって異なります。

付録 C 機器故障の際は

本製品 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/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-services/support-info/>

注意 製品保証に基づく修理のご依頼、並びに有償保守サービスやその他理由による機器交換を頂く場合、必ず事前にお客様にて Nuclias からデバイス UID 削除をし、元々紐づいていたライセンスキーを交換後の AP で使用できる状態にしてください。
もしデバイス UID の削除を実施しておらず、交換後の AP にて新しいライセンスを適用することになった場合でも、苦情およびライセンス期間の延長等はお請けできません。

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 の削除はできません。そのためデバイス UID 削除を忘れたことによる、苦情およびライセンス期間の延長、代替ライセンスの配布等はお請けできません。