D-Link DBG シリーズ

D-Link Nuclias – Cloud networking solution

ユーザマニュアル

D-Link
Building Networks for People

安全にお使いいただくために

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

安全上のご注意　必ずお守りください

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

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

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

⚠危険

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

⃠ 禁止 **ぬれた手でさわらない**
感電の原因となります。

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

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

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

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

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

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

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

⚠警告

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

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

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

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

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

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

⃠ 禁止 **ケーブル / コード類や端子を破損させない**
無理なねじり、引っ張り、加工、重いものの下敷きなどは、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。

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

⃠ 禁止 **各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほ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。

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

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

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

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

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

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

❗ **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。

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

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

⚠警告

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

⚠注意

- 禁止 乳幼児の手の届く場所では使わない
  やけど、ケガまたは感電の原因となります。
- 静電気注意
  コネクタや電源プラグの金属端子に触れたり、
  帯電したものを近づけますと故障の原因となります。
- 禁止 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。
- 禁止 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。
- 禁止 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。
- 禁止 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。
- 禁止 子供が使用する場合は、保護者が取扱いの方法を教え、
  誤った使い方をさせない
  けがや故障などの原因となります。
- 本製品を長時間連続使用する場合は、
  温度が高くなることがあるため、注意する。
  また、使用中に眠ってしまうなどして、
  意図せず長時間触れることがないようにする
  温度の高い部分に直接長時間触れると
  お客様の体質や体調によっては肌の赤みや
  かゆみ、かぶれ、低温やけどの原因となります。
- 禁止 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。
- 禁止 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。

VCCI - B

ご使用上の注意

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

- マニュアルなどに記載されている以外の方法での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。踏みつけられたり躓いたりしない位置に、ケーブルと電源コードを配線し、コンセントに差し込んでください。また、ケーブル上に物を置いたりしないようにしてください。
- 電源ケーブルや電源プラグを改造しないでください。
- システムに対応しているホットプラグ可能な電源装置に電源を接続したり、切り離したりする際には、以下の注意を守ってください。
  - 電源装置を取り付ける場合は、電源装置を取り付けてから、電源ケーブルを電源装置に接続してください。
  - 電源装置を取り外す場合は、事前に電源ケーブルを抜いておいてください。
  - システムに複数の電源がある場合、システムから電源を切り離すには、すべての電源ケーブルを電源装置から抜いておいてください。
- 抜け防止機構のあるコンセントをご使用の場合、そのコンセントの取り扱い説明書に従ってください。
- 本製品は動作中に高温になる場合があります。本製品の移動や取り外しの際には、ご注意ください。
- 本製品は動作中に高温になる場合がありますが、手で触れることができる温度であれば故障ではありません。ただし長時間触れたまま使用しないでください。低温やけどの原因になります。
- 市販のオプション品や他社製品を使用する場合、当社では動作保証は致しませんので、予めご了承ください。
- 製品に貼られているラベルや「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、必ず製品の電源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アダプタを再度接続します。

ラック搭載型製品に関する一般的な注意事項

ラックの安定性および安全性に関する以下の注意事項を遵守してください。また、システムおよびラックに付随する、ラック設置マニュアル中の注意事項や手順についてもよくお読みください。

- システムとは、ラックに搭載されるコンポーネントを指しています。コンポーネントはシステムや各種周辺デバイスや付属するハードウェアも含みます。

警告 前面および側面のスタビライザを装着せずに、システムをラックに搭載すると、ラックが倒れ、人身事故を引き起こす場合があります。ラックにシステムを搭載する前には、必ずスタビライザを装着してください。

警告 接地用伝導体を壊したり、接地用伝導体を適切に取り付けないで装置を操作しないでください。適切な接地ができるかわからない場合、電気保安協会または電気工事士にお問い合わせください。

警告 システムのシャーシは、ラックキャビネットのフレームにしっかり接地される必要があります。接地ケーブルを接続してから、システムに電源を接続してください。電源および安全用接地配線が完了したら、資格を持つ電気検査技師が検査する必要があります。安全用接地ケーブルを配線しなかったり、接続されていない場合、エネルギーハザードが起こります。

- ラックにシステム / コンポーネントを搭載した後は、一度にスライド・アセンブリに乗せて引き出すコンポーネントは 1 つのみとしてください。2 つ以上のコンポーネントが引き出されると、ラックがバランスを失い、倒れて重大な事故につながる恐れがあります。
- ラックに装置を搭載する前に、スタビライザがしっかりとラックに固定されているか、床面まで到達しているか、ラック全体の重量がすべて床にかかるようになっているかをよく確認してください。ラックに搭載する前に、シングルラックには前面および側面のスタビライザを、複数結合型のラックには前面用スタビライザを装着してください。
- ラックへの装置の搭載は、常に下から上へ、また最も重いものから行ってください。
- ラックからコンポーネントを引き出す際には、ラックが水平で、安定しているかどうか確認してから行ってください。
- コンポーネントレール解除ラッチを押して、ラックから、またはラックへコンポーネントをスライドさせる際は、指をスライドレールに挟まないよう、気をつけて行ってください。
- ラックに電源を供給する AC 電源分岐回路に過剰な負荷をかけないでください。ラックの合計負荷が、分岐回路の定格の 80 パーセントを超えないようにしてください。
- ラック内部のコンポーネントに適切な空気流があることを確認してください。
- ラック内の他のシステムを保守する際には、システムやコンポーネントを踏みつけたり、その上に立ったりしないでください。

注意 資格を持つ電気工事士が、DC 電源への接続と接地を行う必要があります。すべての電気配線が、お住まいの地域、および国の電気基準と規制に準拠していることを確認してください。

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、空港やコーヒーショップ、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。

※本機の最大通信速度ではありません。

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）
- コンピュータウィルスなどを流しデータやシステムを破壊する（破壊）

本来、無線 LAN カードや無線アクセスポイントは、これらの問題に対応するためのセキュリティの仕組みを持っていますので、無線 LAN 製品のセキュリティに関する設定を行って製品を使用することで、その問題が発生する可能性は少なくなります。
セキュリティの設定を行わないで使用した場合の問題を充分理解した上で、お客様自身の判断と責任においてセキュリティに関する設定を行い、製品を使用することをお奨めします。

このたびは、弊社製品をお買い上げいただきありがとうございます。
本書は、製品を正しくお使いいただくための取扱説明書です。
必要な場合には、いつでもご覧いただけますよう大切に保管してください。
また、必ず本書、設置マニュアル、および弊社 WEB に掲載された製品保証規程をよくお読みいただき、内容をご理解いただいた上で、記載事項に従ってご使用ください。

製品保証規定は以下を参照ください。
https://www.dlink-jp.com/support/info/product-assurance-provision.html

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、ご使用の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

目次

はじめに

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。

- DBG-2000/B1
- DBG-X1000/A1

第 1 章　Nuclias の概要

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。

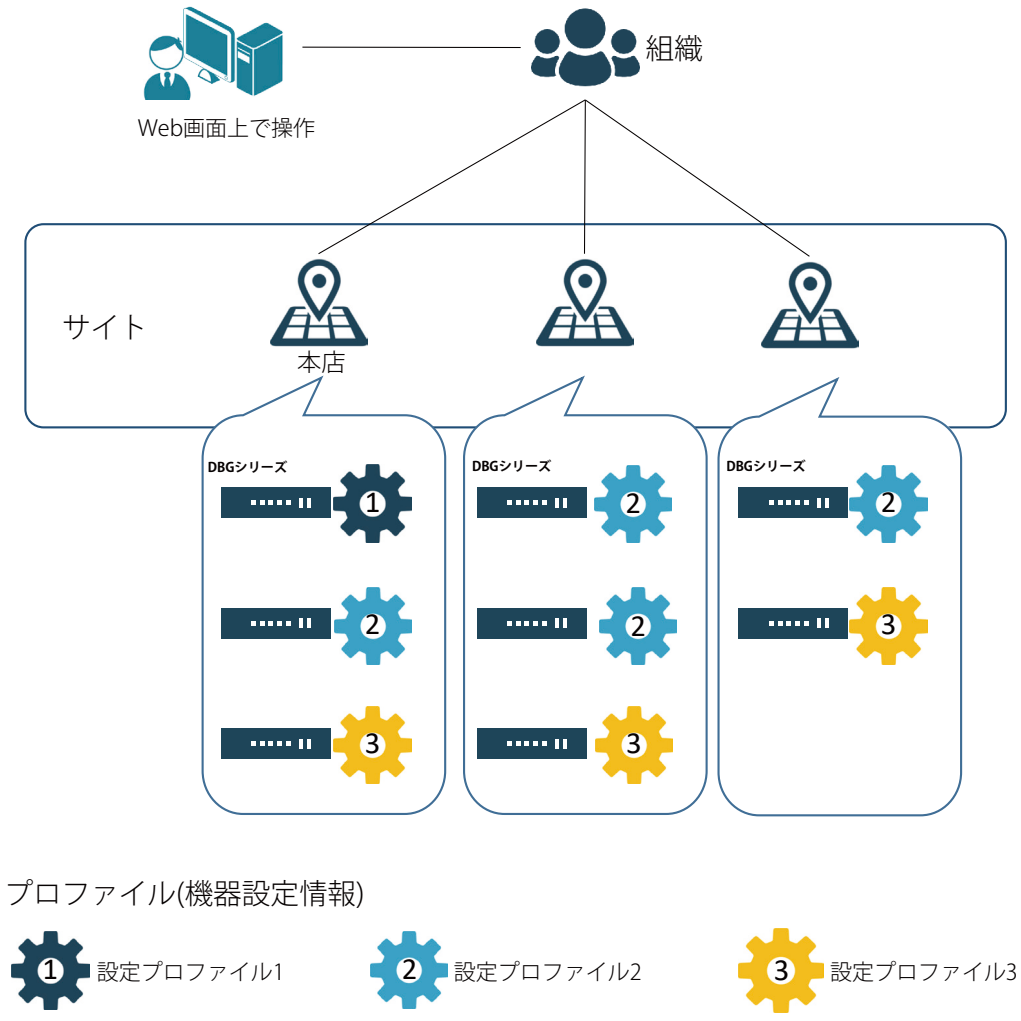


図 1-1　Nuclias 構成概要

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。 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。（2024 年 5 月現在）

■ DBA シリーズ

DBA-1210P※

DBA-2520P

DBA-2620P※

DBA-2720P※

DBA-2820P※

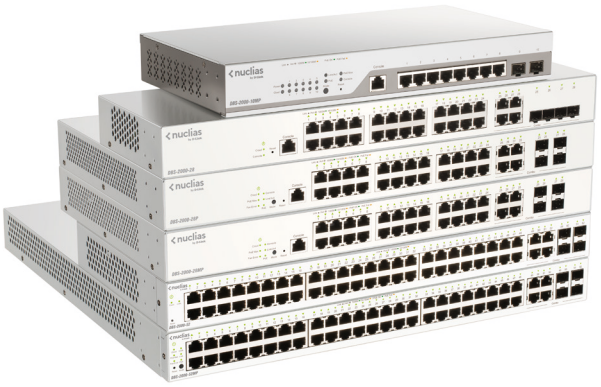
DBA-3621P

DBA-X2830P

DBA-X1230P

※ 販売終了

■ 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、リンクアップをし、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」、および、ドメイン名から IP アドレス（または、その逆）への変換（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)	IP アドレス取得用 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。

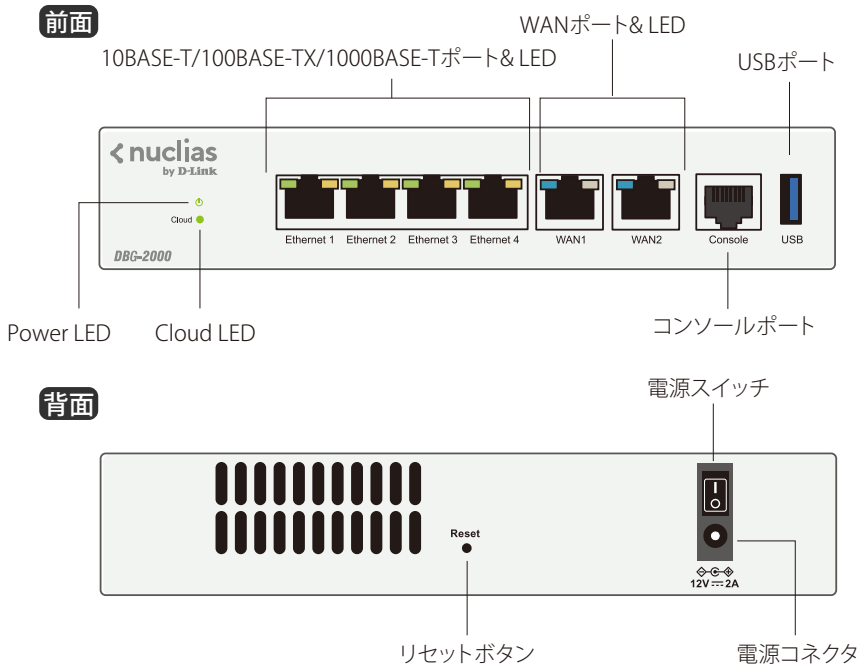
- Google Chrome

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　DBG シリーズのご利用にあたって

DBG-2000 の各部名称

本製品の各部名称について記載します。
LED 表示の詳細については「DBG-2000 LED 表示」を参照してください。



注意　コンソールポート、および USB ポートは未サポートです。

DBG-2000 前面パネルについて

■ LED
システム LED は、電源や Nuclias への接続状態など、本製品のシステムの状態を表します。詳細は「DBG-2000 システム LED」を参照してください。
ポート LED は、ポートのデータ送受信やリンクの状態を表します。詳細は「DBG-2000 LAN ポート LED」「DBG-2000 WAN ポート LED」を参照してください。

■ 10BASE-T/100BASE-TX/1000BASE-T ポート（Ethernet 1/2/3/4 ポート）
ネットワーク ケーブルを使用し、PC、スイッチなどのイーサネットデバイスを接続します。
「Ethernet 1/2/3/4 」ポートは「LAN」ポートです。「WAN」「DMZ」への変更はできません。

■ WAN1 ポート /WAN2 ポート
ネットワークケーブルを使用し、ケーブルモデムまたは DSL モデムなどに接続します。

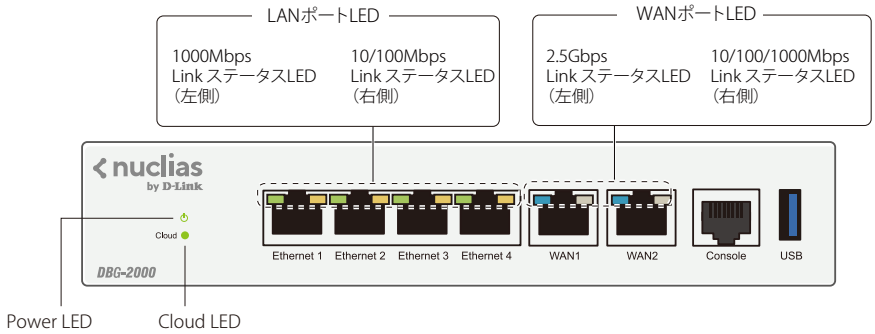
■ コンソールポート
未サポートです。

■ USB ポート
未サポートです。

● DBG-2000 LAN/WAN ポートの初期設定について

ポート	IP アドレスタイプ	IP アドレス	ローカル Web GUI への接続	DHCP サーバ
LAN（Ethernet 1/2/3/4）ポート	Static IP	192.168.10.1	可	有効
WAN1 ポート	DHCP Client	0.0.0.0	不可	無効

DBG-2000 LED 表示



以下の表に LED の状態が意味する本製品の状態を示します。

■ DBG-2000 システム LED

LED	色	状態	状態説明
Power	橙	点灯	電源がオンになり、起動中です。
	緑	点灯	起動が完了し、電源が供給されています。
	ー	消灯	電源が供給されていません。
Cloud	橙	点灯	Nuclias への接続を試みています。
	橙	点滅	ファームウェアのアップグレードを実行しています。 または、工場出荷時設定へのリセットを実行しています。
	緑	点灯	Nuclias と正常に接続されています。
	赤	点灯	Nuclias と接続していません。
	赤	点滅	Nuclias クラウドの設定画面から、「LED 点滅」を実行しています。 「LED 点滅」は**モニタ > ゲートウェイ > デバイス**の順にクリックし、デバイスを選択 →「ツール」タブの「LED 点滅」から実行します。
	ー	消灯	電源が供給されていません。

■ DBG-2000 LAN ポート LED

LED	色	状態	状態説明
1000Mbps Link ステータス LED（左側）	緑	点灯	1000Mbps でリンクが確立しています。
	緑	点滅	1000Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
10/100Mbps Link ステータス LED（右側）	橙	点灯	10/100Mbps でリンクが確立しています。
	橙	点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

■ DBG-2000 WAN ポート LED

LED	色	状態	状態説明
2.5Gbps Link ステータス LED（左側）	青	点灯	2.5Gbps でリンクが確立しています。
	青	点滅	2.5Gbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。
10/100/1000Mbps Link ステータス LED（右側）	緑	点灯	1000Mbps でリンクが確立しています。
	橙	点灯	10/100Mbps でリンクが確立しています。
	緑	点滅	1000Mbps でデータを送受信しています。
	橙	点滅	10/100Mbps でデータを送受信しています。
	ー	消灯	リンクが確立していません。

DBG-2000 背面パネルについて

■　電源スイッチ
電源のオン / オフを行います。

■　電源コネクタ
付属の AC アダプタを接続します。

■　Reset ボタン
設定を工場出荷時の状態にリセットする場合に使用します。
設定のリセットを実行する場合、リセットボタンを 7 ～ 10 秒間押下し続けてから手を離してください。

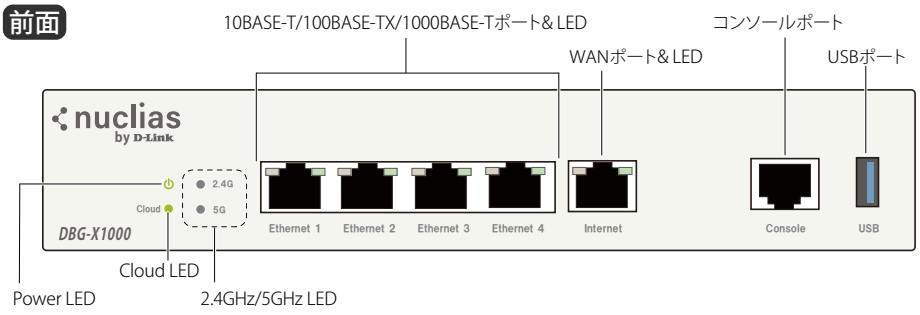
注意　リセットは、DBG-2000 の WAN 側のネットワークケーブルを抜いた状態で行ってください。

注意　リセットボタンは 16 秒以上押下し続けないようにしてください。

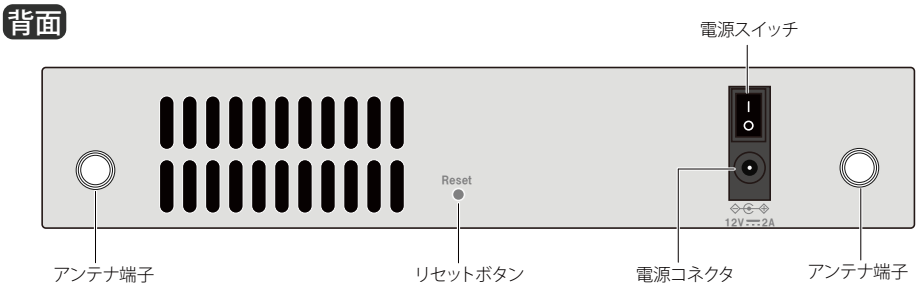
DBG-X1000 の各部名称

本製品の各部名称について記載します。
LED 表示の詳細については「DBG-X1000 システム LED」を参照してください。

前面



背面



注意　コンソールポート、および USB ポートは未サポートです。

DBG-X1000 前面パネルについて

■　LED
システム LED は、電源や Nuclias への接続状態など、本製品のシステムの状態を表します。詳細は「DBG-X1000 システム LED」参照してください。
ポート LED は、ポートのデータ送受信やリンクの状態を表します。詳細は「DBG-X1000 ポート LED」参照してください。

■　10BASE-T/100BASE-TX/1000BASE-T ポート（Ethernet 1/2/3/4 ポート）
ネットワーク ケーブルを使用し、PC、スイッチなどのイーサネットデバイスを接続します。
「Ethernet 1/2/3/4 」ポートは「LAN」ポートです。「WAN」「DMZ」への変更はできません。

■　WAN ポート（Internet ポート）
ネットワークケーブルを使用し、ケーブルモデムまたは DSL モデムなどに接続します。

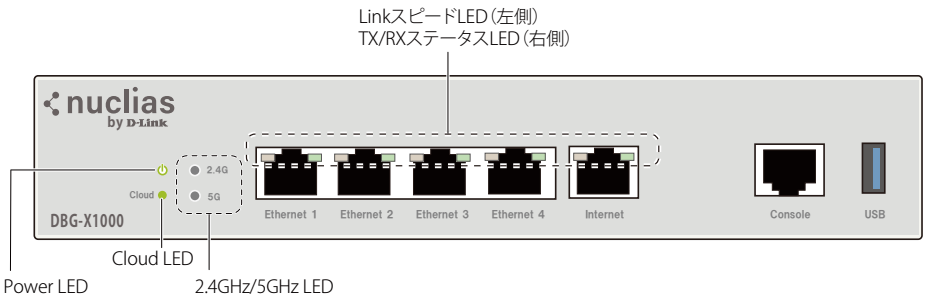
■　コンソールポート
未サポートです。

■　USB ポート
未サポートです。

● DBG-X1000 LAN/WAN ポートの初期設定について

ポート	IP アドレスタイプ	IP アドレス	ローカル Web GUI への接続	DHCP サーバ
LAN（Ethernet 1/2/3/4）ポート	Static IP	192.168.10.1	可	有効
WAN（Internet）ポート	DHCP Client	0.0.0.0	不可	無効

DBG-X1000 LED 表示



以下の表に LED の状態が意味する本製品の状態を示します。

■ DBG-X1000 システム LED

LED	色	状態	状態説明
Power	橙	点灯	電源がオンになり、起動中です。
	緑	点灯	起動が完了し、電源が供給されています。
	ー	消灯	電源が供給されていません。
Cloud	橙	点灯	Nuclias への接続を試みています。
	橙	点滅	ファームウェアのアップグレードを実行しています。 または、工場出荷時設定へのリセットを実行しています。
	緑	点灯	Nuclias と正常に接続されています。
	赤	点灯	Nuclias と接続していません。
	赤	点滅	Nuclias クラウドの設定画面から、「LED 点滅」を実行しています。 「LED 点滅」は**モニタ > ゲートウェイ > デバイス**の順にクリックし、デバイスを選択 →「ツール」タブの「LED 点滅」から実行します。
	ー	消灯	電源が供給されていません。
2.4GHz LED	緑	点灯	無線 LAN（2.4GHz）による通信が可能です。
	緑	点滅	データを送受信しています。
	ー	消灯	無線 LAN（2.4GHz）による通信が利用できません。
5GHz LED	緑	点灯	無線 LAN（5GHz）による通信が可能です。
	緑	点滅	データを送受信しています。
	ー	消灯	無線 LAN（5GHz）による通信が利用できません。

■ DBG-X1000 ポート LED

LED	色	状態	状態説明
Link スピード LED（左側）	緑	点灯	速度は 1000Mbps です。
	橙	点灯	速度は 100Mbps です。
	ー	消灯	速度は 10Mbps です。
TX/RX ステータス LED（右側）	緑	点灯	リンクが確立しています。
	緑	点滅	データを送受信しています。
	ー	消灯	リンクが確立していません。

DBG-X1000 背面パネルについて

■ 電源スイッチ
電源のオン / オフを行います。

■ 電源コネクタ
付属の AC アダプタを接続します。

■ Reset ボタン
設定を工場出荷時の状態にリセットする場合に使用します。
設定のリセットを実行する場合、リセットボタンを 7 ～ 10 秒間押下し続けてから手を離してください。

注意 リセットは、DBG-X1000 の WAN 側のネットワークケーブルを抜いた状態で行ってください。

注意 リセットボタンは 16 秒以上押下し続けないようにしてください。

第 3 章　DBG シリーズの設置

DBG-2000 の設置

DBG-2000 設置前の準備

本製品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。

- 動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- 換気のため、少なくとも製品の前後に 7.62cm（3 inches）以上の空間を保つようにしてください。
- 本製品側面の通気孔をふさいでしまう構造のラックには設置しないでください。扉の閉められるラックに設置する場合は、ファンやルーバーなどによって適切な換気ができることを確認してください。
- 設置前に、以下の環境に該当しないことを確認してください。
  - 設置面が湿っている、または濡れている
  - 接地が正しく行われていない

DBG-2000 ゴム足の取り付け

同梱されているゴム足を本製品裏面の四隅に取り付けます。本製品の周囲に十分な通気を確保するようにしてください。

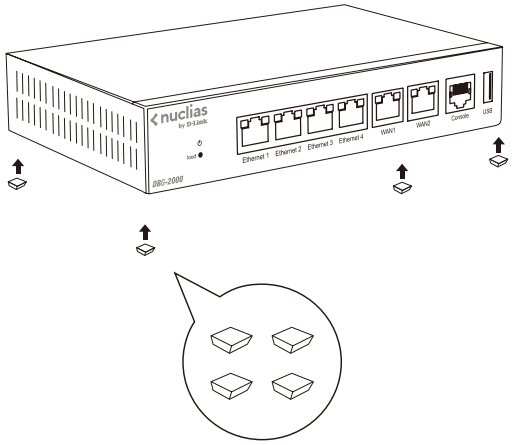


図 3-1　DBG-2000 ゴム足の取り付け

DBG-2000 ネットワーク接続前の準備

ネットワークへの接続方法は以下の通りです。

- ネットワークケーブルの一端を「WAN1」ポートに接続します。
  もう一端はモデム、ISP などに接続します。

- 別のネットワークケーブルの一端を「Ethernet 1/2/3/4」ポートのいずれかに接続します。
  もう一端はスイッチ、または LAN ネットワークセグメント内の PC に接続します。

DBG-2000 電源の投入

1. ネットワークケーブルが「DBG-2000 ネットワーク接続前の準備」のとおりに接続されていることを確認します。
2. 電源ケーブルを本製品の電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
3. 電源スイッチを ON にします。本製品の起動中は Power LED が橙色に点灯し、起動が完了すると緑色に点灯します。

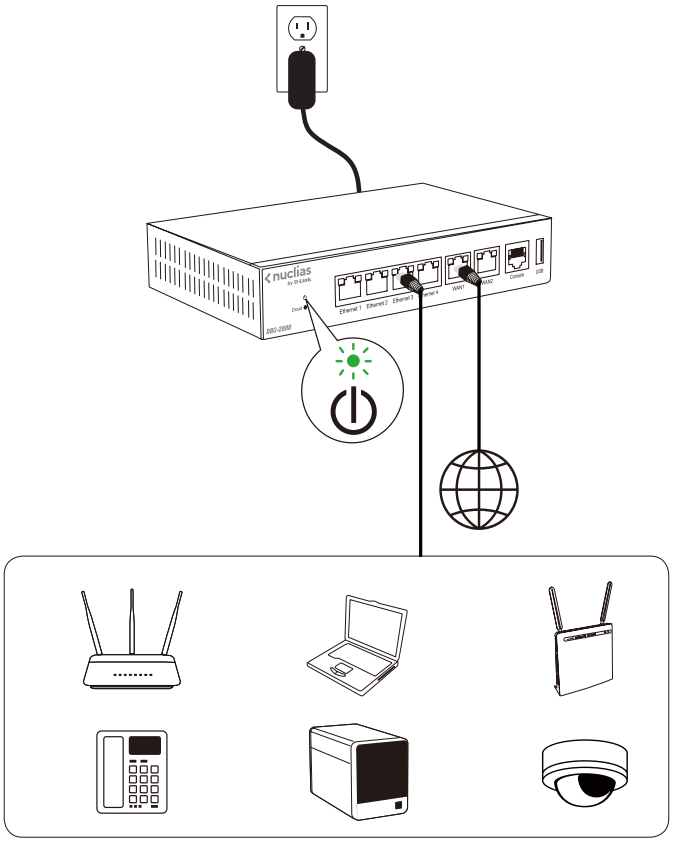


図 3-2　接続図

DBG-X1000 の設置

DBG-X1000 設置前の準備

本製品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。

- 電源に接続されていない状態で設置を行ってください。
- 動作環境範囲内の温度と湿度を保つことができる、なるべく涼しくて乾燥した場所に設置してください。
- 換気のため、少なくとも製品の前後に 7.62cm（3 inches）以上の空間を保つようにしてください。
- 本製品側面の通気孔をふさいでしまう構造のラックには設置しないでください。扉の閉められるラックに設置する場合は、ファンやルーバーなどによって適切な換気ができることを確認してください。
- 設置前に、以下の環境に該当しないことを確認してください。
    - 設置面が湿っている、または濡れている
    - 接地が正しく行われていない

DBG-X1000 ゴム足の取り付け

同梱されているゴム足を本製品裏面の四隅に取り付けます。本製品の周囲に十分な通気を確保するようにしてください。

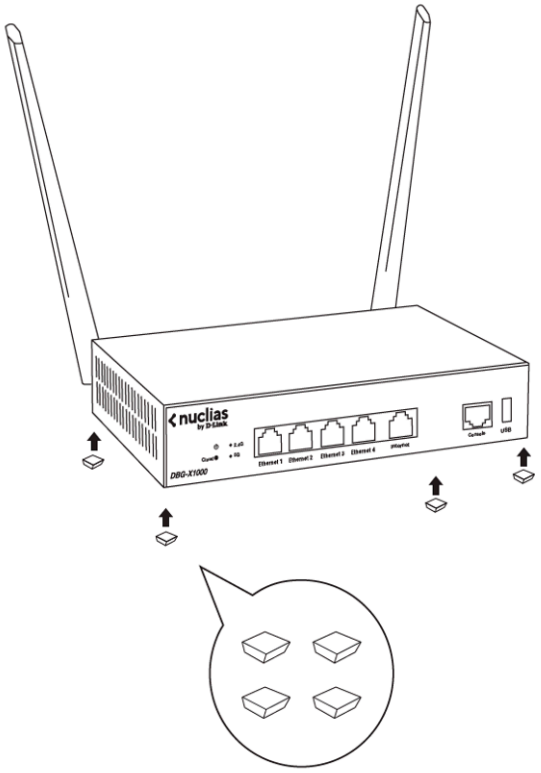


図 3-3　DBG-X1000 ゴム足の取り付け

DBG-X1000 ネットワークへの接続方法

ネットワークへの接続方法は以下の通りです。

- ネットワークケーブルの一端を「Internet」ポートに接続します。
  もう一端はモデム、ISP などに接続します。

- 別のネットワークケーブルの一端を「Ethernet 1」「Ethernet 2」「Ethernet 3」「Ethernet 4」ポートのいずれかに接続します。
  もう一端はスイッチ、または LAN ネットワークセグメント内の PC に接続します。

DBG-X1000 電源の投入

1. ネットワークケーブルが「DBG-X1000 ネットワークへの接続方法」のとおりに接続されていることを確認します。
2. 電源ケーブルを本製品の電源コネクタに接続します。電源ケーブルのプラグを電源コンセントに接続します。
3. 電源スイッチを ON にします。本製品の起動中は Power LED が橙色に点灯し、起動が完了すると緑色に点灯します。

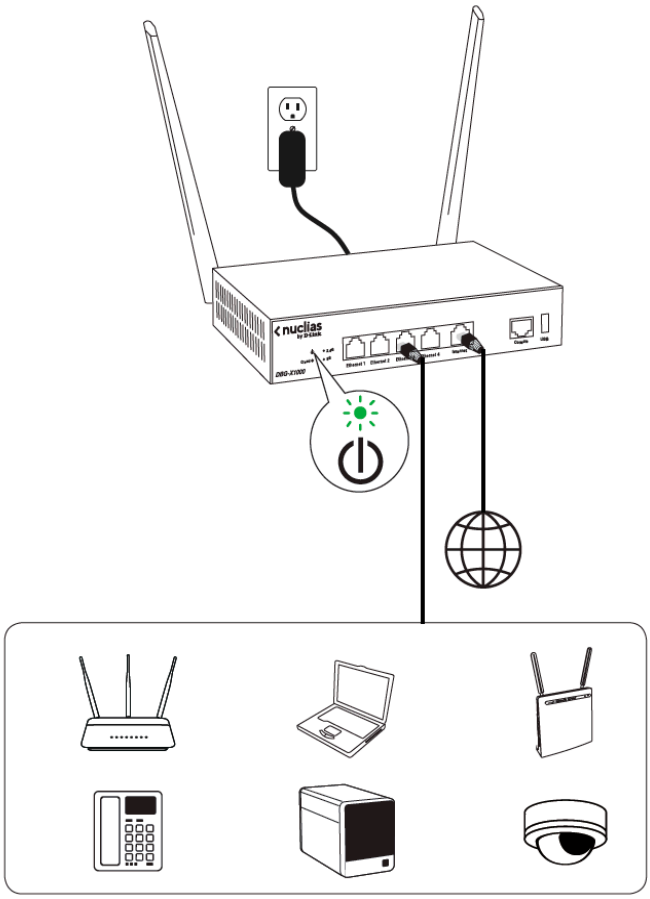


図 3-4　DBG-X1000 接続図

DBG シリーズの設定について

DBG シリーズの接続方法

DBG シリーズの設定や管理は、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、Nuclias クラウドで設定を行うことで、Nuclias クラウドに登録した複数の DBG シリーズ を一度に設定・管理できます。

注意 WAN 設定はデフォルトで DHCP クライアントとなっており、Nuclias 用ゲートウェイが DHCP 経由でクラウドの Nuclias ポータルに接続可能である場合、ローカル Web GUI からのネットワーク設定を行わずに Nuclias Cloud からデバイス設定を行うことができます。

注意 ローカル Web GUI からは、ネットワーク設定など、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 4 章　Web GUI の設定」を参照してください。

Nuclias を経由した接続例

以下は Nuclias を経由した接続例の図です。
Nuclias 経由で DBG シリーズ とコンピュータを接続します。複数の DBG シリーズ を一度に設定、管理することができます。

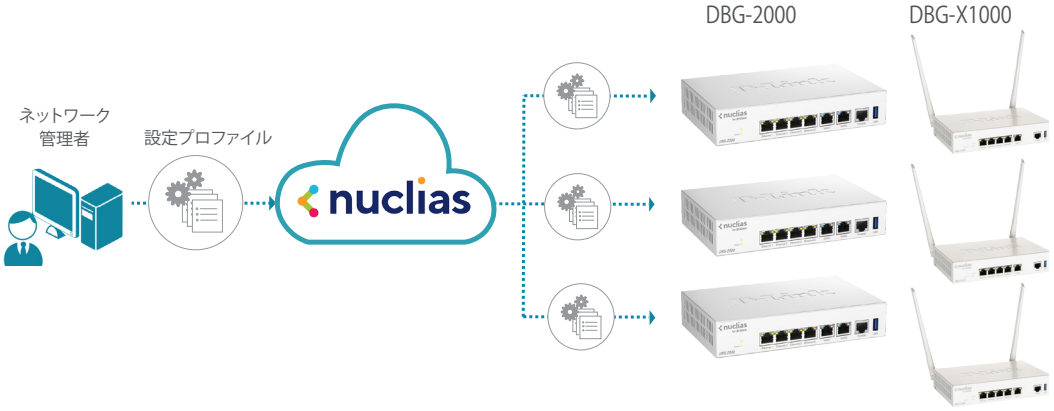


図 3-5　Nuclias を経由した接続例

具体的な接続設定方法については、第 5 章以降の章を参照してください。

■ Nuclias に接続する前の準備

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 からはインターネット設定など、一部の項目のみ設定することができます）

図 3-6　直接接続

● ローカル Web GUI へのログイン方法

直接接続には「Ethernet 1/2/3/4」のいずれかのポートを使用できます。
いずれのポートを使用した場合でも、ローカル Web GUI のアドレスは同一です。

- ローカル Web GUI のアドレス：「 http://192.168.10.1/ 」

ログインに使用するユーザ名とパスワードの初期値は以下のとおりです。

- ユーザ名：「admin」
- パスワード：「admin」

Web GUI の詳細は「第 4 章　Web GUI の設定」を参照してください。

第 4 章　Web GUI 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 DBG シリーズに直接アクセスし、ブラウザで設定を行う「Web GUI」について説明します。

注意　WAN 設定はデフォルトで DHCP クライアントとなっており、Nuclias 用ゲートウェイが DHCP 経由でクラウドの Nuclias ポータルに接続可能である場合、ローカル Web UI からのネットワーク設定を行わずに Nuclias Cloud からデバイス設定を行うことができます。

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。
その他の設定項目については、Nuclias クラウドから設定を行ってください。

- ネットワーク設定
- NTP サーバの設定
- 工場出荷時設定へのリセット
- ファームウェアアップグレード

注意　リセットは、DBG シリーズの WAN 側のネットワークケーブルを抜いた状態で行ってください。

DBG-2000 の Web GUI 設定

DBG-2000 Web GUI 設定画面へのログイン

1. 設定を行う PC と、DBG-2000 の「Ethernet 1/2/3/4」ポートのいずれかをネットワークケーブルで接続します。
   PC の IP アドレスは、DHCP クライアントまたは、192.168.10.0/24 サブネットのスタティック IP アドレスに設定します。
2. 設定を行う PC で Web ブラウザを開きます。
3. Web ブラウザのアドレス欄に Web GUI のアドレス「 http://192.168.10.1/」を入力し、「Enter」キーを押下します。
   「Ethernet 1/2/3/4」のうち、どのポートを使用しても Web GUI のアドレスは同じです。
4. 接続に成功すると、次のようなログイン画面が表示されます。

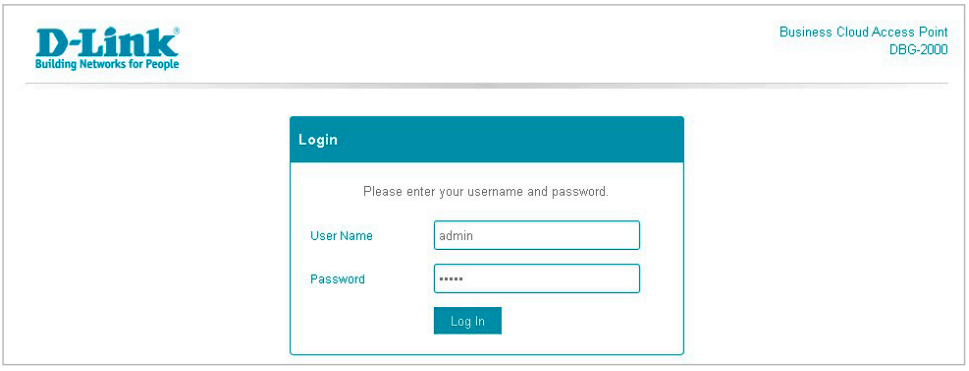


図 4-1　DBG-2000 ログイン

5. 「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。
   ユーザ名の初期値は「admin」、パスワードの初期値は「admin」です。

Nuclias に DBG シリーズを登録すると、Web GUI のログイン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 > ゲートウェイ > 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「デバイス情報」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 DBG-2000 についての様々な情報を参照できます。

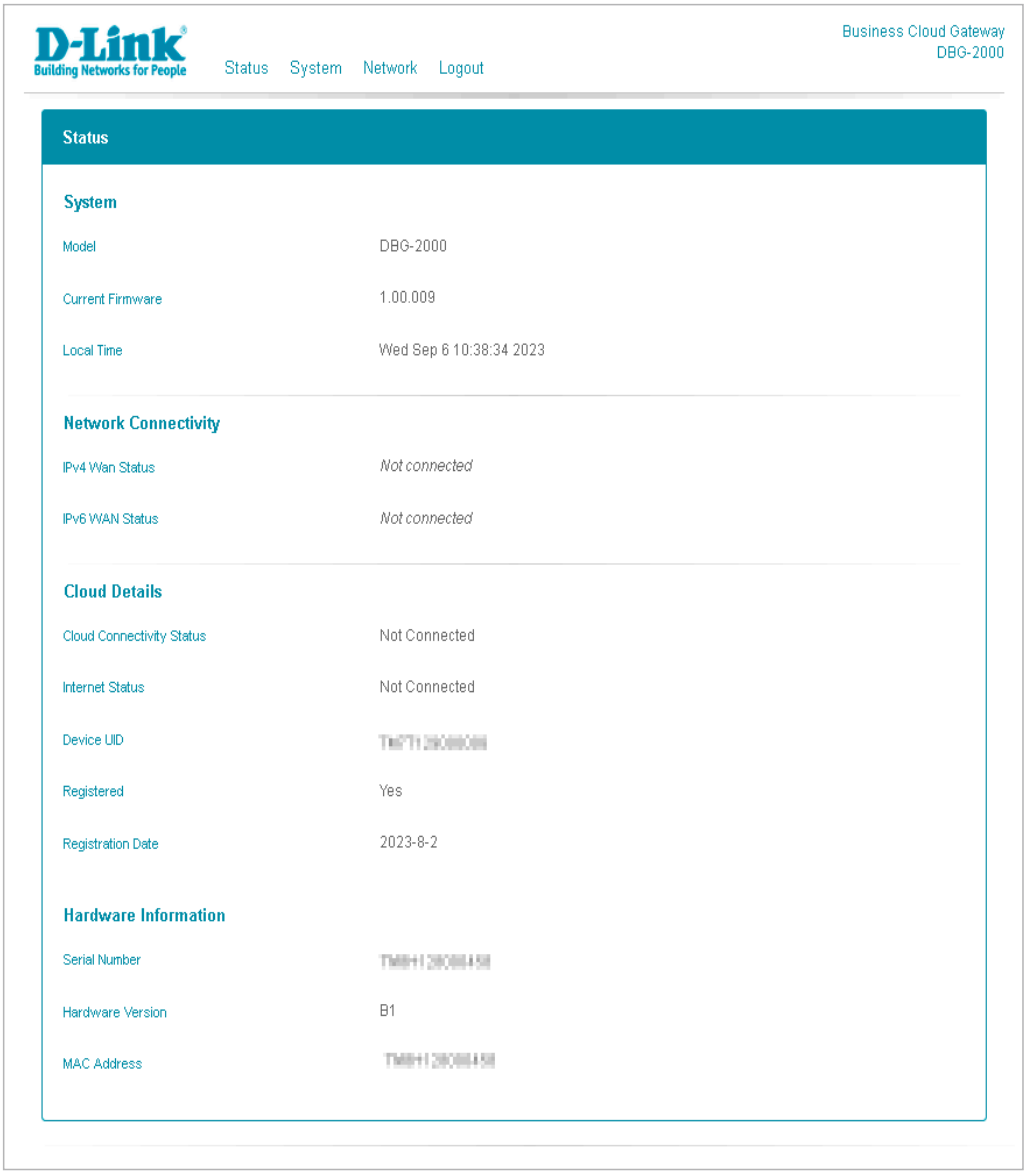


図 4-2　DBG-2000 ステータス

本画面には以下の項目があります。

項目	説明
System	
Model	デバイスのモデル名（型番）を表示します。
Current Firmware	現在のファームウェアバージョンを表示します。
Local Time	現地の時刻を表示します。
Network Connectivity	
IPv4 Wan Status	IPv4 による WAN ネットワークの接続状況を表示します。
IPv6 WAN Status	IPv6 による WAN ネットワーク接続状況を表示します。
Cloud Details	
Cloud Connectivity Status	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。
Internet Status	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。
Device UID	本体のデバイス UID を表示します。
Registered	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。
Registration Date	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。
Hardware Information	
Serial Number	製品のシリアル番号を表示します。
Hardware Version	製品のハードウェアバージョンを表示します。
MAC Address	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

システム画面では、ホスト名の確認と NTP サーバの設定を行う事ができます。

1. 「System」（システム）メニューで「System」（システム）を選択します。
2. 次の画面で設定を行います。

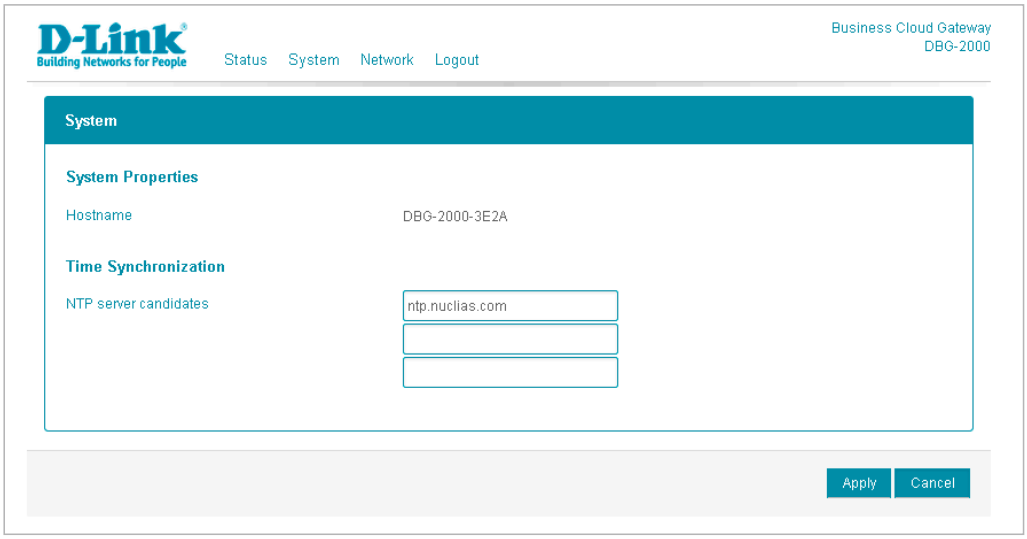


図 4-3　　DBG-2000 システム

本画面には以下の項目があります。

項目	説明
Hostname	本体のホスト名が記載されています。 命名規則は「DBG-2000-（MAC アドレス下 4 桁）」です。
NTP server candidates	NTP サーバの情報を入力します。 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。

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

システム > リセットとファームウェアアップグレード

Web GUI で設定のリセットとファームウェアアップグレード行う方法について説明します。

1. 「System」（システム）メニューで「Reset and Firmware Upgrade」（リセットとファームウェアアップグレード）を選択します。
2. 次の画面で設定のリセットとファームウェアアップグレードを行います。

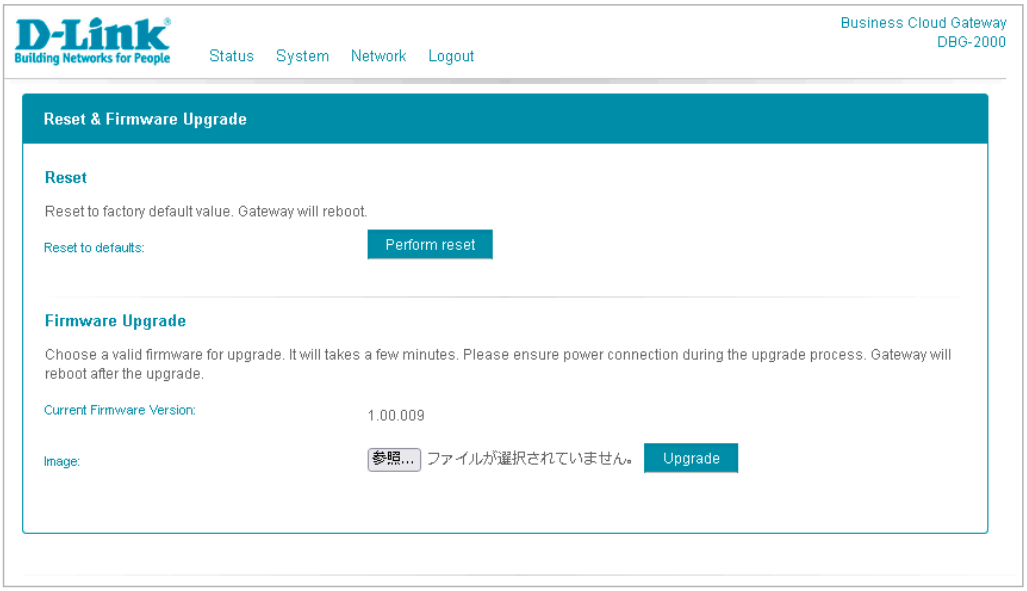


図 4-4　DBG-2000 リセットとファームウェアアップグレード

本画面には以下の項目があります。

項目	説明
Reset to defaults	「Perform reset」（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。 注意　リセットは、DBG シリーズの WAN 側のネットワークケーブルを抜いた状態で行ってください。
Current Firmware Version	現在のファームウェアバージョンを表示します。
Image	アップグレードするファームウェアを選択し、「Upgrade」（アップグレード）をクリックします。

ネットワーク > 基本設定

本製品の IP アドレス設定を行います。
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「Connection Type」（接続タイプ）を「Static IP」に変更します。

1. 「Network」（ネットワーク）メニューで「Common Configuration」（基本設定）を選択します。
2. 次の画面で IPv4 アドレスの「Connection Type」（接続タイプ）を「DHCP client」「Static IP」「PPPoE」「DS-Lite」「MAP-E」から選択します。
   設定項目は選択したタイプによって異なります。

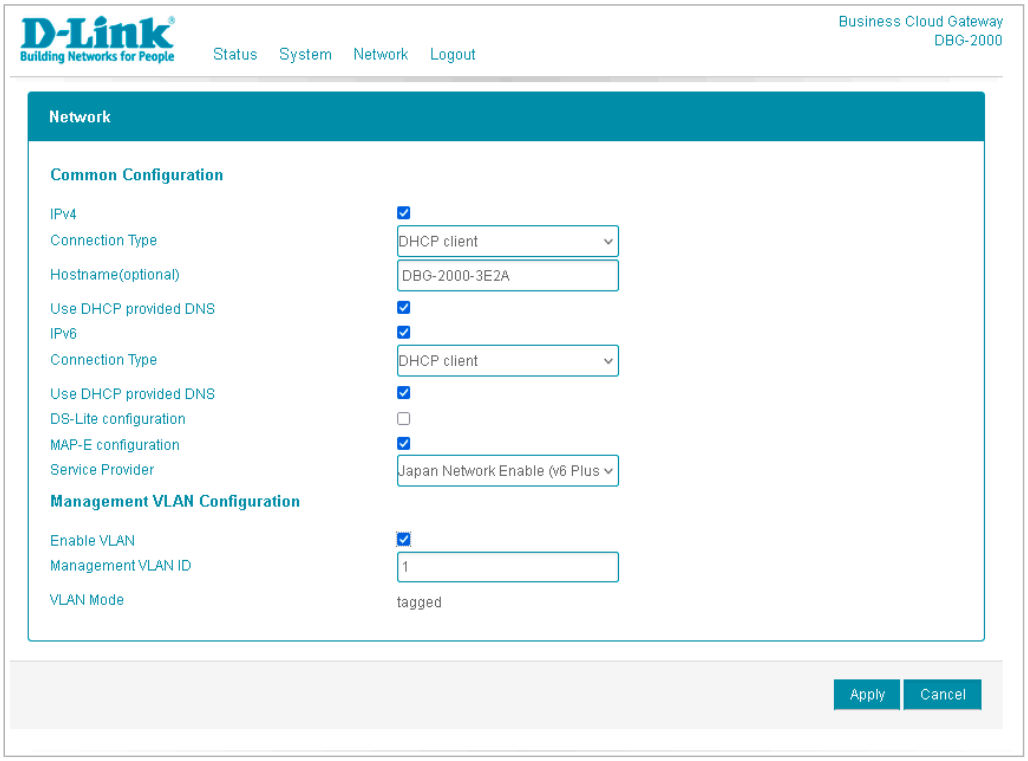


図 4-5　DBG-2000 ネットワーク - 基本設定（DHCP client 選択時）

設定項目の詳細は以下を参照してください。

- IPv4 アドレスの「Connection Type」で「DHCP client」を選択した場合 (DBG-2000)
- IPv4 アドレスの「Connection Type」で「Static IP」を選択した場合 (DBG-2000)
- IPv4 アドレスの「Connection Type」で「PPPoE」を選択した場合 (DBG-2000)
- IPv4 アドレスの「Connection Type」で「DS-Lite」を選択した場合 (DBG-2000)
- IPv4 アドレスの「Connection Type」で「MAP-E」を選択した場合 (DBG-2000)

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

■ IPv4 アドレスの「Connection Type」で「DHCP client」を選択した場合 (DBG-2000)

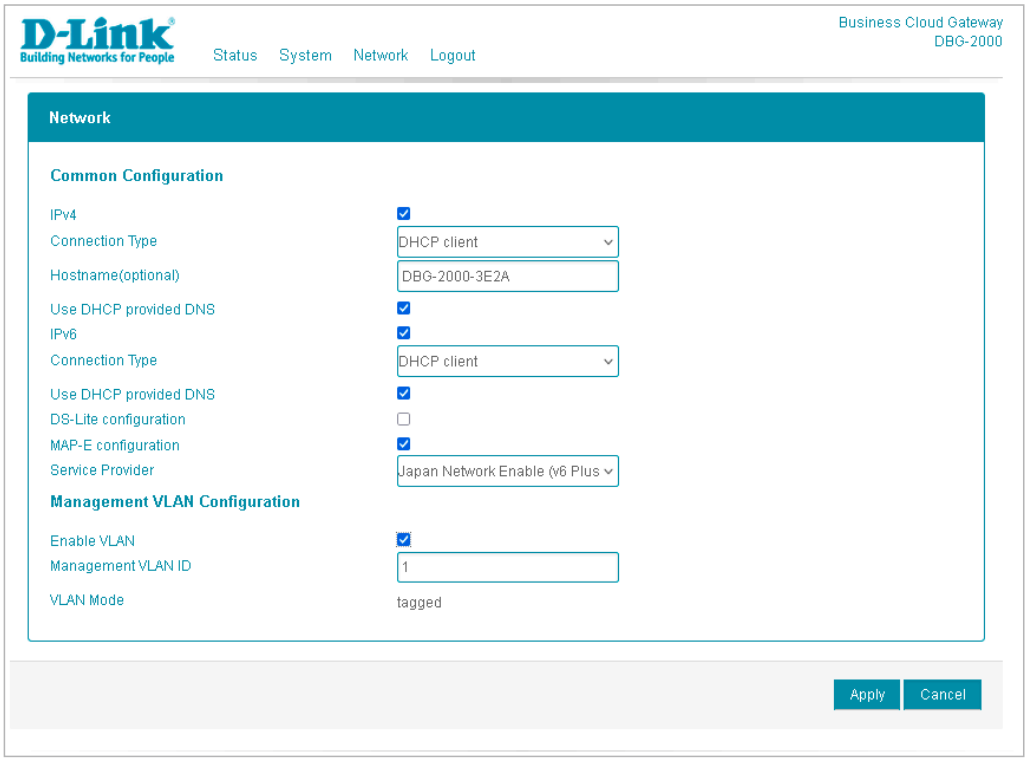


図 4-6　DBG-2000 ネットワーク - 基本設定（DHCP client 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「DHCP client」に設定します。
Hostname(optional)	ISP で必要な場合は、ホスト名を入力します。
Use DHCP provided DNS	DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
IPv6	
IPv6	IPv6 アドレスを有効 / 無効に設定します。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ IPv4 アドレスの「Connection Type」で「Static IP」を選択した場合 (DBG-2000)

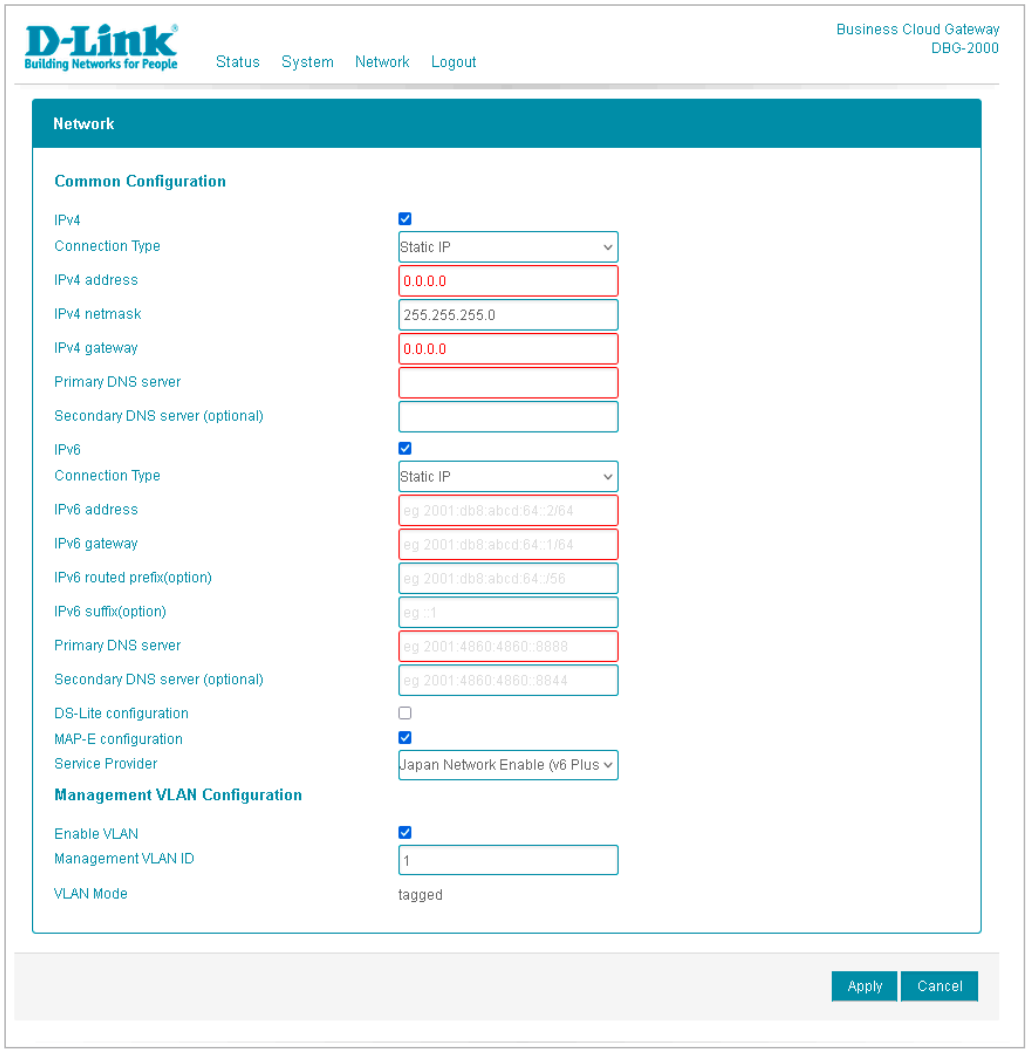


図 4-7　DBG-2000 ネットワーク - 基本設定（Static IP 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「Static IP」に設定します。 IPv4 アドレス、IPv4 ネットマスク、IPv4 ゲートウェイ、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
IPv6	
IPv6	IPv6 アドレスを有効 / 無効に設定します。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。

項目	説明
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ IPv4 アドレスの「Connection Type」で「PPPoE」を選択した場合 (DBG-2000)

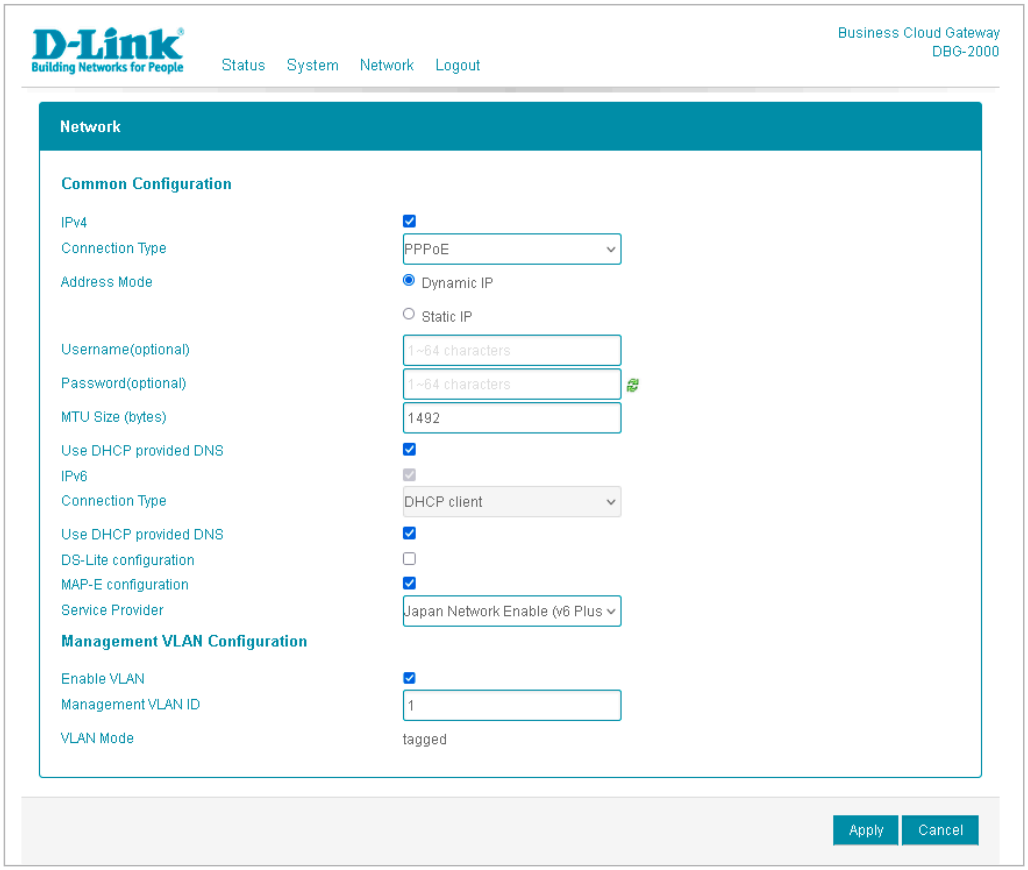


図 4-8　DBG-2000 ネットワーク - 基本設定（PPPoE 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「PPPoE」に設定します。
Address Mode	「Dynamic IP」または「Static IP」を選択します。 「Static IP」を選択した場合は、IPv4 アドレス、IPv4 ネットマスク、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）を指定します。
Username(optional)	PPPoE ユーザ名を入力します。本項目はオプションです。
Password(optional)	PPPoE パスワードを入力します。本項目はオプションです。
MTU Size (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。
Use DHCP provided DNS	アドレスモードで「Dynamic IP」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、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプには「DHCP client」が自動的に選択され変更できません。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。

項目	説明
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ **IPv4 アドレスの「Connection Type」で「DS-Lite」を選択した場合 (DBG-2000)**

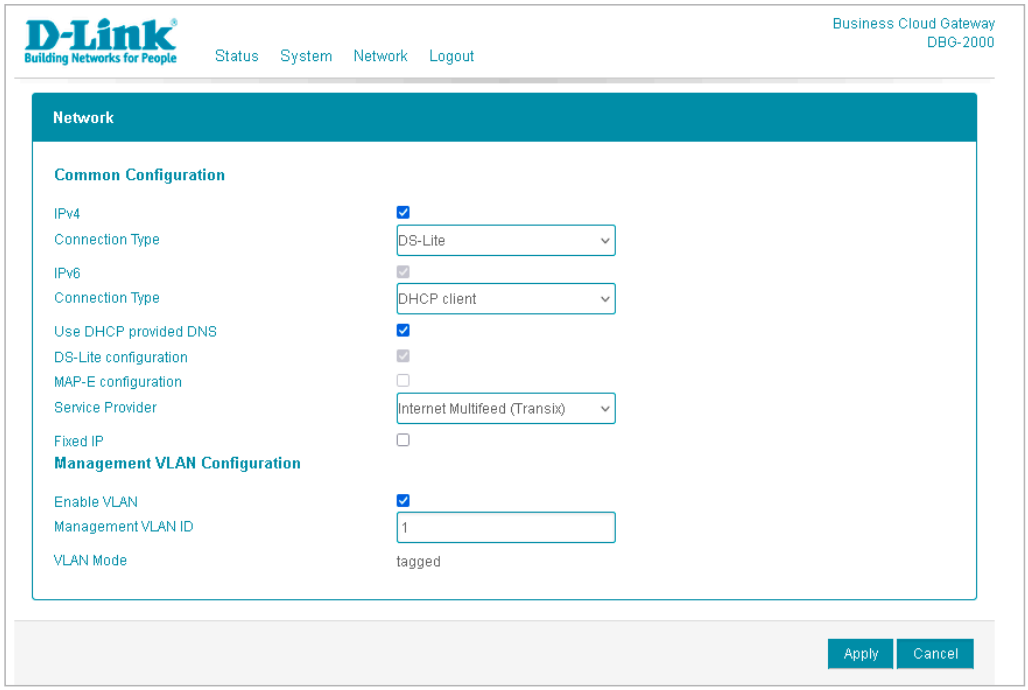


図 4-9　DBG-2000 ネットワーク - 基本設定（DS-Lite 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「DS-Lite」に設定します。
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定が有効になります。
MAP-E configuration	MAP-E 設定は無効になります。
Service Provider	プロバイダを選択します。

項目	説明
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ **IPv4 アドレスの「Connection Type」で「MAP-E」を選択した場合 (DBG-2000)**

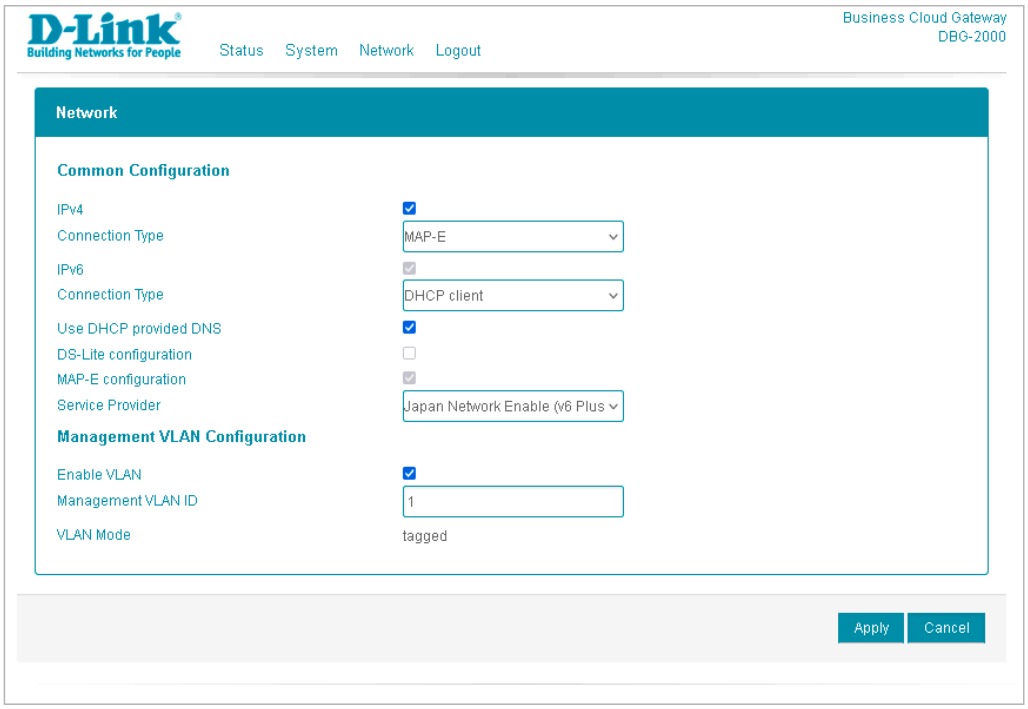


図 4-10　DBG-2000 ネットワーク - 基本設定（MAP-E 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「MAP-E」に設定します。
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定は無効になります。
MAP-E configuration	MAP-E 設定が有効になります。
Service Provider	プロバイダを選択します。
Fixed IP	「NTT Com(OCN)」を選択し、固定 IP アドレスを設定する場合はチェックをいれます。 有効にした場合はグローバル IPv4 アドレスを入力します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

ネットワーク > 詳細設定

プロキシの設定を行います。

1. 「Network」（ネットワーク）メニューで「Advanced Configuration」（詳細設定）を選択します。
2. 次の画面で設定を行います。

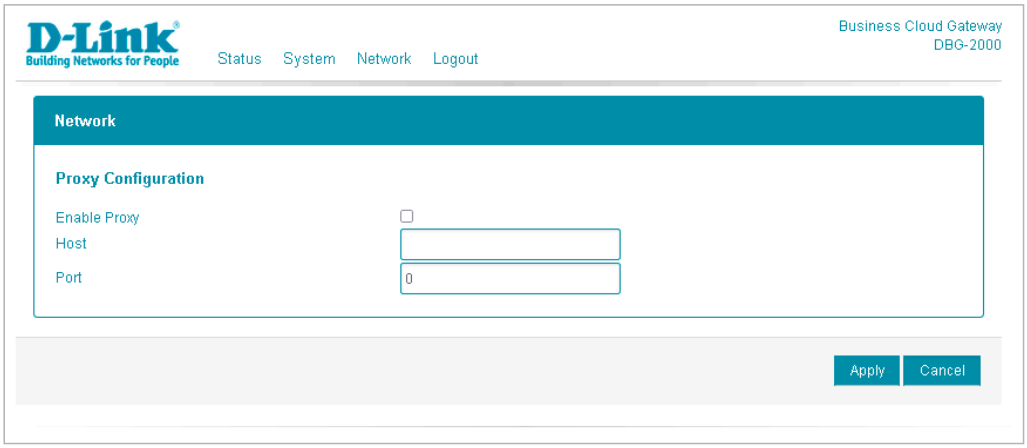


図 4-11　DBG-2000 ネットワーク - 詳細設定

本画面には以下の項目があります。

項目	説明
Proxy Configuration	
Enable Proxy	DBG-2000 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。
Host	プロキシサーバのホストを入力します。
Port	プロキシサーバのポート番号を入力します。

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

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。

DBG-X1000 の Web GUI 設定

Web GUI 設定画面へのログイン

1. 設定を行う PC と、DBG-X1000 の「Ethernet 1/2/3/4」ポートのいずれかをネットワークケーブルで接続します。
   PC の IP アドレスは、DHCP クライアントまたは、192.168.10.0/24 サブネットのスタティック IP アドレスに設定します。
2. 設定を行う PC で Web ブラウザを開きます。
3. Web ブラウザのアドレス欄に Web GUI のアドレス「 http://192.168.10.1/ 」を入力し、「Enter」キーを押下します。
   「Ethernet 1/2/3/4」のうち、どのポートを使用しても Web GUI のアドレスは同じです。
4. 接続に成功すると、次のようなログイン画面が表示されます。

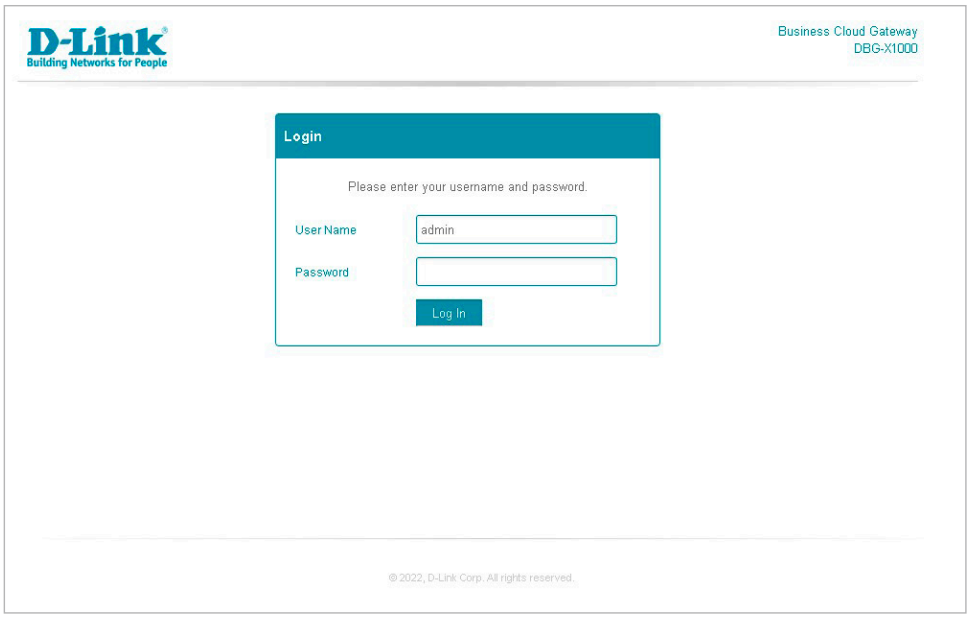


図 4-12　DBG-X1000 ログイン

5. 「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。
   ユーザ名の初期値は「admin」、パスワードの初期値は「admin」です。

Nuclias に DBG シリーズを登録すると、Web GUI のログイン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 > ゲートウェイ > 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「デバイス情報」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 DBG-X1000 についての様々な情報を参照できます。

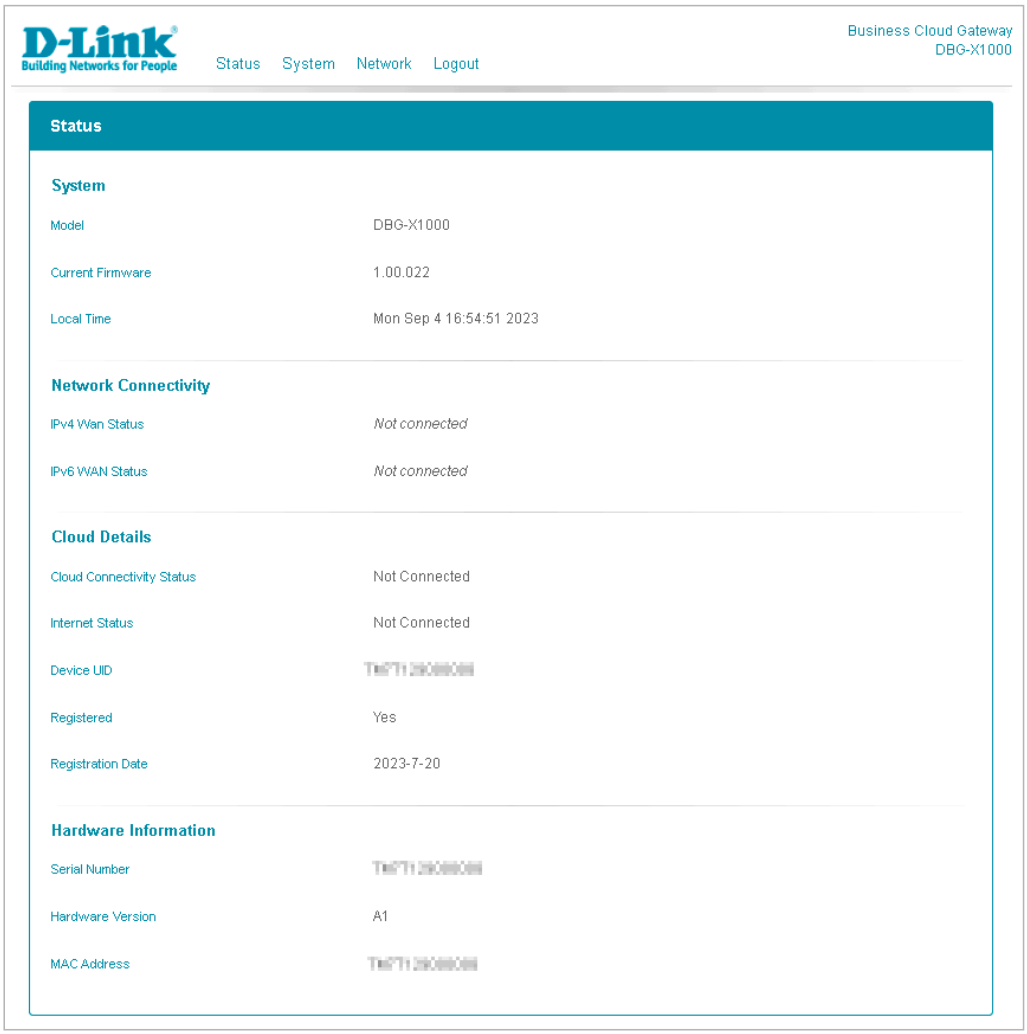


図 4-13　DBG-X1000 ステータス

本画面には以下の項目があります。

項目	説明
System	
Model	デバイスのモデル名（型番）を表示します。
Current Firmware	現在のファームウェアバージョンを表示します。
Local Time	現地の時刻を表示します。
Network Connectivity	
IPv4 Wan Status	IPv4 による WAN ネットワークの接続状況を表示します。
IPv6 WAN Status	IPv6 による WAN ネットワーク接続状況を表示します。
Cloud Details	
Cloud Connectivity Status	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。
Internet Status	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。
Device UID	本体のデバイス UID を表示します。
Registered	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。
Registration Date	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。
Hardware Information	
Serial Number	製品のシリアル番号を表示します。
Hardware Version	製品のハードウェアバージョンを表示します。
MAC Address	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

システム画面では、ホスト名の確認と NTP サーバの設定を行う事ができます。

1. 「System」（システム）メニューで「System」（システム）を選択します。
2. 次の画面で設定を行います。

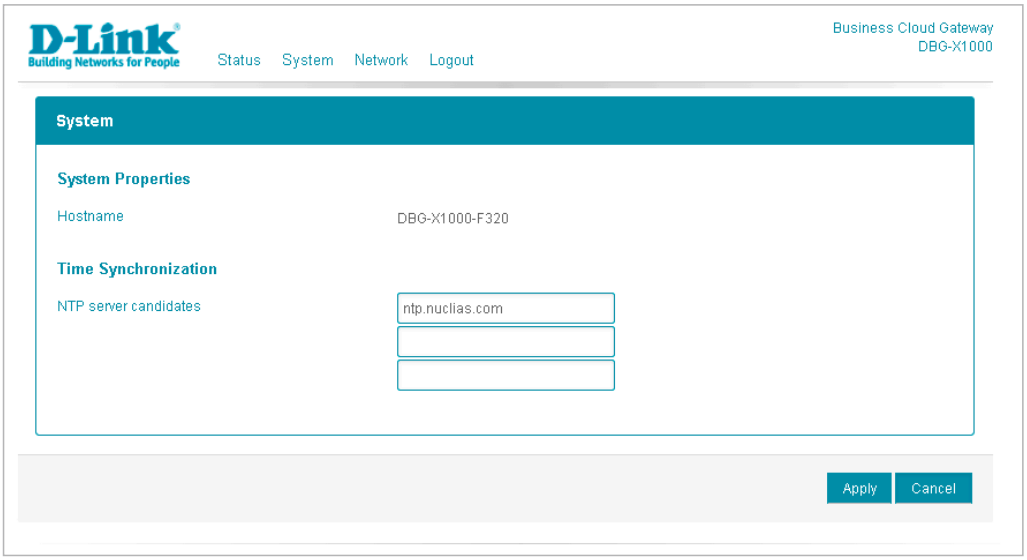


図 4-14　DBG-X1000 システム

本画面には以下の項目があります。

項目	説明
Hostname	本体のホスト名が記載されています。 命名規則は「DBG-X1000-（MAC アドレス下 4 桁）」です。
NTP server candidates	NTP サーバの情報を入力します。 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。

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

システム > リセットとファームウェアアップグレード

Web GUI で設定のリセットとファームウェアアップグレード行う方法について説明します。

1. 「System」（システム）メニューで「Reset and Firmware Upgrade」（リセットとファームウェアアップグレード）を選択します。
2. 次の画面で設定のリセットとファームウェアアップグレードを行います。

図 4-15　DBG-X1000 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
Reset to defaults	「Perform reset」（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。 注意　リセットは、DBG シリーズの WAN 側のネットワークケーブルを抜いた状態で行ってください。
Current Firmware Version	現在のファームウェアバージョンを表示します。
Image	アップグレードするファームウェアを選択し、「Upgrade」（アップグレード）をクリックします。

ネットワーク > 基本設定

本製品の IP アドレス設定を行います。
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「Connection Type」（接続タイプ）を「Static IP」に変更します。

1. 「Network」（ネットワーク）メニューで「Common Configuration」（基本設定）を選択します。
2. 次の画面で IPv4 アドレスの「Connection Type」（接続タイプ）を「DHCP client」「Static IP」「PPPoE」「DS-Lite」「MAP-E」から選択します。
   設定項目は選択したタイプによって異なります。

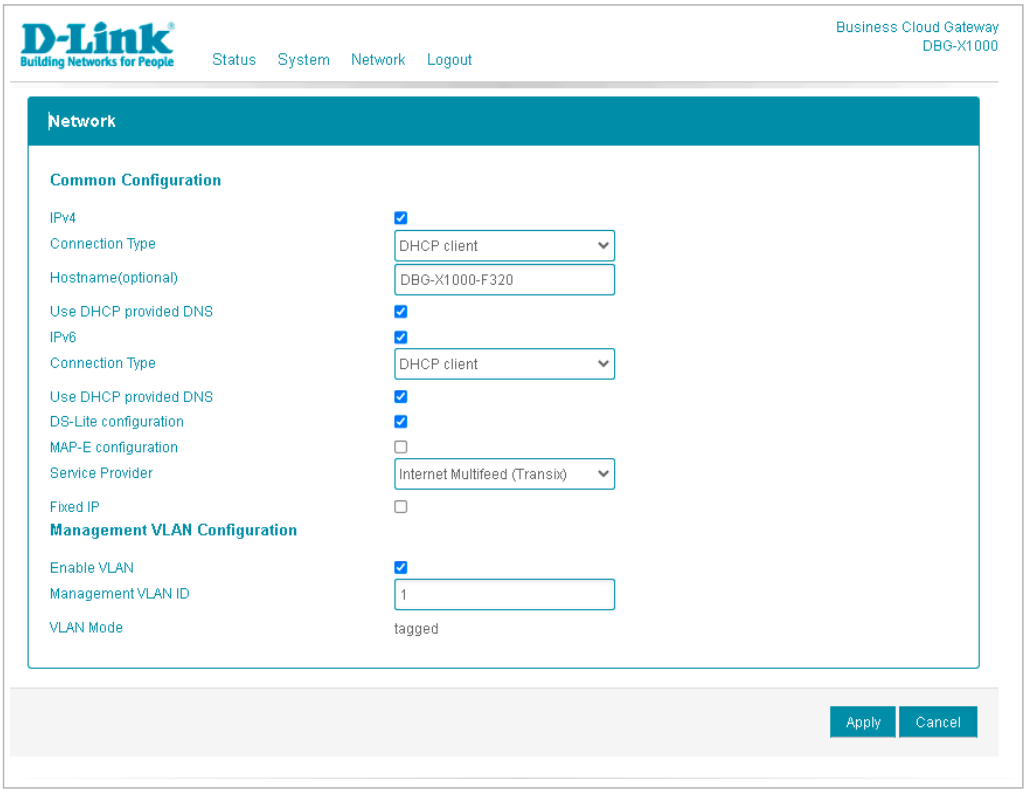


図 4-16　DBG-X1000 ネットワーク - 基本設定（DHCP client 選択時）

設定項目の詳細は以下を参照してください。

- IPv4 アドレスの「Connection Type」で「DHCP client」を選択した場合（DBG-X1000）
- IPv4 アドレスの「Connection Type」で「Static IP」を選択した場合（DBG-X1000）
- IPv4 アドレスの「Connection Type」で「PPPoE」を選択した場合（DBG-X1000）
- IPv4 アドレスの「Connection Type」で「DS-Lite」を選択した場合（DBG-X1000）
- IPv4 アドレスの「Connection Type」で「MAP-E」を選択した場合（DBG-X1000）

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

■ IPv4 アドレスの「Connection Type」で「DHCP client」を選択した場合（DBG-X1000）

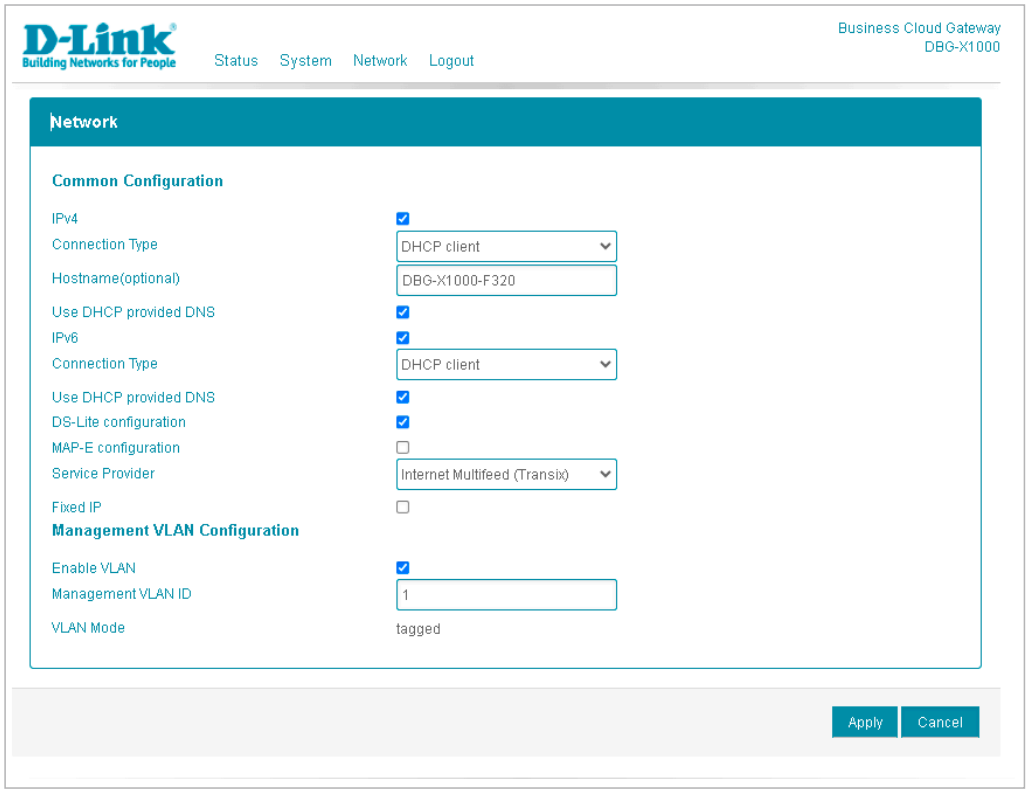


図 4-17　DBG-X1000 ネットワーク - 基本設定（DHCP client 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「DHCP client」に設定します。
Hostname(optional)	ISP で必要な場合は、ホスト名を入力します。
Use DHCP provided DNS	DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
IPv6	
IPv6	IPv6 アドレスを有効 / 無効に設定します。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ IPv4 アドレスの「Connection Type」で「Static IP」を選択した場合（DBG-X1000）

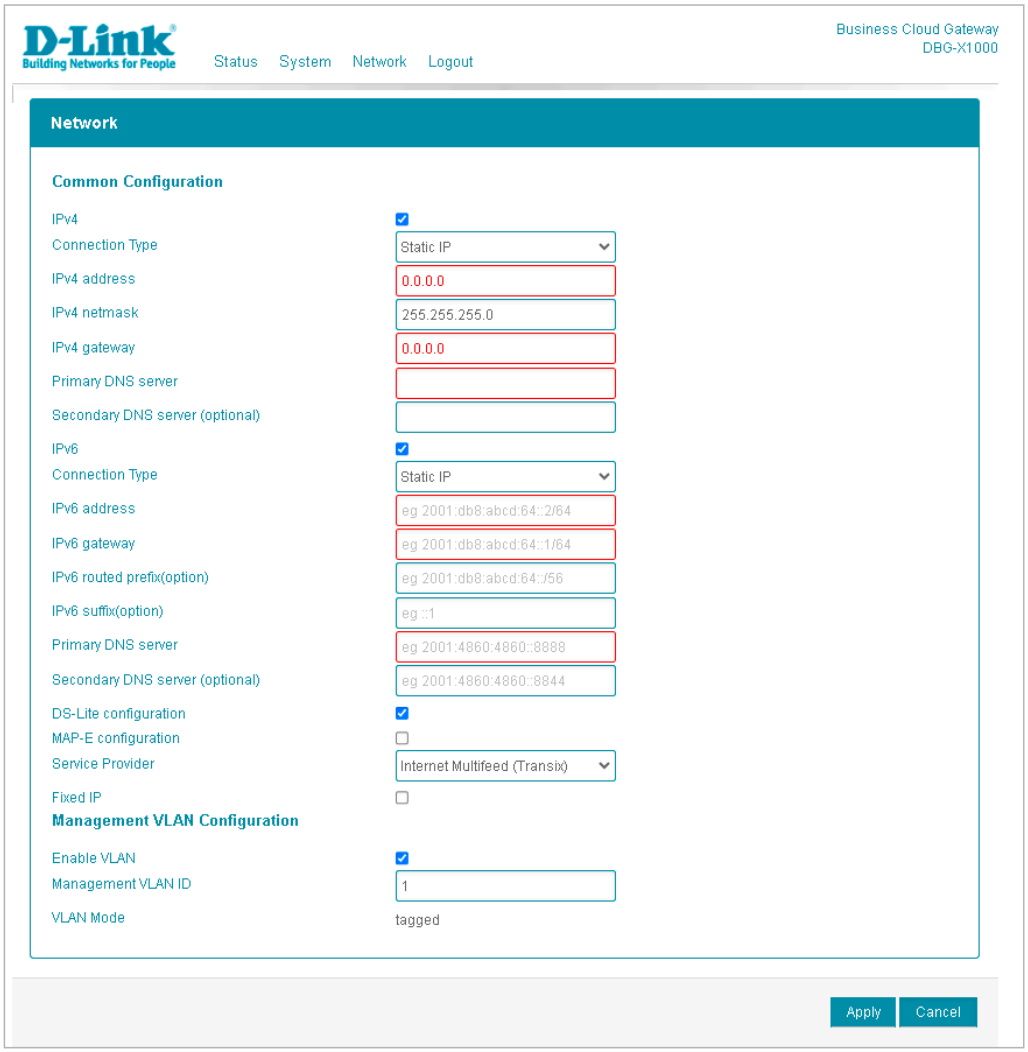


図 4-18　DBG-X1000 ネットワーク - 基本設定（Static IP 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「Static IP」に設定します。 IPv4 アドレス、IPv4 ネットマスク、IPv4 ゲートウェイ、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
IPv6	
IPv6	IPv6 アドレスを有効 / 無効に設定します。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。

項目	説明
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ IPv4 アドレスの「Connection Type」で「PPPoE」を選択した場合（DBG-X1000）

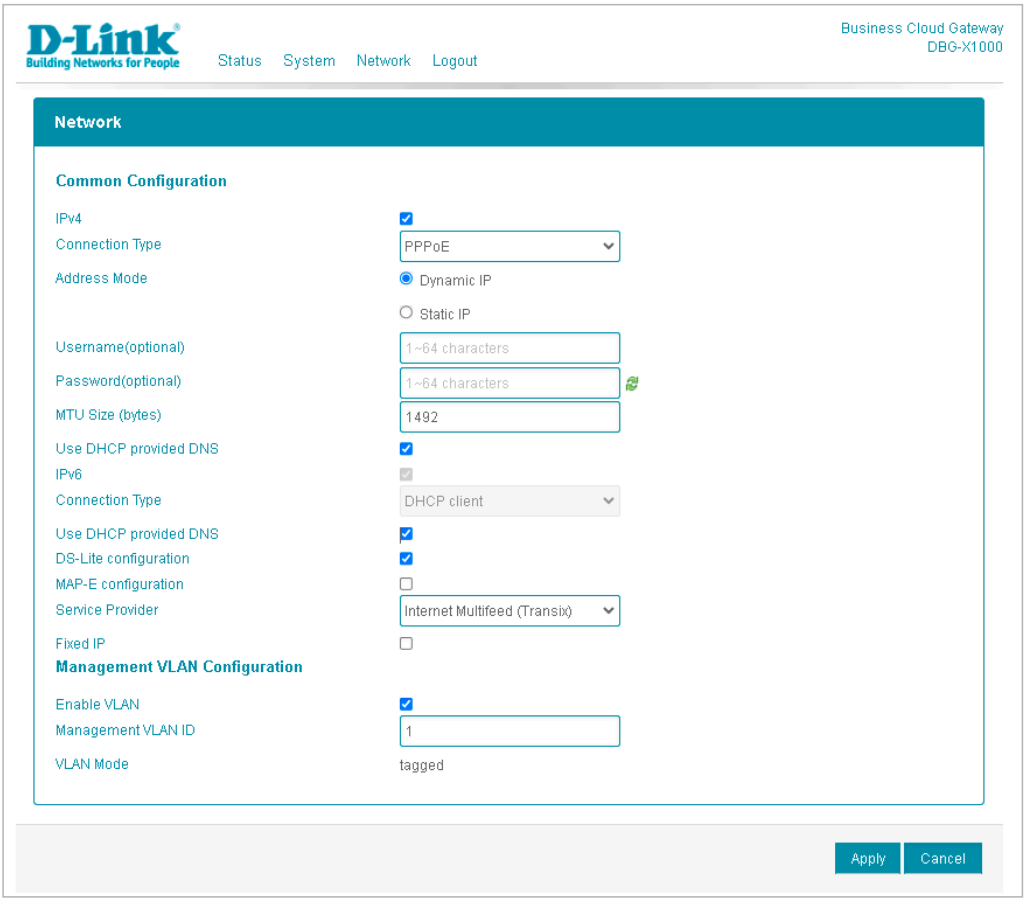


図 4-19　DBG-X1000 ネットワーク - 基本設定（PPPoE 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「PPPoE」に設定します。
Address Mode	「Dynamic IP」または「Static IP」を選択します。 「Static IP」を選択した場合は、IPv4 アドレス、IPv4 ネットマスク、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）を指定します。
Username(optional)	PPPoE ユーザ名を入力します。本項目はオプションです。
Password(optional)	PPPoE パスワードを入力します。本項目はオプションです。
MTU Size (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。
Use DHCP provided DNS	アドレスモードで「Dynamic IP」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、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。

項目	説明
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプには「DHCP client」が自動的に選択されます。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定を有効にする場合はチェックをいれます。
MAP-E configuration	MAP-E 設定を有効にする場合はチェックをいれます。
Service Provider	DS-Lite または MAP-E を有効にした場合は、プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Japan Network Enable(v6 Plus)」「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ **IPv4 アドレスの「Connection Type」で「DS-Lite」を選択した場合（DBG-X1000）**

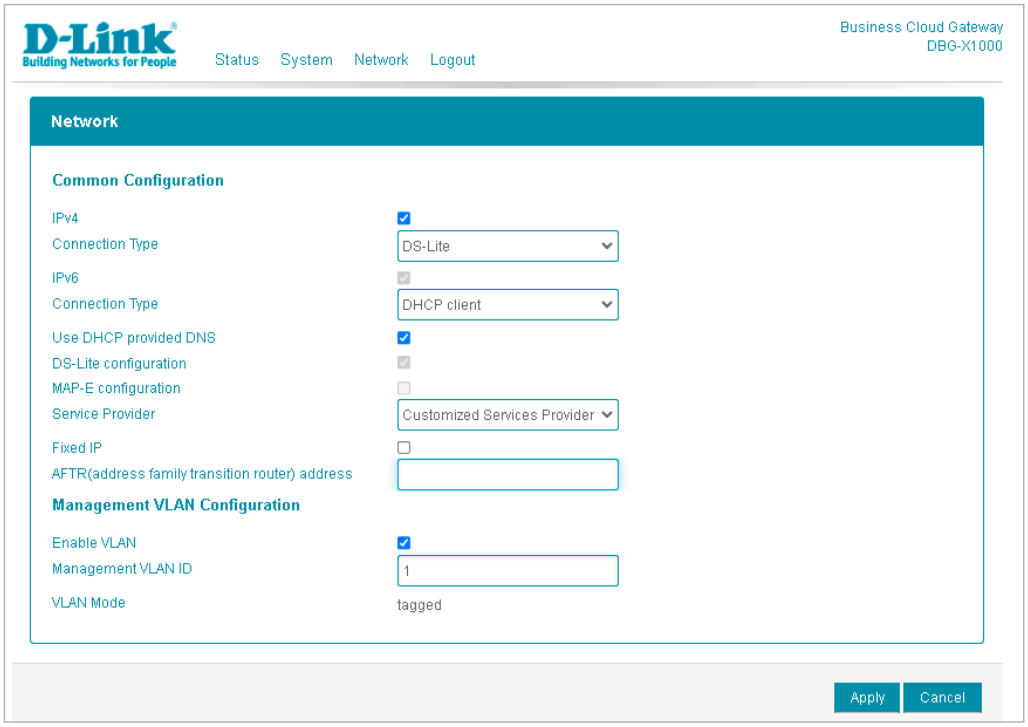


図 4-20　DBG-X1000 ネットワーク - 基本設定（DS-Lite 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「DS-Lite」に設定します。

項目	説明
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定が有効になります。
MAP-E configuration	MAP-E 設定は無効になります。
Service Provider	プロバイダを選択します。
Fixed IP	固定 IP アドレスを設定する場合はチェックをいれます。「Service Provider」で「Customized Service Provider」を選択した場合、本項目は表示されません。 本項目を有効にした場合はピアトンネル IPv6 アドレス、BR アドレス、インターフェイス ID、アップデート URL、ユーザ名、パスワード、グローバル IPv4 アドレスなどを入力します。設定項目は「Service Provider」での選択内容により異なります。
AFTR(address family transition router) address	「Service Provider」で「Customized Service Provider」を選択した場合に、AFTR アドレスを指定します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

■ **IPv4 アドレスの「Connection Type」で「MAP-E」を選択した場合（DBG-X1000）**

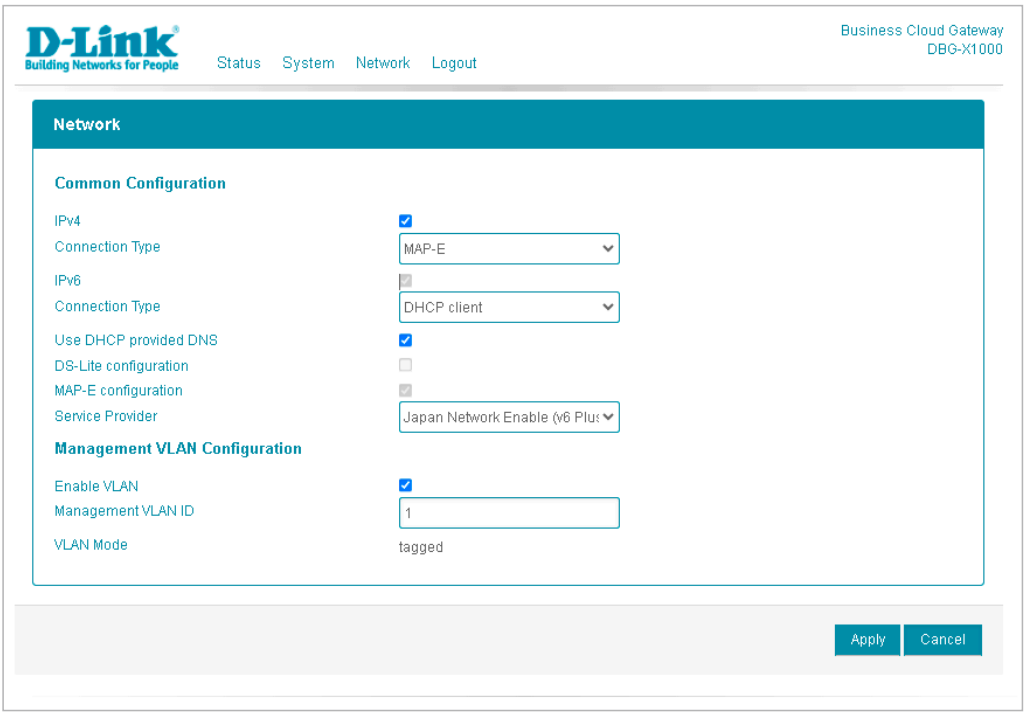


図 4-21　DBG-X1000 ネットワーク - 基本設定（MAP-E 選択時）

本画面には以下の項目があります。

項目	説明
IPv4	
IPv4	IPv4 アドレスを有効 / 無効に設定します。
Connection Type	IPv4 アドレスの接続タイプを「MAP-E」に設定します。

項目	説明
IPv6	
IPv6	IPv6 アドレスは有効になります。
Connection Type	IPv6 アドレスの接続タイプを「DHCP client」「Static IP」から設定します。 「Static IP」を選択した場合は、IPv6 アドレス、IPv6 ゲートウェイ、IPv6 ルートプレフィックス（オプション）、IPv6 サフィックス（オプション）、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の項目を入力します。
Use DHCP provided DNS	IPv6 アドレスの接続タイプを「DHCP client」に設定した場合に表示されます。 DHCP サーバが提供する DNS を使用する場合は、本項目に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本項目のチェックを外し、プライマリ DNS サーバ、セカンダリ DNS サーバ（オプション）の情報を入力します。
DS-Lite configuration	DS-Lite 設定は無効になります。
MAP-E configuration	MAP-E 設定が有効になります。
Service Provider	プロバイダを選択します。
Fixed IP	「NTT Com(OCN)」を選択し、固定 IP アドレスを設定する場合はチェックをいれます。 有効にした場合はグローバル IPv4 アドレスを入力します。
Management VLAN Configuration	
Enable VLAN	VLAN を有効にする場合はチェックを入れます。
Management VLAN ID	VLAN を有効にした場合は、管理 VLAN ID を設定します。
VLAN Mode	VLAN モードを表示します。

ネットワーク > 詳細設定

プロキシの設定を行います。

1. 「Network」（ネットワーク）メニューで「Advanced Configuration」（詳細設定）を選択します。
2. 次の画面で設定を行います。

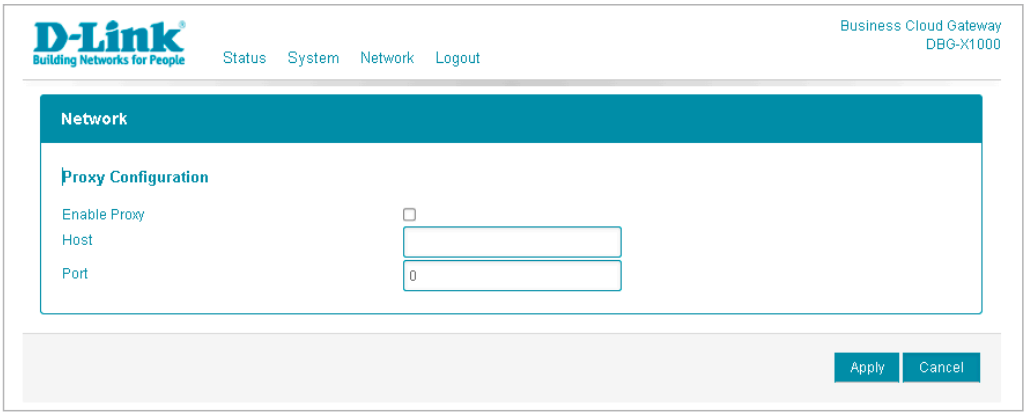


図 4-22　DBG-X1000 ネットワーク - 詳細設定

本画面には以下の項目があります。

項目	説明
Proxy Configuration	
Enable Proxy	DBG-X1000 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。
Host	プロキシサーバのホストを入力します。
Port	プロキシサーバのポート番号を入力します。

3. 設定後、「Apply」（適用）をクリックし設定を保存します。

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。

第 5 章　Nuclias の基本設定

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 でサイトの設定などを行い、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。

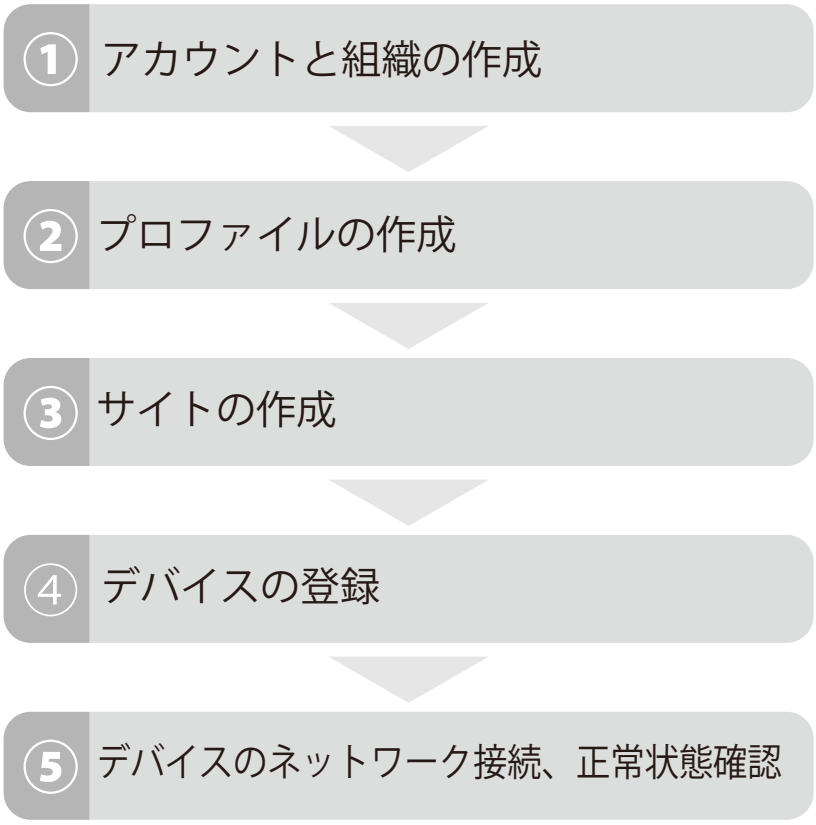


図 5-1　初期設定手順

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 5-2　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 5-3　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 5-4　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。

設定後、「次」をクリックします。

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。

図 5-5　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 5-6　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 ユーザインターフェイスについて

Nuclias 管理画面上部のユーザインターフェイスは下記の通りです。

図 5-7　ユーザインターフェイス

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。 ユーザプロファイルの閲覧や変更、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 7 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、本製品へ配信する設定をまとめたものです。プロファイルの設定項目については「第 9 章　設定」を参照してください。

1. **設定** > **ゲートウェイ** > **プロファイル**の順にクリックします。

図 5-8　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 5-9　プロファイルの作成

3. プロファイル作成画面の項目を入力し、「プロファイルの作成」をクリックします。

図 5-10　プロファイル作成画面

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	モデル名は、「DBG-X1000/DBG-2000(B1)」を選択する必要があります。
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」: 既に存在するプロファイルをコピーして使用します。

4. **設定 > ゲートウェイ > プロファイル**画面に作成したプロファイルが表示されます。
5. 「アクション」欄の「ネットワーク」「セキュリティ」をクリックし、プロファイルの設定を行います。
   以下は「ネットワーク」設定画面の例です。

図 5-11　プロファイル設定画面（ネットワーク）

参照　プロファイルの設定項目の詳細については「第 9 章　設定」を参照してください。

■ プロファイルリストの表示

作成したプロファイルは、**設定 > ゲートウェイ > プロファイル**画面に表示されます。

図 5-12　プロファイルリスト

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プロファイル	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	「ネットワーク」「セキュリティ」設定のページに移行します。

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 5-13　組織管理メニュー

2. 「サイトの作成」をクリックします。

図 5-14　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、入力は不要です。

図 5-15　サイトの作成

4. 「適用」をクリックします。

Nuclias 対応機器の登録

1. **管理 > デバイスの追加**の順にクリックします。

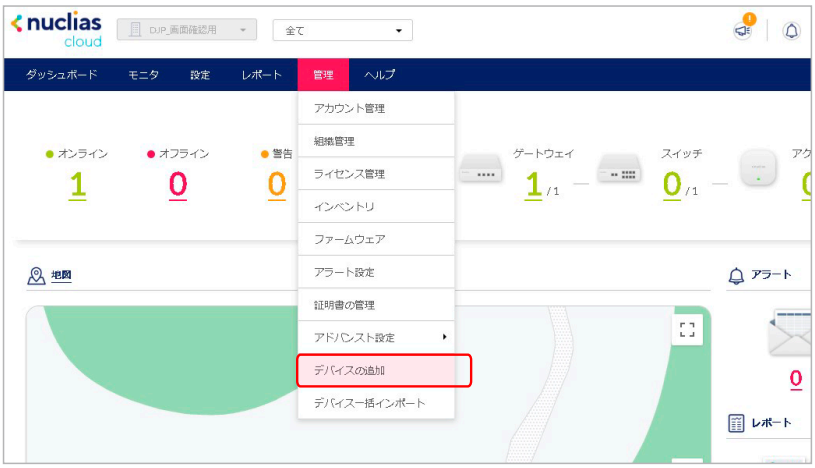


図 5-16　デバイスの追加メニュー

2. 「デバイスの追加」画面が表示されます。

図 5-17　デバイスの追加

3. 下記の項目を入力します。

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。

4. 入力後、「保存」をクリックします。

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。

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。

DBG-X1000 の Internet ポートや DBG-2000 の WAN1 ポートに LAN ケーブルが接続されていない状態で、既に本体が起動しているときは、そのまま LAN ケーブルを接続してオンラインになるのを待つよりも、一旦本体を電源 OFF し、LAN ケーブルを接続したあと再度電源 ON にしたほうが、早くオンライン状態にできる場合がございます。

2. 機器が正常にオンライン状態になり、Nuclias 上でオンライン表示になると設定完了です。

図 5-18　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。

第 6 章　ユーザプロファイル

ユーザプロファイル

マイプロフィール

Nuclias 管理画面の右上部のユーザ名から「ユーザプロファイル」をクリックし、「マイプロフィール」タブで現在ログインしているユーザの情報を確認します。

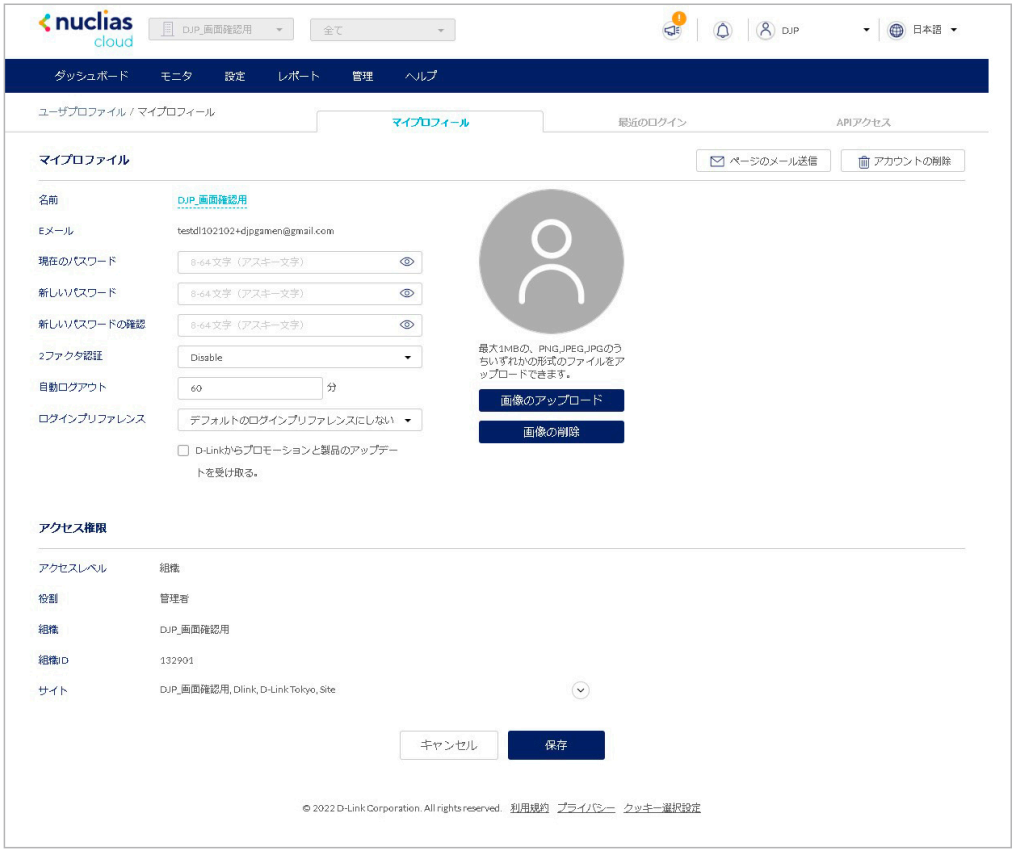


図 6-1　　ユーザプロファイル

ログイン中ユーザのユーザ名、ログインパスワードの変更、イメージ画像の変更を行うことができます。
また、E メールアドレスや、権限、アクセス可能なサイトの確認が可能です。

本画面には以下の項目があります。

項目	説明
名前	ログイン時に表示されるユーザ名です。自身で編集できます。
E メール	ユーザに紐づいている E メールアドレスです。変更できません。
現在のパスワード 新しいパスワード	ログイン時に利用するパスワードを変更します。 「現在のパスワード」に現在のパスワード、「新しいパスワード」と「新しいパスワードの確認」に新しいパスワードを入力し、「保存」をクリックします。
2 ファクタ認証	Nuclias にログインする際に、本画面で設定したパスワードのほかに E-mail または Google Authenticator による認証を行う機能です。 • 「Disable」：2 ファクタ認証を無効にします。 • 「Email authentication」：パスワードによる認証のほかに、E-mail による認証を行います。登録した E-mail アドレスに送付されるパスコードを使用してください。 • 「Google authenticator」：パスワードによる認証のほかに、Google 認証システム（Google Authenticator）による認証を行います。Nuclias アカウントを Google 認証システムに追加し、「2 ファクタ認証コードのテスト」で認証を確認してください。
自動ログアウト	自動ログアウト時間（単位：分）を設定します。 Nuclias にログイン後、本項目で設定した時間内に操作を行わなかった場合、Nuclias から自動的にログアウトします。
ログインプリファレンス	Nuclias Cloud と Nuclias Connect のどちらかをログイン後に表示する画面として指定できます。 • 「デフォルトのログインプリファレンスにしない」：ログイン後に表示する画面を指定しません。 • 「Nuclias クラウドポータルをデフォルトに設定する」：ログイン後に Nuclias Cloud の画面を表示します。 • 「Nuclias クラウドコネクトをデフォルトに設定する」：ログイン後に Nuclias Connect の画面を表示します。

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「ユーザプロファイル」をクリックし、「最近のログイン」タブをクリックします。

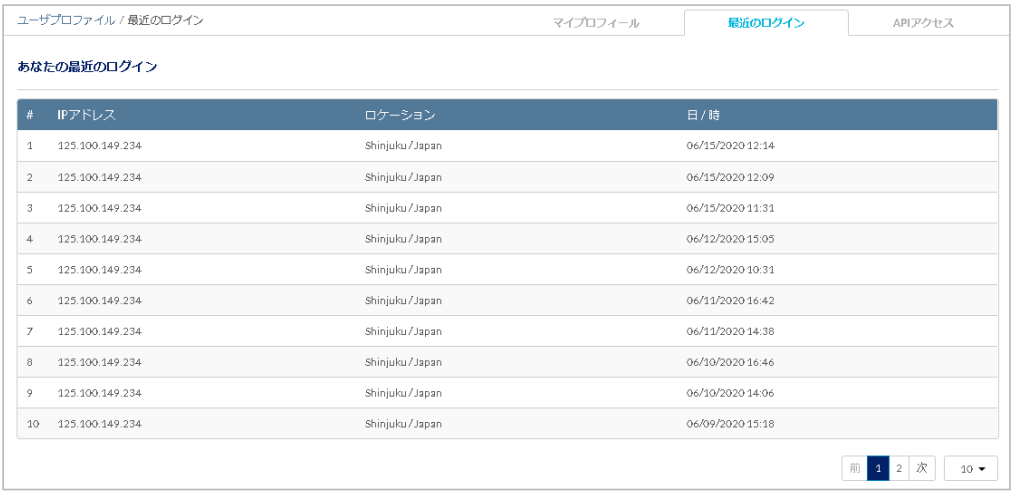


図 6-2　　ログイン履歴

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イスです。
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「ユーザプロファイル」をクリックし、「API アクセス」タブをクリックします。

図 6-3　　API アクセス

■ API キーの生成

1. 「API key の生成」をクリックし、次の画面を表示します。

図 6-4　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. 次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 6-5　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 6-6　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 7 章　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 7-1　　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 7-2　　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 7-3　　ダッシュボード（概要）

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。

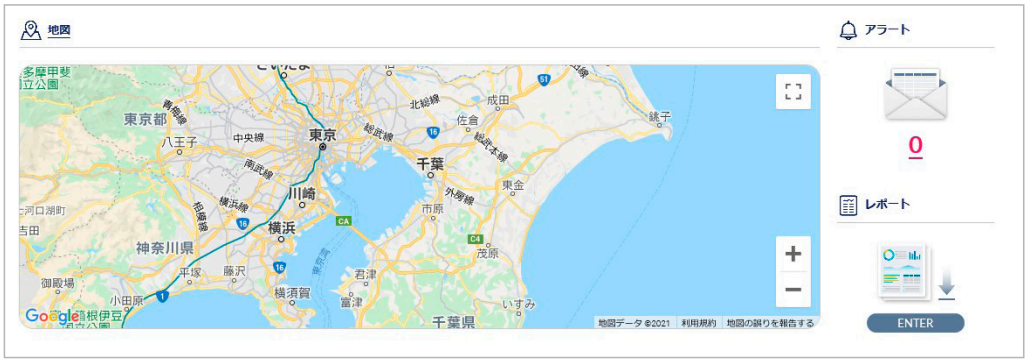


図 7-4　　ダッシュボード（マップ + アラート + レポート）

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 7-5　　ダッシュボード（最近 24 時間サマリ）

第 8 章　モニタ

ゲートウェイ - デバイス

モニタ > ゲートウェイ > 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 8-1　　デバイス一覧

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。
マネジメント IP	デバイスのマネジメント IP アドレスを表示します。
デフォルト WAN IPv4	デバイスのデフォルト WAN IPv4 アドレスを表示します。
デフォルト WAN IPv6	デバイスのデフォルト WAN IPv6 アドレスを表示します。
ローカル IP	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。
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。
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。
デバイス UID	デバイスの UID 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	現在接続しているクライアントの数を表示します。
使用量	使用量を表示します。
チャネル	無線対応機器の場合、現在使用しているチャネルを表示します。「(2.4G 帯のチャネル)/(5G 帯のチャネル)」表示です。 無線非対応機器の場合は - が表示されます。
送信電波出力	デバイスにて設定されている送信電波出力の値を表示します。無線非対応機器の場合は - が表示されます。
チャネル帯域	現在選択しているチャネル帯域を表示します。

■ 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。

ゲートウェイ - クライアント

モニタ > ゲートウェイ > クライアントの順にクリックし、本製品に接続されている、または接続されていたクライアント状態を確認できます。

注意 VPN 接続されているクライアントは、クライアントリストには表示されません。

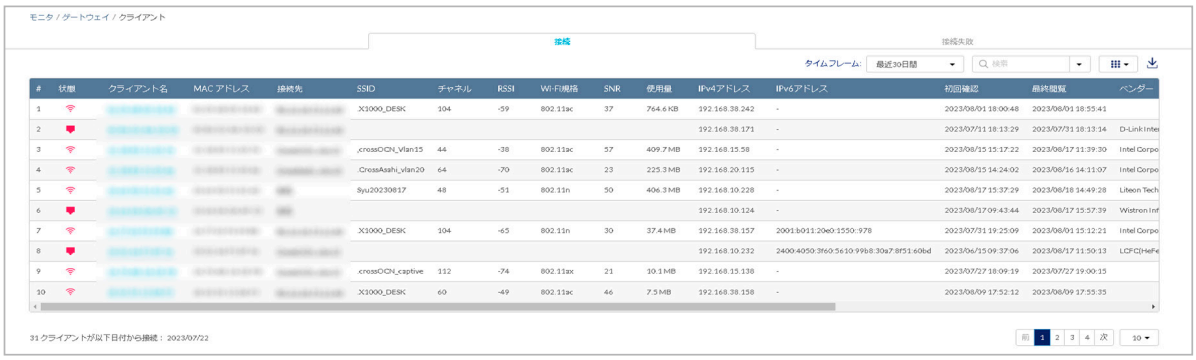


図 8-2　クライアント一覧

表の各項目の説明は下記の通りです。

項目	説明
状態	クライアントの接続状態をアイコンで表示します。 有線接続のクライアントの場合は LAN ポートのアイコン、無線接続のクライアントの場合は Wi-Fi のアイコンが表示されます。 • 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。
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	無線接続の場合は、接続している SSID の名前を表示します。
チャネル	無線接続の場合は、クライアントが接続しているチャネルを表示します。
RSSI	無線接続の場合は、RSSI（Received Signal Strength Indicator）の値を表示します。 RSSI は、クライアントのデバイスが本製品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	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。
使用量	無線接続の場合は、クライアントの通信容量を表示します。
IPv4 アドレス	クライアントの IPv4 アドレスを表示します。
IPv6 アドレス	クライアントの IPv6 アドレスを表示します。
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を表示します。
キャプティブポータル	無線接続の場合は、クライアントのキャプティブポータルを表示します。
ユーザ ID	クライアントのユーザ ID を表示します。
E メール	キャプティブポータルで使用される E メールアドレスが表示されます。
ダイナミック VLAN	ダイナミック VLAN の情報を表示します。（ダイナミック VLAN は未サポートです。）

■ 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。

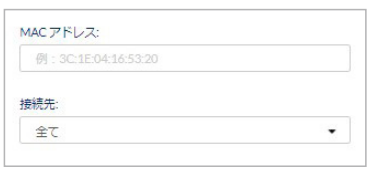


図 8-3　クライアントの検索

■ 表示する項目の変更

をクリックし、表示する項目を選択します。

■ 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。

なお、「接続失敗」タブを選択すると、接続に失敗したクライアントが表示されます。

ゲートウェイ - イベントログ

モニタ > ゲートウェイ > イベントログ の順にクリックし、サイト内で発生したイベントについて表示します。

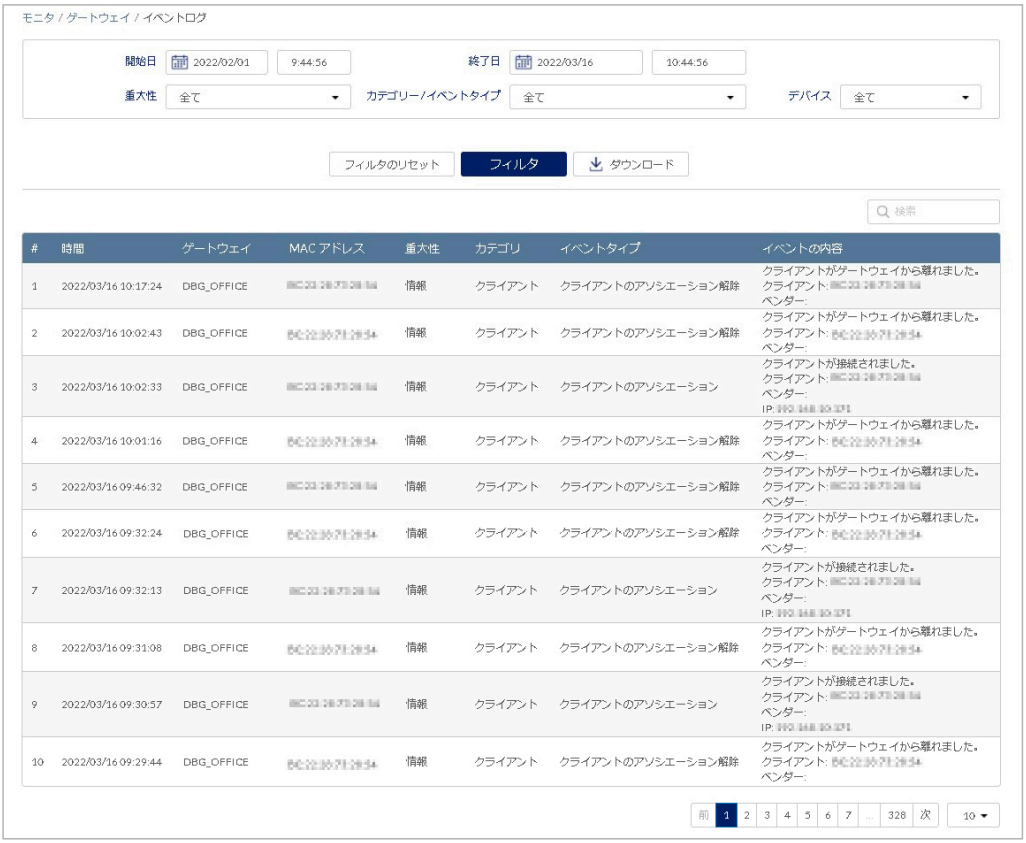


図 8-4　　イベントログ

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。
ゲートウェイ	イベントの発生したゲートウェイを表示します。
MAC アドレス	イベントが発生したゲートウェイの 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。
カテゴリ	イベントのカテゴリを表示します。
イベントタイプ	イベントの種類を表示します。
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、デバイスから 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、表示されるイベントのリストを絞り込むことができます。

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。
カテゴリー / 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、設定したフィルタを基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：デバイスが登録されていないか、デバイス登録済であるが Nuclias に未接続である状態を示しています。

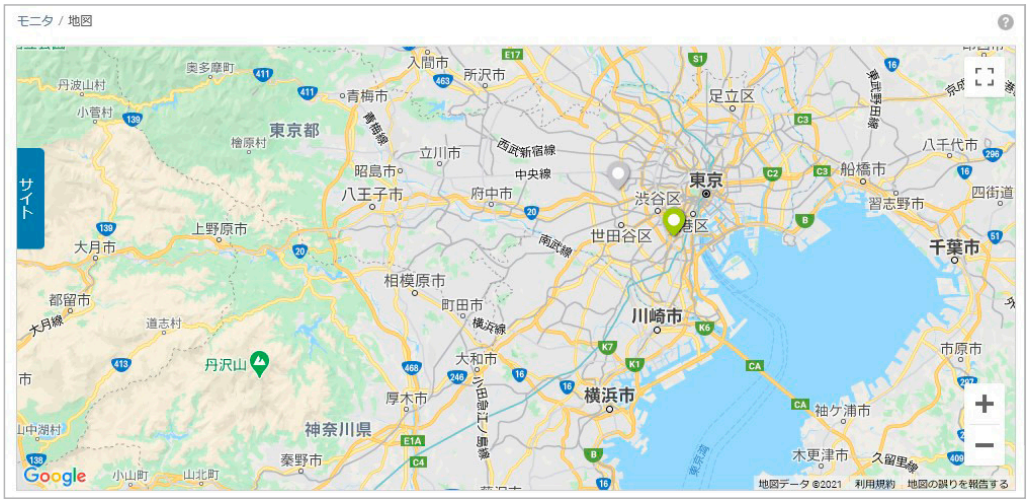


図 8-5　地図

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。
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。

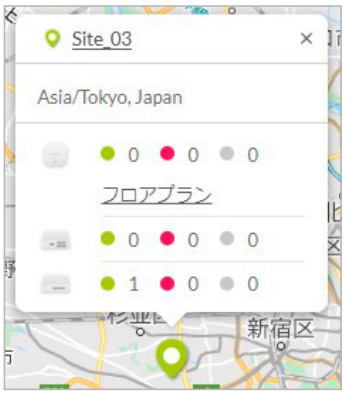


図 8-6　地図 - サイト情報

地図左端の「サイト」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。

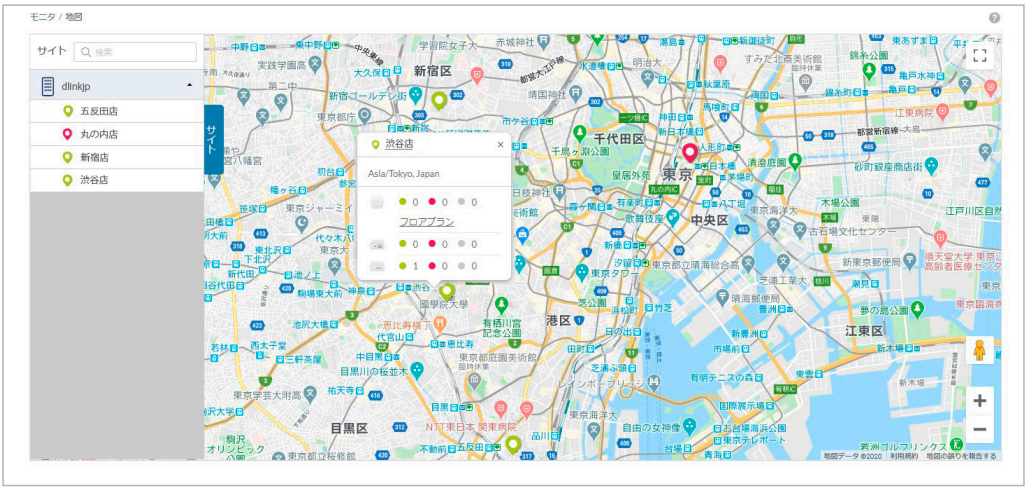


図 8-7　　地図 - サイトのリスト

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。

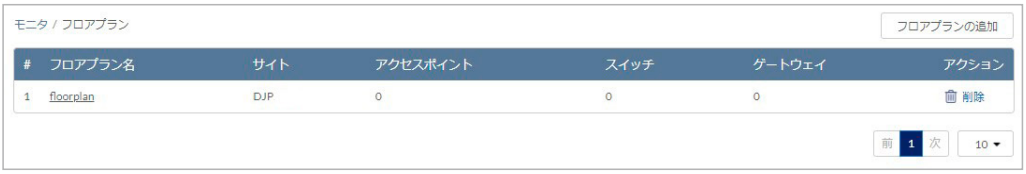


図 8-8　　フロアプラン

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 8-9　　フロアプランの追加

3. 「保存」をクリックすると、次の画面が表示されます。

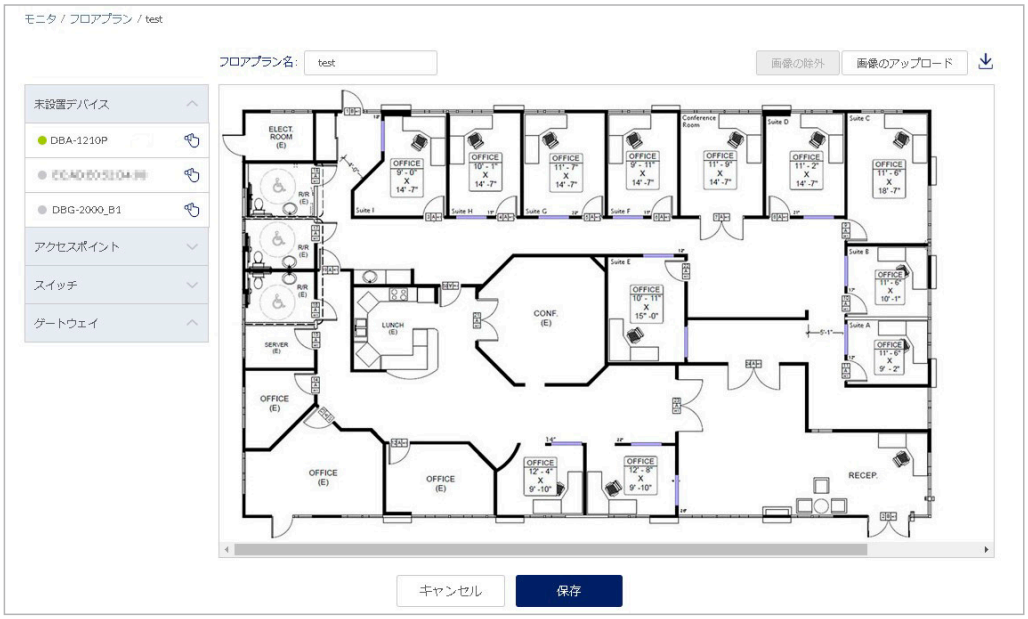


図 8-10　フロアプランの編集

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」にはフロアマップ上にまだ配置されていないデバイスが表示されます。
     ドラッグしてフロアマップ上の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。
   - フロアマップ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。
アクセスポイントの検知を行うのは無線対応機器のみです。

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ネルの± 1 の範囲のチャネルにおいて、SSID を検知します。5GHz 帯では、現在使用しているチャネルの± 4 の範囲のチャネルにおいて、SSID を検知します。

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。

図 8-11　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 ～ー 55 の範囲内にある場合に表示します。 • 「UNKNOWN」：RSSI 値がー 55 より低い場合に表示します。
検知元	情報を検知したデバイスを表示します。
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。
チャネル	検知したアクセスポイントのチャネルを表示します。
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。

ネットワーク

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。

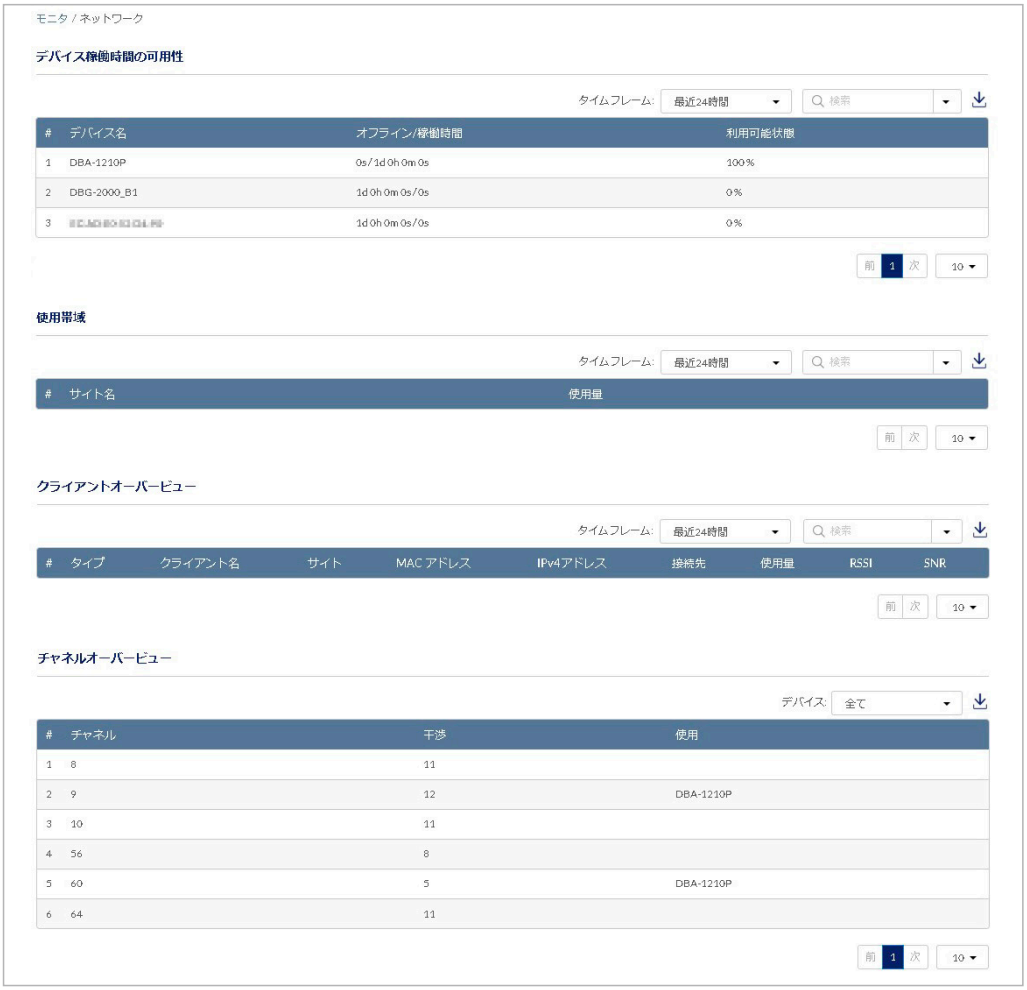


図 8-12　ネットワーク

■ 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。

■ 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。

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、デバイスを指定、表示することもできます。

第 9 章　設定

本章では、Nuclias クラウドのトップ画面にある「設定」メニューについて説明します。

デバイス設定とプロファイル設定

設定 > ゲートウェイ > プロファイル画面と**設定 > ゲートウェイ > デバイス**画面では、セキュリティ設定やネットワーク設定など、Nuclias ゲートウェイの設定を行うことができます。

注意　本章では、**設定 > ゲートウェイ > デバイス**画面に表示される項目の順に設定内容の説明を行います。

■ 設定 > ゲートウェイ > プロファイル画面からの設定

設定 > ゲートウェイ > プロファイル画面で、「ネットワーク」または「セキュリティ」をクリックします。表示されたプロファイルの設定画面でプロファイルの設定を行います。プロファイルとは、デバイスに適用する設定データの集まりです。プロファイルに紐づけられているデバイスすべてに同じ設定を適用することができます。プロファイルの設定画面には「ネットワーク」タブ、および「セキュリティ」タブがあります。

■ 設定 > ゲートウェイ > デバイス画面からの設定

設定 > ゲートウェイ > デバイス画面から、Nuclias クラウドに登録されているデバイスを選択し、選択したデバイスに対して適用する設定を行います。また、デバイス画面では選択したデバイスの情報を確認できます。
デバイスの設定画面には、「ネットワーク」「セキュリティ」タブのほか、「基本」「サマリ」「VPN」「ツール」「ライセンス」タブがあります。

デバイス設定時とプロファイル設定時の表示タブ一覧

- 「基本」タブ（**設定 > ゲートウェイ > デバイス**画面でデバイスを選択した場合のみ表示）
  デバイス名、シリアル番号など、デバイスの情報を確認できます。
- 「サマリ」タブ（**設定 > ゲートウェイ > デバイス**画面でデバイスを選択した場合のみ表示）
  ポートやトラフィックの状態、インターネット使用率などを確認できます。
- 「ネットワーク」タブ
  設定 > ゲートウェイ > デバイス画面と**設定 > ゲートウェイ > プロファイル**画面の両方に表示されます。
  インターフェイス、VLAN などネットワークに関する設定を行います。
- 「セキュリティ」タブ
  設定 > ゲートウェイ > デバイス画面と**設定 > ゲートウェイ > プロファイル**画面の両方に表示されます。
  ファイアウォール、IPS、WEB コンテンツフィルター、アプリケーションコントロールの設定を行います。
- 「VPN」タブ（**設定 > ゲートウェイ > デバイス**画面でデバイスを選択した場合のみ表示）
  VPN の設定を行います。
- 「ツール」タブ（**設定 > ゲートウェイ > デバイス**画面でデバイスを選択した場合のみ表示）
  Ping、トレースルート、デバイスの再起動などを行います。
- 「ライセンス」タブ（**設定 > ゲートウェイ > デバイス**画面でデバイスを選択した場合のみ表示）
  ライセンスの情報を確認できます。

ゲートウェイ - プロファイル画面

プロファイルとは、デバイスに適用する設定データの集まりです。プロファイルに紐づけられているデバイスすべてに同じ設定を適用することができます。本製品のプロファイルでは、VLAN などのネットワーク設定、ファイアウォール、コンテンツフィルタリングなどのセキュリティ設定を行うことができます。

設定 > ゲートウェイ > プロファイルを選択し、本製品に適用するプロファイルを作成、編集する画面を表示します。

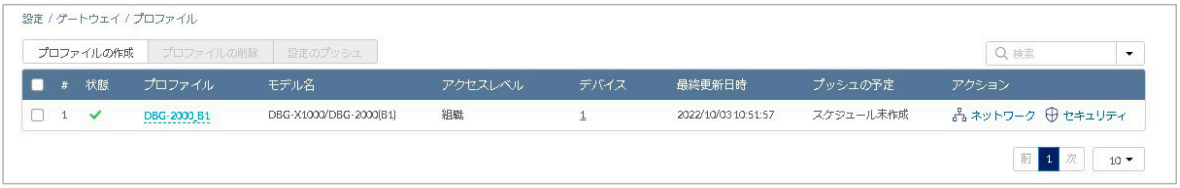


図 9-1　　プロファイル一覧

本画面には以下の項目が含まれます。

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。
プロファイル	プロファイル名が表示されています。プロファイルの名を変更する場合は、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	プロファイルの設定を行います。 • 「ネットワーク」：クリックするとネットワークの設定を行う画面に移行します。 詳細は「「ネットワーク」タブ」を参照してください。 • 「セキュリティ」：クリックするとセキュリティの設定を行う画面に移行します。 詳細は「「セキュリティ」タブ」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検索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 > ゲートウェイ > プロファイル**画面の「プロファイルの作成」をクリックし、次の画面で設定を行います。

図 9-2　　プロファイルの作成

本画面には以下の項目が含まれます。

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	モデル名は、「DBG-X1000/DBG-2000(B1)」を選択する必要があります。
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」: 既に存在するプロファイルをコピーして使用します。

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 > ゲートウェイ > 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 > ゲートウェイ > 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. 次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 9-3　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 > ゲートウェイ > 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 プロファイルの画面のアクション欄で「ネットワーク」または「セキュリティ」を選択して表示される画面からも「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」アイコンに橙色のマークが表示されます。

ゲートウェイ - デバイス画面

設定 > ゲートウェイ > デバイスを選択し、Nuclias に登録されているデバイスの一覧を表示します。
「デバイス名」のリンクをクリックすると、そのデバイスの設定画面に移行します。

図 9-1　　デバイス一覧

画面には以下の項目が含まれます。

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 8 章 モニタ「ゲートウェイ - 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。
マネジメント IP	デバイスのマネジメント IP アドレスを表示します。
デフォルト WAN IPv4	デバイスのデフォルト WAN IPv4 アドレスを表示します。
デフォルト WAN IPv6	デバイスのデフォルト WAN IPv6 アドレスを表示します。
ローカル IP	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	デバイスに最新のデバイス設定が同期されているかを表示します。
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。
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。
デバイス UID	デバイスの UID 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	接続されているクライアント数を表示します。
使用量	使用量を表示します。
チャネル	無線対応機器の場合、現在使用しているチャネルを表示します。「(2.4G 帯のチャネル)/(5G 帯のチャネル)」表示です。 無線非対応機器の場合は - が表示されます。
送信電波出力	デバイスにて設定されている送信電波出力の値を表示します。無線非対応機器の場合は「-」が表示されます。
チャネル帯域	現在選択しているチャネル帯域を表示します。

■ デバイスの追加
「デバイスの追加」の詳細については第 11 章 管理「デバイスの追加」を参照してください。

■ 表示する期間の変更
「タイムフレーム」で表内の「接続」欄に表示するタイムバーの期間を選択します。

■ 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。表示する項目のチェックボックス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。

「基本」タブ

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**基本**」タブを選択

「基本」タブでは、デバイスやデフォルト WAN、サイトの情報を確認できます。

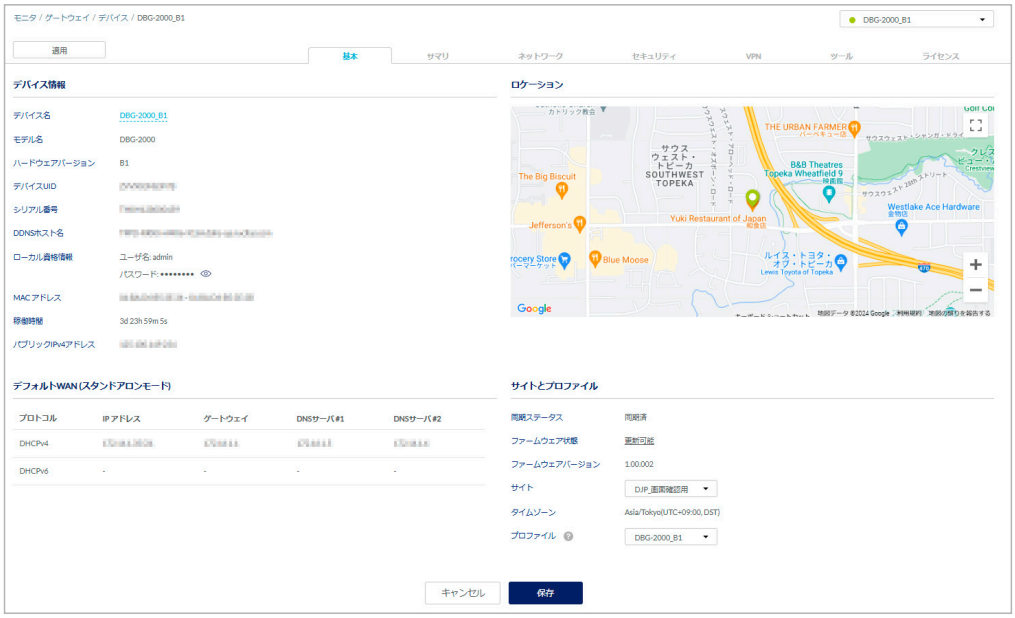


図 9-2　　デバイス - 基本

■ デバイス情報
デバイス名、モデル名、ハードウェアバージョン、デバイス UID、シリアル番号、DDNS ホスト名、ローカル資格情報、MAC アドレス、稼働時間、パブリック IPv4 アドレスを表示します。
デバイス名は変更可能です。

注意　「ハードウェアバージョン」項目は、DBG-2000 のみに表示されます。

■ デフォルト WAN
WAN 接続の状態を表示します。DHCPv4、DHCPv6、PPPoE 等で使用している IP アドレスを表示します。

■ 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、プロファイルを表示します。
サイトとプロファイルはドロップダウンリストから選択できます。

設定後、「保存」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。

「サマリ」タブ

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**サマリ**」タブを選択

「サマリ」タブでは、本製品の設定の概要を確認できます。

サマリ - 状態

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**サマリ**」タブ >「**状態**」タブを選択

ポートの使用状況やトラフィック量を確認できます。

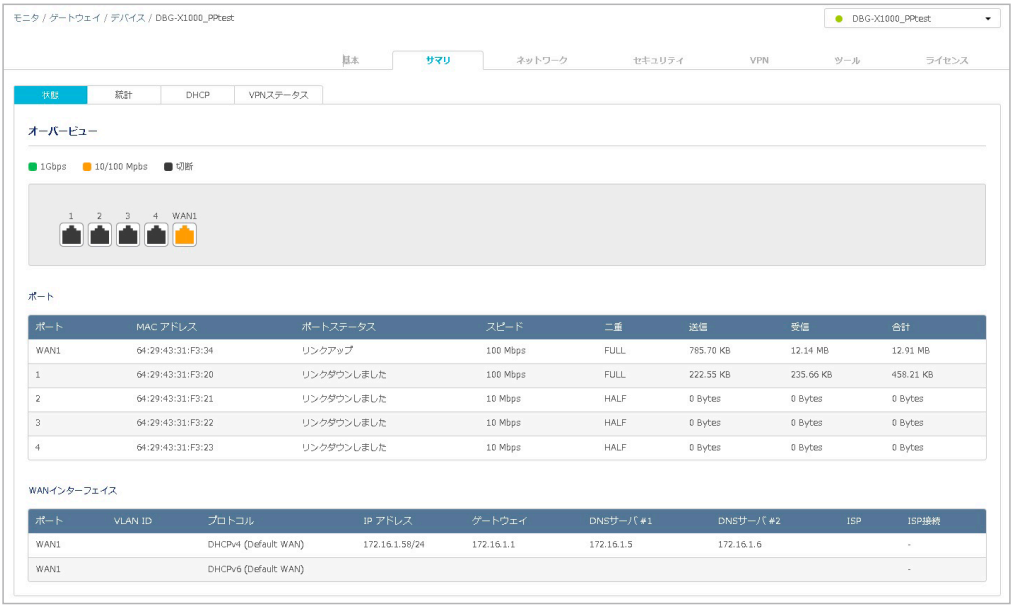


図 9-3　　状態（DBG-2000）

■ オーバービュー

各ポートの状態をイラストで表示します。

- 水色：2.5Gbps で接続されています。
- 緑色：1Gbps で接続されています。
- 橙色：10/100Mbps で接続されています。
- 黒色：接続されていません。またはポートが無効になっています。

注意　2.5Gbps での接続は、DBG-2000 のみ対応しています。

■ ポート

各ポートの MAC アドレスと使用状況を表示します。

■ WAN インターフェイス

WAN1/WAN2 ポートで使用しているプロトコル、IP アドレス、ゲートウェイ、 DNS サーバ #1、DNS サーバ #2、ISP、ISP 接続を表示します。

注意　WAN2 ポートを使用するデュアル WAN 機能は、DBG-2000 で今後サポート予定です。

サマリ - 統計

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**サマリ**」タブ >「**統計**」タブを選択

接続クライアント数、ワイヤレス、インターネットトラフィック、インターネット使用量の情報を表示します。

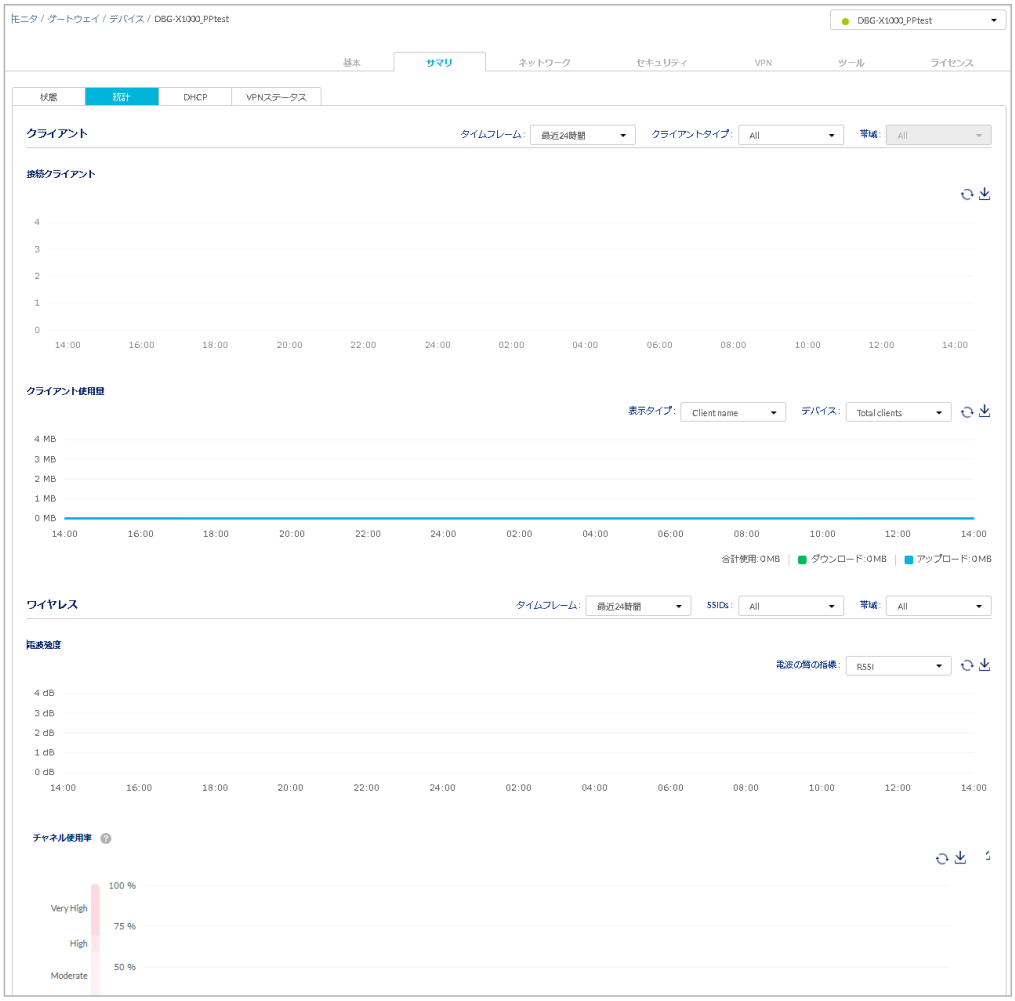


図 9-4　「統計」タブ

注意　「ワイヤレス」欄は、DBG-X1000 のみに表示されます。

■ 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。
表示の対象とする時間の範囲を「タイムフレーム」、表示するクライアントの種別を「クライアントタイプ」、表示対象とする帯域を「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、「タイムフレーム」の設定に応じて時間別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**
  クライアントの使用量を、「タイムフレーム」の設定に応じて時間別または日別に曲線グラフで表示します。表示の種類、および表示の対象とするデバイスを選択できます。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」：表示の種別をプルダウンメニューから選択します。
  - 「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

1 時間ごと、または 1 日ごとの電波の強度、チャネルの使用率、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」、表示する SSID の種別を「SSIDs」、表示対象とする帯域を「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。

- **チャネル使用率**
  チャ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。

■ インターネットトラフィック

一時間ごとのインターネットのトラフィック量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。

■ インターネット使用

「タイムフレーム」で指定した時間の範囲のインターネットの使用量をインターフェイスタイプ別に表示します。以下の項目を設定します。
- 「インターフェイスタイプ」：表示の対象とするインターフェイスの種類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。

サマリ - DHCP

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**サマリ**」タブ >「**DHCP**」タブを選択

DHCPv4 と DHCPv6 のサブネットとリースの情報を表示します。
DHCP（Dynamic Host Configuration Protocol）は、LAN 内のパソコンやスマートフォンなどのデバイスに、IP アドレスを自動で割り当てる機能です。割り当てには IP アドレスプールを使用します。デバイスがネットワークに追加され、DHCP サーバから IP アドレスを動的に取得するよう要求されると、設定された IP プール内の IP アドレスがデバイスに割り当てられます。割り当てられた IP アドレスは、一定の期間のみクライアントに割り当てられる仕組み（DHCP リース）になっています。DHCP リースの期間が終了すると、リースの更新が行われます。

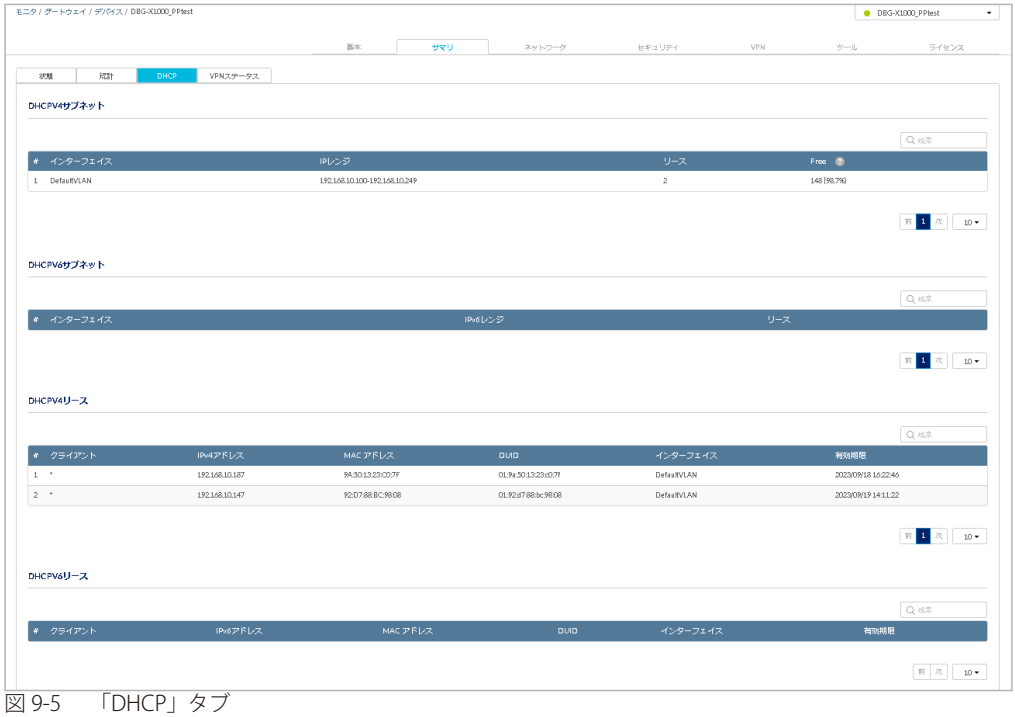


図 9-5　「DHCP」タブ

■ DHCPV4 サブネット / DHCPV6 サブネット

IP アドレス範囲、設定されているインターフェイス、使用中の IP アドレス数、IP アドレスプールの使用状況を表示します。

項目	説明
DHCPV4 サブネット	
インターフェイス	DHCP サブネットが設定されているインターフェイスを表示します。
IP レンジ	割り当てることができる IP アドレスの範囲を表示します。
リース	割り当てられている IP アドレスの数を表示します。
Free	割り当てられていない IP アドレスの数と、DHCP プール内の空いている IP アドレスの割合を表示します。
DHCPV6 サブネット	
インターフェイス	DHCP サブネットが設定されているインターフェイスを表示します。
IPv6 レンジ	割り当てることができる IPv6 アドレスの範囲を表示します。
リース	割り当てられている IP アドレスの数を表示します。

■ DHCPV4 リース / DHCPV6 リース

DHCP リース時間は、DHCP サーバによって IP アドレスがクライアントに割り当てられる時間です。
DHCP リースエリアでは、ネットワーク上のクライアントに提供される DHCP リースの一覧を表示します。

項目	説明
DHCPV4 リース	
クライアント	IPv4 アドレスが割り当てられているクライアントの名前を表示します。
IPv4 アドレス	クライアントに割り当てられた IPv4 アドレスを表示します。
MAC アドレス	IP アドレスが予約されているクライアントの MAC アドレスを表示します。
DUID	DUID (DHCP Unique Identifier) を表示します。
インターフェイス	クライアントが接続されているインターフェイスを表示します。
有効期限	DHCP リースの有効期限を表示します。
DHCPV6 リース	
クライアント	IPv6 アドレスが割り当てられているクライアントの名前を表示します。
IPv6 アドレス	クライアントに割り当てられた IPv6 アドレスを表示します。
MAC アドレス	IP アドレスが予約されているクライアントの MAC アドレスを表示します。
DUID	DUID (DHCP Unique Identifier) を表示します。
インターフェイス	クライアントが接続されているインターフェイスを表示します。
有効期限	DHCP リースの有効期限を表示します。

サマリ - VPN ステータス

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**サマリ**」タブ >「**VPN ステータス**」タブを選択

VPN の使用情報を表示します。

「VPN タイプの表示」で、表示する VPN タイプを選択します。「概要」を選択した場合はすべての VPN タイプを表示します。
右上の アイコンをクリックすると表示を切り替えられます。

図 9-6　　VPN ステータス

VPN 設定の詳細については「「VPN」タブ」を参照してください。

「ネットワーク」タブ

● 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブを選択

● 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「ネットワーク」を選択

本製品のネットワーク設定について説明します。ネットワークの設定画面には、以下のタブが表示されます。
表示されるタブの種類は、デバイス設定時とプロファイル設定時で異なります。

- 「イーサネット」タブ
  ポートの設定を行います。ポートのステータスやリンク速度、WAN ポートの接続構成などを設定します。
- 「ワイヤレス」タブ
  無線対応機器の場合、SSID、および無線機能の設定を行います。
- 「アドレッシング」タブ
  VLAN、および IP プールの設定を行います。
- 「ルーティング」タブ
  ルーティング（スタティックルート、ポリシールート、RIP、および OSPFV2）の設定を行います。
- 「トラフィック管理」タブ
  トラフィック帯域幅、およびセッション制限の設定を行います。
- 「キャプティブポータル」タブ
  認証に使用するキャプティブポータルの設定を行います。

注意　プロファイル設定時とデバイス設定時では、表示される画面が一部異なります。以下ではデバイス設定時の画面を使用して説明します。

注意　「プロファイルコンフィグを使用する」を有効にすると、プロファイル画面で設定した内容が本製品に適用されます。
「プロファイルコンフィグを使用する」を無効にすると、デバイス画面で設定した内容が本製品に適用されます。

参照 設定項目の詳細については以下を参照してください。

「ネットワーク - イーサネット」
「ネットワーク - ワイヤレス」
「ネットワーク - アドレッシング」
「ネットワーク - ルーティング」
「ネットワーク - トラフィック管理」
「ネットワーク - キャプティブポータル」

ネットワーク - イーサネット

- 画面の表示手順（デバイス設定時）：**設定** > **ゲートウェイ** > **デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**イーサネット**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定** > **ゲートウェイ** > **プロファイル** 画面で「ネットワーク」を選択 →「**イーサネット**」タブを選択

以下では、ネットワークのイーサネット設定について説明します。
ポートステータスやリンク速度、WAN ポートの接続構成の設定などを行います。

本画面には以下の項目が表示されます。

図 9-7　「イーサネット」タブ

設定後、画面上部の「適用」をクリックします。

ネットワーク - イーサネット - ポート設定

図 9-8　ポート設定

各ポートの設定を表示、編集することができます。

項目	説明
ポート	ポートを表示します。
リンクステート	リンク速度を表示します。
ポートステータス	ポートの有効 / 無効を表示します。
アクション	ポートの設定を変更できます。

「編集」をクリックすると次の画面が表示され、ポートの有効 / 無効とリンク速度を設定できます。

図 9-9　LAN ポートの編集

ネットワーク - イーサネット - インターフェイス設定

WAN ポートを設定し、インターネットへの接続を確立できます。
インターネットの利用にはサービスプロバイダ（ISP）との契約が必要です。本製品のセットアップに必要な情報については、ISP またはネットワーク管理者にお問い合わせください。
次の画面で WAN ポートの設定を追加、編集、削除できます。

図 9-10　インターフェイス設定（DBG-2000）

■ ネットワーク - イーサネット - インターフェイス設定（WAN ポートの編集 / 追加）

アクション欄の「編集」をクリックし、次の画面で WAN ポートの編集を行います。

図 9-11　WAN ポートの編集（DHCPv4 選択時）

回線の設定を追加する場合には、「追加」をクリックして設定追加ウィンドウを表示し、「プロトコル」を選択します。
以下は PPPoE を使用する場合の画面です。

図 9-12　プロトコルの選択

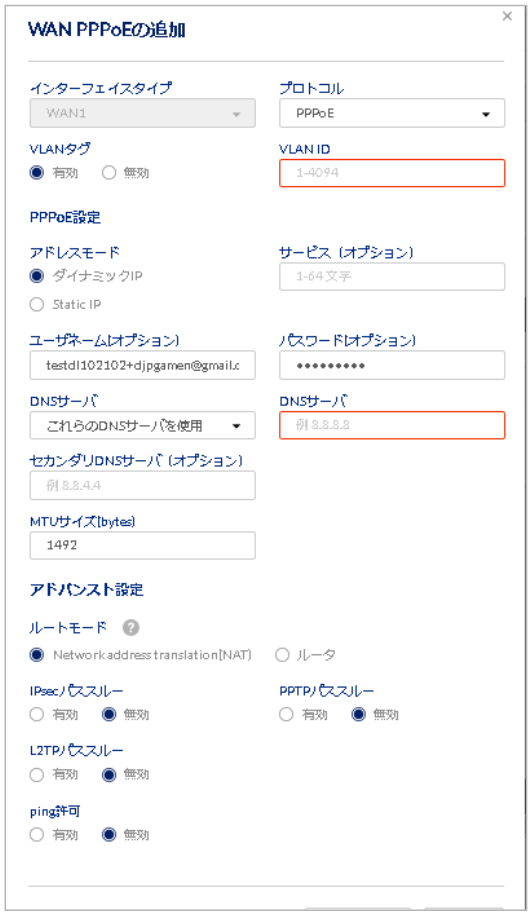


図 9-13　WAN PPPoE の追加

● 接続タイプごとの設定

ポートの接続タイプによって、設定する項目が異なります。接続タイプごとの設定は以下を参照してください。

- 「WAN ポートの設定 - DHCPv4 を選択した場合」
- 「WAN ポートの設定 - DHCPv6 を選択した場合」
- 「WAN ポートの設定 - スタティック IPv4 を選択した場合」
- 「WAN ポートの設定 - スタティック IPv6 を選択した場合」
- 「WAN ポートの設定 - PPPoE を選択した場合」
- 「WAN ポートの設定 - DS-Lite/IPIP を選択した場合」
- 「WAN ポートの設定 - MAP-E を選択した場合」

WAN ポートの設定 - DHCPv4 を選択した場合

「プロトコル」で「DHCPv4」を選択した場合の設定項目について説明します。

項目	説明
VLAN タグ	VLAN タグが有効になります。VLAN ID を指定します。
DHCPv4	
ホスト名（オプション）	ISP で必要な場合は、ホスト名を入力します。
DNS サーバ	「ISP からダイナミックを取得」または「これらの DNS サーバを使用」のいずれかを選択します。
プライマリ DNS サーバ	「これらの DNS サーバを使用」を選択した場合は、プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS サーバ（オプション）	「これらの DNS サーバを使用」を選択した場合は、セカンダリ DNS サーバの IP アドレスを入力します。 本項目はオプションです。
MTU サイズ (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。
アドバンスト設定	
ルートモード	ルーティングモードを NAT モードまたはルータモードに設定します。
IPsec パススルー	IPsec パススルーを有効 / 無効に設定します。 有効にすると、IPsec による VPN 通信を通過させることが可能となります。
PPTP パススルー	PPTP パススルーを有効 / 無効に設定します。 有効にすると、PPTP による VPN 通信を通過させることが可能となります。
L2TP パススルー	L2TP パススルーを有効 / 無効に設定します。 有効にすると、L2TP による VPN 通信を通過させることが可能となります。
ping 許可	Ping の許可を有効 / 無効に設定します。

WAN ポートの設定 - DHCPv6 を選択した場合

「プロトコル」で「DHCPv6」を選択した場合の設定項目について説明します。

項目	説明
VLAN タグ	VLAN タグが有効になります。VLAN ID を指定します。
DHCPv6	
ホスト名（オプション）	ISP で必要な場合は、ホスト名を入力します。
DNS サーバ	「ISP からダイナミックを取得」または「これらの DNS サーバを使用」のいずれかを選択します。
プライマリ DNS サーバ	「これらの DNS サーバを使用」を選択した場合は、プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS サーバ（オプション）	「これらの DNS サーバを使用」を選択した場合は、セカンダリ DNS サーバの IP アドレスを入力します。 本項目はオプションです。
MTU サイズ (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。
アドバンスト設定	
ping 許可	Ping の許可を有効 / 無効に設定します。

WAN ポートの設定 - スタティック IPv4 を選択した場合

「プロトコル」で「スタティック IPv4」を選択した場合の設定項目について説明します。

項目	説明
VLAN タグ	VLAN タグが有効になります。VLAN ID を指定します。
スタティック IPv4	
IP アドレス	ISP から提供されたスタティック IP アドレスを入力します。
IP サブネットマスク	IP サブネットマスクを入力します。
ゲートウェイ IP アドレス	デフォルトゲートウェイの IP アドレスを入力します。
プライマリ DNS サーバ	プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS サーバ（オプション）	セカンダリ DNS サーバの IP アドレスを入力します。本項目はオプションです。
MTU サイズ (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。

項目	説明
アドバンスト設定	
ルートモード	ルーティングモードを NAT モードまたはルータモードに設定します。
IPsec パススルー	IPsec パススルーを有効 / 無効に設定します。 有効にすると、IPsec による VPN 通信を通過させることが可能となります。
PPTP パススルー	PPTP パススルーを有効 / 無効に設定します。 有効にすると、PPTP による VPN 通信を通過させることが可能となります。
L2TP パススルー	L2TP パススルーを有効 / 無効に設定します。 有効にすると、L2TP による VPN 通信を通過させることが可能となります。
ping 許可	Ping の許可を有効 / 無効に設定します。

WAN ポートの設定 - スタティック IPv6 を選択した場合

「プロトコル」で「スタティック IPv6」を選択した場合の設定項目について説明します。

項目	説明
VLAN タグ	VLAN タグが有効になります。VLAN ID を指定します。
Static IPv6	
IPv6 アドレス	ISP から提供されたスタティック IPv6 アドレスを入力します。
IPv6 ゲートウェイ	デフォルトゲートウェイの IPv6 アドレスを入力します。
IPv6 routed プレフィックス（オプション）	IPv6 アドレス範囲を設定します。本項目はオプションです。
IPv6 サフィックス（オプション）	IPv6 サフィックスを入力します。本項目はオプションです。
プライマリ DNS サーバ	プライマリ DNS サーバの IPv6 アドレスを入力します。
セカンダリ DNS サーバ（オプション）	セカンダリ DNS サーバの IPv6 アドレスを入力します。本項目はオプションです。
MTU サイズ (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。
アドバンスト設定	
ping 許可	Ping の許可を有効 / 無効に設定します。

WAN ポートの設定 - PPPoE を選択した場合

「プロトコル」で」「PPPoE」を選択した場合の設定項目について説明します。

項目	説明
VLAN タグ	VLAN タグの有効 / 無効を選択します。有効にした場合は VLAN ID を選択します。
PPPoE 設定	
アドレスモード	「ダイナミック IP」または「Static IP」を選択します。
サービス（オプション）	ISP がサービス名をサポートしている場合は、ここに入力します。本項目はオプションです。
ユーザネーム（オプション）	PPPoE ユーザ名を入力します。本項目はオプションです。
パスワード（オプション）	PPPoE パスワードを入力します。本項目はオプションです。
IP アドレス	「アドレスモード」で「Static IP」を選択した場合は、ISP から提供された IP アドレスを入力します。
IP サブネットマスク	「アドレスモード」で「Static IP」を選択した場合は、ISP から提供されたサブネットマスクを入力します。
DNS サーバ	「ISP からダイナミックを取得」または「これらの DNS サーバを使用」のいずれかを選択します。
DNS サーバ	「これらの DNS サーバを使用」を選択した場合は、プライマリ DNS サーバの IP アドレスを入力します。
セカンダリ DNS サーバ（オプション）	「これらの DNS サーバを使用」を選択した場合は、セカンダリ DNS サーバの IP アドレスを入力します。 本項目はオプションです。
MTU サイズ (bytes)	MTU サイズを入力します。 MTU（Maximum Transmit Unit）は、ネットワークで一回に送信できる最大のデータサイズ（単位：byte）です。 例えば、B フレッツは 1454bytes、DS-Lite は 1460bytes です。 その他の回線の場合も、使用するネット回線に合わせて適正な値を入力してください。

項目	説明
アドバンスト設定	
ルートモード	ルーティングモードを NAT モードまたはルータモードに設定します。
IPsec パススルー	IPsec パススルーを有効 / 無効に設定します。 有効にすると、IPsec による VPN 通信を通過させることが可能となります。
PPTP パススルー	PPTP パススルーを有効 / 無効に設定します。 有効にすると、PPTP による VPN 通信を通過させることが可能となります。
L2TP パススルー	L2TP パススルーを有効 / 無効に設定します。 有効にすると、L2TP による VPN 通信を通過させることが可能となります。
ping 許可	Ping の許可を有効 / 無効に設定します。

WAN ポートの設定 - DS-Lite/IPIP を選択した場合

「プロトコル」で「DS-Lite/IPIP」を選択した場合の設定項目について説明します。

選択したサービスプロバイダによって設定項目が異なります。

項目	説明	
DS-Lite 設定		
サービスプロバイダ	サービスプロバイダを以下から選択します。 • 「インターネットマルチフィード（Transix）」 • 「日本ネットワークイネイブラー（v6 plus-fixed IP）」 • 「ASAHI ネット v6 コネクト」 • 「カスタマイズドサービス」	
	「インターネットマルチフィード（Transix）」選択時	
	AFTR アドレスを指定	「ISP から情報を取得」または「AFTR アドレスを指定」を選択します。 「ISP から情報を取得」を選択した場合、以降の設定項目は表示されません。
	ピアトンネル IPv6 アドレス	ピアトンネル IPv6 アドレスを入力します。
	インタフェース ID	インタフェース ID を入力します。
	グローバル IPv4 アドレス	グローバル IPv4 アドレスを入力します。
	アップデート URL	アップデートサーバの URL を設定します。
	ユーザネーム（オプション）	ユーザ名を設定します。本項目はオプションです。
	パスワード（オプション）	パスワードを設定します。本項目はオプションです。
	「日本ネットワークイネイブラー（v6 plus-fixed IP）」選択時	
	BR アドレス	BR の IPv6 アドレスを入力します。
	インタフェース ID	インタフェース ID を入力します。
	グローバル IPv4 アドレス	グローバル IPv4 アドレスを入力します。
	アップデート URL	アップデートサーバの URL を設定します。
	ユーザネーム（オプション）	ユーザ名を設定します。本項目はオプションです。
	パスワード（オプション）	パスワードを設定します。本項目はオプションです。
	「ASAHI ネット v6 コネクト」選択時	
	AFTR アドレスを指定	「ISP から情報を取得」または「AFTR アドレスを指定」を選択します。 「ISP から情報を取得」を選択した場合、以降の設定項目は表示されません。
	ピアトンネル IPv6 アドレス	ピアトンネル IPv6 アドレスを入力します。
	インタフェース ID	インタフェース ID を入力します。
	グローバル IPv4 アドレス	グローバル IPv4 アドレスを入力します。
	アップデート URL	アップデートサーバの URL を設定します。
	ユーザネーム（オプション）	ユーザ名を設定します。本項目はオプションです。
	パスワード（オプション）	パスワードを設定します。本項目はオプションです。
	「カスタマイズドサービス」選択時	
	AFTR (address family transition router) address	AFTR アドレスを指定します。

項目	説明
アドバンスト設定	
サービスプロバイダに「カスタマイズドサービス」を選択した場合は表示されません。 「AFTR アドレスを指定」で「ISP から情報を取得」を選択した場合は表示されません。	
ルートモード	ルーティングモードを NAT モードまたはルータモードに設定します。
IPsec パススルー	IPsec パススルーを有効 / 無効に設定します。 有効にすると、IPsec による VPN 通信を通過させることが可能となります。
PPTP パススルー	PPTP パススルーを有効 / 無効に設定します。 有効にすると、PPTP による VPN 通信を通過させることが可能となります。
L2TP パススルー	L2TP パススルーを有効 / 無効に設定します。 有効にすると、L2TP による VPN 通信を通過させることが可能となります。

WAN ポートの設定 - MAP-E を選択した場合

「プロトコル」で「MAP-E」を選択した場合の設定項目について説明します。

項目	説明
MAP-E 設定	
サービスプロバイダ	サービスプロバイダを以下から選択します。 • 「Japan Network Enabler（v6 Plus）」 • 「NTT Com (OCN)」
IPv4 アドレスモード	「NTT Com (OCN)」を選択した場合、IPv4 アドレスモードを「ダイナミック IP」「固定 IP」から選択します。
グローバル IPv4 アドレス	IPv4 アドレスモードを「固定 IP」に設定した場合、グローバル IPv4 アドレスを入力します。

ネットワーク - イーサネット - デフォルト WAN 設定

デフォルト WAN を設定します。

図 9-14　デフォルト WAN 設定

本画面には以下の項目が含まれます。

項目	説明
IPv4 デフォルト WAN	IPv4 デフォルト WAN を選択します。
IPv6 デフォルト WAN	IPv6 デフォルト WAN を選択します。

ネットワーク - イーサネット - WAN モード設定

WAN モード設定エリアの設定内容について説明します。

注意 DBG-X1000 は「WAN モード設定」には対応していません。本項目は DBG-2000 のデバイスの設定画面にのみ表示されます。

「WAN モード」を「スタンドアロンモード」「自動ロールオーバー」「ロードバランシング」から選択します。
選択した WAN モードによって、設定する内容は異なります。

注意 以下の機能は、ここでの WAN モードの設定にかかわらず、専用の WAN の設定に基づいて動作します。
・「SITE TO SITE マニュアル VPN」「スタティックルート」「ポリシールート」

注意 「自動ロールオーバー」と「ロードバランシング」は、IPv4 にのみ適用されます。「自動ロールオーバー」と「ロードバランシング」を設定した場合、IPv4 デフォルト WAN の設定は適用されません。IPv6 には、IPv6 デフォルト WAN の設定が適用されます。

※自動ロールオーバー、ロードバランシングは IPv4 のみサポートされています。IPv6 は今後のアップデートでサポート予定です。
IPoE については、未サポートです。

■「WAN モード」に「スタンドアロンモード」を選択した場合

「自動ロールオーバー」「ロードバランシング」機能を使用しない場合は、「WAN モード」に「スタンドアロンモード」を選択します。

図 9-15　WAN モード設定

■「WAN モード」に「自動ロールオーバー」を選択した場合

「自動ロールオーバー」を使用すると、何らかの理由でプライマリ WAN ポートがダウンした場合、セカンダリ WAN ポートを使用して通信を行うことができます。本機能を使用するには、プライマリ / セカンダリ両方の WAN ポートが ISP へ接続可能である必要があります。セカンダリ WAN ポートは、プライマリ WAN ポートで障害が検出されるまでは未接続の状態となります。プライマリ WAN ポートの接続の状態は、事前に設定した一定の間隔でチェックされます。

図 9-16　WAN モード設定（自動ロールオーバー）

本画面には以下の項目が含まれます。

項目	説明
プライマリ WAN	プライマリ WAN ポートを選択します。
セカンダリ WAN	セカンダリ WAN ポートを選択します。
ヘルスチェック方法	ヘルスチェックは、負荷分散を行う WAN ポートが通信可能な状態かチェックする機能です。 ヘルスチェックを行う方法を選択します。 • 「WAN DNS サーバ」：WAN に設定された WAN DNS サーバを使用してヘルスチェックを行います。 • 「DNS サーバ」：特定の DNS サーバを使用してヘルスチェックを行います。「DNS サーバ」を選択した場合は、表示される「プライマリ WAN」と「セカンダリ WAN」欄で DNS サーバの IPv4/IPv6 アドレスを入力します。 • 「Ping IP アドレス」：IP アドレスに Ping を送信してヘルスチェックを行います。「Ping IP アドレス」を選択した場合は、表示される「プライマリ WAN」と「セカンダリ WAN」欄で IPv4/IPv6 アドレスを入力します。
プライマリ WAN	本項目は、「ヘルスチェック方法」で「DNS サーバ」「Ping IP アドレス」を選択した場合に表示されます。 プライマリ WAN ポートを使用してヘルスチェックを行う IPv4/IPv6 アドレスを入力します。
セカンダリ WAN	本項目は、「ヘルスチェック方法」で「DNS サーバ」「Ping IP アドレス」を選択した場合に表示されます。 セカンダリ WAN ポートを使用してヘルスチェックを行う IPv4/IPv6 アドレスを入力します。

項目	説明
ヘルスチェックインターバル	WAN のヘルスチェックを行う間隔（単位：秒）を入力します。 初期値では 30 秒ごとにヘルスチェックを行います。
ヘルスチェックリトライ	ポートがダウンしたと見なされるまでのヘルスチェックの失敗回数を入力します。

■「WAN モード」に「ロードバランシング」を選択した場合

ロードバランシング（負荷分散）は、複数の WAN リンクを使用して、トラフィックの負荷が均等になるように処理を振り分ける機能です。
負荷を分散する方法には「ラウンドロビン」と「スピルオーバー」の 2 種類があります。

- **ラウンドロビン**
  複数の WAN リンクに対し均等に処理を振り分けます。
  1 つのパケットが 1 つ目の WAN ポートに転送されると、次のパケットは自動的に 2 つ目の WAN ポートに転送されます。これにより、トラフィックの負荷がすべてのアクティブな WAN ポートに分散されます。
- **スピルオーバー**
  設定した帯域幅のしきい値に達するまで、1 つ目の WAN ポートが処理を行います。しきい値に達すると、2 つ目の WAN ポートが処理を行います。
  帯域幅のしきい値は、「ロード許容範囲」（帯域幅の割合）と「最大帯域幅」で設定します。
  （例）：
  「最大帯域幅」が 1000Mbps で「ロード許容範囲」が 70 の場合：
  1 つ目の WAN ポートで、帯域幅が 1000Mbps の 70% に達した場合、2 つ目の WAN ポートに切り替わります。

図 9-17　ロードバランシング（ラウンドロビン）

図 9-18　ロードバランシング（スピルオーバー）

本画面には以下の項目が含まれます。

項目	説明
Load balancing	ロードバランシングの方法を「ラウンドロビン」「スピルオーバー」から選択します。
プライマリ WAN	プライマリ WAN として使用する WAN を「WAN1」または「WAN2」より選択します。
セカンダリ WAN	「プライマリ WAN」で選択しなかった方の WAN が自動的に選択されます。
ヘルスチェック方法	ヘルスチェックは、負荷分散を行う WAN ポートが通信可能な状態かチェックする機能です。 ヘルスチェックを行う方法を以下から選択します。 • 「WAN DNS サーバ」：WAN に設定された WAN DNS サーバを使用して WAN リンクのヘルスチェックを行います。 • 「DNS サーバ」：特定の DNS サーバを使用して WAN リンクのヘルスチェックを行います。「DNS サーバ」を選択した場合は、表示される「プライマリ WAN」「セカンダリ WAN」欄で DNS サーバの IPv4/IPv6 アドレスを入力します。 • 「Ping IP アドレス」：IP アドレスに Ping を送信して WAN リンクのヘルスチェックを行います。「Ping IP アドレス」を選択した場合は、表示される「プライマリ WAN」「セカンダリ WAN」欄で IPv4/IPv6 アドレスを入力します。
ヘルスチェックインターバル	WAN のヘルスチェックを行う間隔（単位：秒）を入力します。 初期値では 30 秒ごとにチェックを行います。
ヘルスチェックリトライ	ポートがダウンしたと見なされるまでのヘルスチェック失敗の回数を入力します。
プライマリ WAN ロード許容範囲	「Load balancing」に「スピルオーバー」を選択した場合に表示されます。 しきい値となる帯域幅の割合を入力します。この割合を超えると、「セカンダリ WAN」に設定された WAN に切り替わります。 設定可能範囲：20 - 80
プライマリ WAN 最大帯域幅	「Load balancing」に「スピルオーバー」を選択した場合に表示されます。 しきい値となる帯域幅を入力します。この帯域幅に対するロード許容範囲を超えると、「セカンダリ WAN」に設定された WAN に切り替わります。 設定可能範囲：1 - 2500（Mbps）

ネットワーク - イーサネット - ダイナミック DNS

ダイナミック DNS（DDNS）は、割り当てられたグローバル IP アドレスを、固定のドメインと紐付けるサービスです。
DDNS を使用する場合は、DynDNS、FreeDNS、NO-IP、3322.org などのサービスプロバイダを指定します。

次の画面で DDNS を設定できます。また、アクション欄からは編集と削除を実行できます。

図 9-19　ダイナミック DNS 設定

■ DDNS の追加

「追加」をクリックし、次の画面で DDNS の設定を行います。

図 9-20　DDNS の追加

本画面には以下の項目が含まれます。

項目	説明
サービスプロバイダ	サービスプロバイダを「Nuclias.com」「DynDNS」「FreeDNS」「NO-IP」「3322.org」から選択します。 サービスプロバイダを「Nuclias.com」に設定した場合は、「ホスト名」の設定のみ行います。
WAN インターフェイス	WAN インターフェイスを選択します。
IP アドレスタイプ	IP アドレスタイプを「IPv4」「IPv6」から選択します。「3322.org」を選択した場合は「IPv4」が選択されます。
ユーザ名	サービスプロバイダのアカウントユーザ名を入力します。
パスワード	サービスプロバイダのアカウントのパスワードを入力します。
ホスト名	選択した DDNS サービスで WAN インターフェイス IP とマッピングするホスト名を指定します。
パブリック IP を使用	有効にすると、デバイスの WAN IP アドレスの代わりに外部（NAT ルータ）の IP アドレスが使用されます。
強制アップデートインターバル	DDNS サービスのホスト情報を自動的に更新する間隔を指定します。

「保存」をクリックし、設定を保存します。

ネットワーク - ワイヤレス

- 画面の表示手順（デバイス設定時）：**設定** > **ゲートウェイ** > **デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**ワイヤレス**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定** > **ゲートウェイ** > **プロファイル** 画面で「ネットワーク」を選択 →「**ワイヤレス**」タブを選択

注意　「ワイヤレス」の設定は無線対応機器でのみ可能です。DBG-2000 のデバイス設定画面では、「ワイヤレス」タブが表示されません。

次の画面で無線設定を行います。

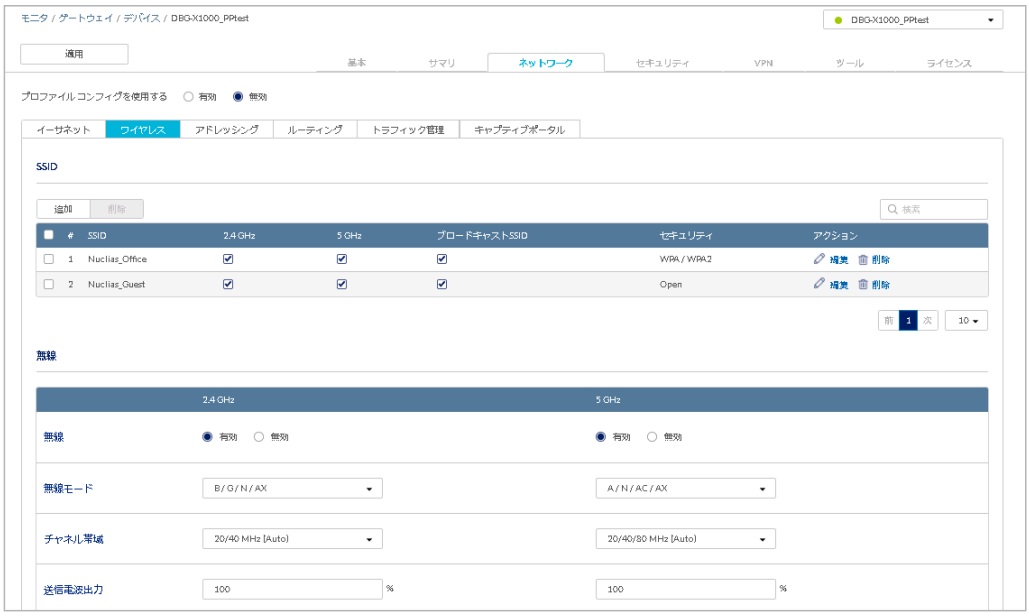


図 9-21　ワイヤレス（DBG-X1000 デバイス画面）

ネットワーク - ワイヤレス - SSID

SSID 一覧の「アクション」欄で「編集」をクリックすると、下記の画面が表示されます。

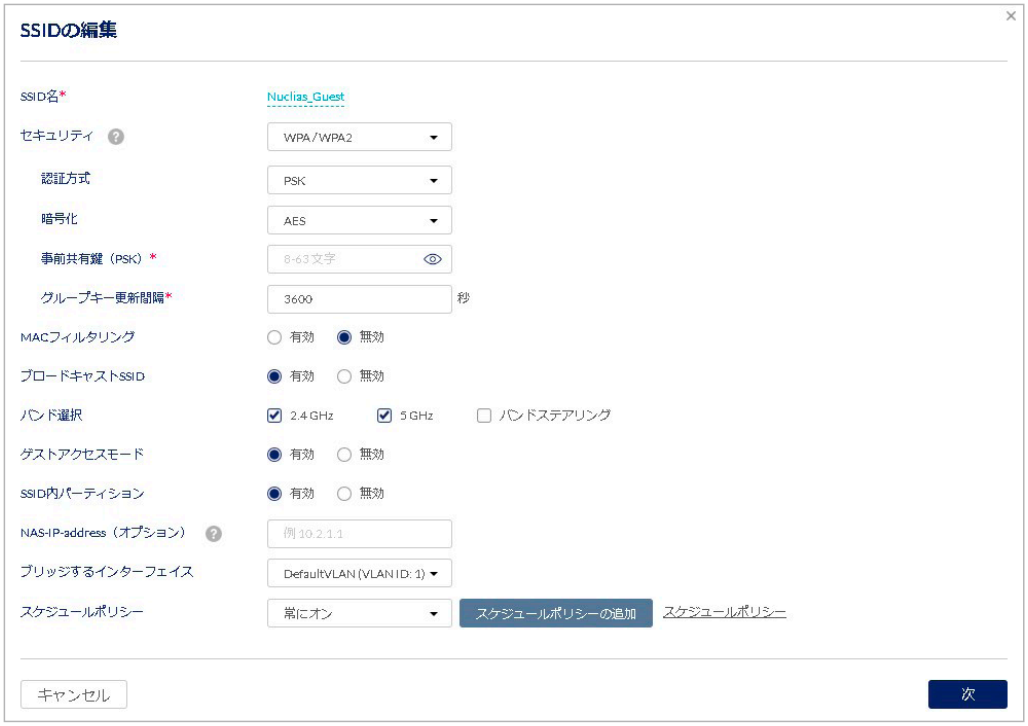


図 9-22　SSID の編集

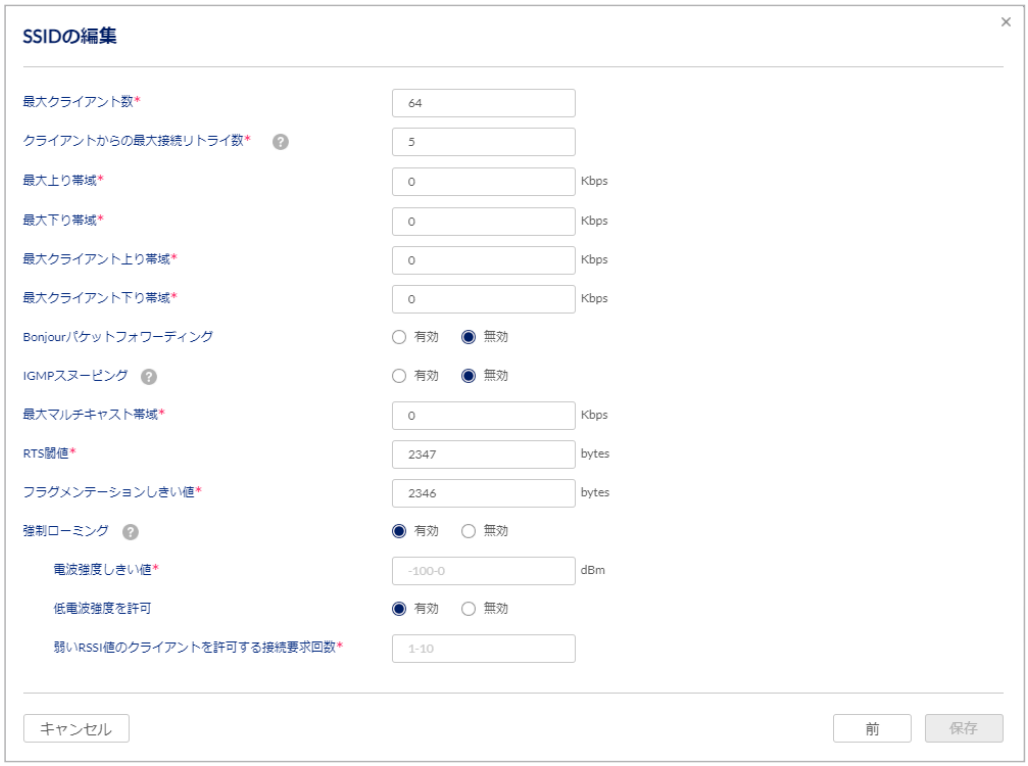


図 9-23　SSID の編集

本画面には以下の項目が含まれます。

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。 特殊文字：「?」「"」「$」「[」「\」「]」「+」 制限概要：使用できません。 特殊文字：「!」「#」「;」 制限概要：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。
MAC フィルタリング	MAC フィルタリングの有効 / 無効を指定します。 有効にした場合、MAC ACL を指定、または RADIUS サーバを選択します。 ● MAC ACL 時は下記の設定を行います。 ・「MAC ACL ポリシ」：ポリシーによる「許可」または「拒否」を選択します。 ・「MAC ACL 名」：MAC ACL を選択します。「MAC ACL の追加」をクリックして、新規エントリを作成することもできます。 ● 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」：RADIUS サーバを指定します。「RADIUS サーバの追加」をクリックして、新規エントリを作成することもできます。
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。
バンド選択	SSID のバンド（帯域）を選択します。「2.4GHz」「5GHz」から選択し、5GHz を優先させる場合は「バンドステアリング」にもチェックを入れます。
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。 ・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。
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-IP-address（オプション）	NAS-IP-address（Network access server IP address ）は、RADIUS アクセス要求元への通知に使用され、RADIUS サーバがその要求に対するポリシーを選択できるようにします。

項目	説明
ブリッジするインターフェイス	SSID を VLAN と紐づける場合、本プルダウンメニューから選択します。
スケジュールポリシー	SSID を有効にするスケジュールを指定します。 「スケジュールポリシーの追加」からスケジュールを追加できます。
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 の範囲で指定できます。
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）の範囲で指定します。 「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。
Bonjour パケットフォワーディング	クライアントからの Bonjour パケットフォワーディングの有効 / 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。
RTS 閾値	送信者による RTS プロトコルを使用の際のフレームサイズ（RTS のしきい値）を指定します。主に隠れ端末問題などを解決します。256 - 2347（bytes）から指定できます。
フラグメンテーションしきい値	パケット分割しきい値を設定します。257-2346（bytes）から指定できます。
強制ローミング	有効にすると、DBG-X1000 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 DBG-X1000 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デバイス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 DBG-X1000 への接続を試みた場合に、クライアントと DBG-X1000 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する接続要求回数」で行います。
弱い RSSI 値のクライアントを 許可する接続要求回数	信号強度の弱いクライアントが DBG-X1000 への接続を試みる回数を指定します。 1 - 10（回）の範囲で指定します。

注意 SSID のセキュリティに WPA を使用し、かつ、その認証方式に RADIUS を選択した場合、RADIUS Request を送信する送信元 IP として「ブリッジするインターフェイス」で設定した IP アドレスを使用します。

注意 SSID におけるダイナミック VLAN は未サポートです。

■ セキュリティモード設定

セキュリティに「WPA2」「WPA/WPA2」「WPA3」「WPA2/WPA3」のいずれかを選択した場合、以下の項目が表示されます。
「Open」「Enhanced Open」「Enhanced Open + Open」のいずれかを選択した場合、以下の設定は行いません。

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「PSK」「SAE」「RADIUS」から選択します。 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。「セキュリティ」に「WPA2/WPA3」を選択している場合は、「PSK/SAE」が自動的に選択され、変更できません。 **注意** SSID のセキュリティに WPA を使用し、かつ、その認証方式に RADIUS を選択した場合、RADIUS Request を送信する送信元 IP として「ブリッジするインターフェイス」で設定した IP アドレスを使用します。 **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」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設定します。 - 「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」「アクセスレベル」 **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、MAC フィルタリングのみで有効です。 ・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。

ネットワーク - ワイヤレス - 無線

図 9-24　無線

本画面には以下の項目が含まれます。

項目	説明
無線	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。 • 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」
チャネル帯域	チャネル帯域を選択します。 • 2.4GHz -「20MHz」「20/40MHz(Auto)」 • 5GHz -「20MHz」「20/40MHz(Auto)」「20/40/80MHz(Auto)」
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。
オートチャネル	オートチャネルの有効 / 無効を切り替えます。 オートチャネルを無効にすると、各帯域（2.4GHz と 5GHz）にチャ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ネルを手動で選択します。
チャネル	オートチャネルを「無効」に設定した場合に手動でチャネルを選択します。
有効チャネル	オートチャネル機能で利用するチャネルを選択します。デフォルトでは、全てのチャネルが選択された状態となっています。 オートチャネルで利用するチャネルは「青地に白色の文字」、利用しないチャネルは「白地に黒色の文字」で表示されます。チャネルの数字をクリックすることにより、使用の有無を切り替えることができます。
サイト	サイトを表示します。プロファイル画面では本項目は表示されません。
強制オートチャネルスキャン	オートチャネルを強制的に実行する機能の有効 / 無効を設定します。 有効にすると、クライアントが DBG-X1000 に接続している場合でもオートチャネルが実行されます。ただし、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。

項目	説明
オートチャネル実行	本システムがオートチャネル有効の状態で動作している状態で「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。
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）におけるビーコンが送信される頻度を設定します。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する間隔です。DTIM インターバルで設定したビーコンの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。
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の有効 / 無効を設定します。 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）が短くなります。結果、データの送信時間が短縮されますが、データの干渉が起こりやすくなります。無効にすることで通信が安定する場合があります。
U-APSD	U-APSD の有効 / 無効を設定します。 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。
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、画面上部の「適用」をクリックします。

注意 DFS 検知により使用可能なチャネルがないと判断された場合は、30 分間停波します。

ネットワーク - アドレッシング

- 画面の表示手順（デバイス設定時）：**設定** > **ゲートウェイ** > **デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**アドレッシング**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定** > **ゲートウェイ** > **プロファイル** 画面で「ネットワーク」を選択 →「**アドレッシング**」タブを選択

アドレッシングでは、VLAN や IP プールの設定を行います。

本画面には以下の項目が表示されます。

図 9-25　アドレッシング

設定内容については以下を参照してください。
「ネットワーク - アドレッシング - VLAN 設定」
「ネットワーク - アドレッシング - IP 管理リスト」

設定後、画面上部の「適用」をクリックします。

ネットワーク - アドレッシング - VLAN 設定

本製品の LAN ポート（1 ～ 4）には、IP アドレス「192.168.10.1」が割り当てられています。
初期値では、本製品は LAN インターフェイスでタグなしのトラフィックのみを受け入れます。よって、タグ付きのトラフィックに対して、ユーザは VLAN を明示的に追加する必要があります。

次の画面は、VLAN の設定内容を表示します。また、設定の編集、削除、追加を実行できます。

図 9-26　VLAN 設定

■ VLAN プロファイルの追加

VLAN の設定をします。「追加」をクリックして VLAN プロファイルの追加ウィンドウを表示し、各項目を入力します。

図 9-27　VLAN プロファイルの追加

本画面には以下の項目が含まれます。

項目	説明
名前	VLAN 名を設定します。
Untagged ポート	Untagged ポートとして VLAN を適用する Ethernet ポートを、LAN1 ～ LAN4 から選択します（複数選択可）。
VLAN ID	VLAN ID を設定します。
Tagged ポート	Tagged ポートとして VLAN を適用する Ethernet ポートを、LAN1 ～ LAN4 から選択します（複数選択可）。
InterVLAN	VLAN ネットワーク間の通信を許可するかどうかを、有効 / 無効で設定します。 本項目で「有効」を選択した場合、InterVLAN の設定が同様に「有効」となっている VLAN との通信が可能になります。 **注意**　「セキュリティ」タブの「ファイアウォール」タブで設定したファイアウォールルールと、VLAN プロファイルの設定内容が相違する場合、ファイアウォールルールの設定内容が優先されます。
ブリッジするインターフェイス	ブリッジするインターフェイスを「None」「L2TPv3 Client」から選択します。 本項目はプロファイル設定画面では表示されません。 **注意**　L2TPv3 クライアント、および L2TPv3 サーバは未サポートです。
VLAN サブネット	
プロトコル	「ブリッジするインターフェイス」で「L2TPv3 Client」を選択した場合、プロトコルを「None」「スタティック IPv4」「DHCPv4」から選択します。 • 「None」を選択した場合： プロトコルを使用しません。 • 「スタティック IPv4」を選択した場合： 「IP アドレス」「サブネットマスク」「Gateway IP address（オプション）」「RADIUS ゲートウェイ IP アドレス」を入力します。 • 「DHCPv4」を選択した場合： 「RADIUS ゲートウェイ IP アドレス」を入力します。 **注意**　L2TPv3 クライアント、および L2TPv3 サーバは未サポートです。
IP アドレス	VLAN の IP アドレスを入力します。
サブネットマスク	VLAN のサブネットマスクを入力します。

項目	説明
DHCP モード	DHCP モードを以下から選択します。 • 「None」：DHCP がオフになります。 • 「DHCP サーバ」：ゲートウェイがネットワーク上の DHCP サーバとして機能します。 DHCP サーバを選択した場合は、ドメイン名、DNS プロキシなどの設定を行います。 詳細は「DHCP サーバの設定」を参照してください。 • 「DHCP リレー」：ネットワーク上の DHCP クライアントは、別のサブネット上の DHCP サーバから IP アドレスリースを受信します。DHCP リレーを選択した場合は、「リレーゲートウェイ」にリレーゲートウェイの IP アドレスを入力します。
RA モード	RA モードを「リレー」「サーバ」から選択します。
NDP プロキシ	NDP プロキシを有効 / 無効に設定します。
DHCPv6 モード	DHCPv6 モードを「DHCPv6 リレー」「DHCPv6 サーバ」「無効」から選択します。
IPv6 アサインメント	DHCPv6 モードを「DHCPv6 サーバ」に設定した場合、IPv6 割り当てを有効 / 無効に設定します。 有効にした場合は、IPv6 割り当ての設定を行います。IPv6 割り当ての設定については「IPv6 割り当ての設定」を参照してください。 無効にした場合は、IPv6 アドレスを入力します。
IPv6 自動設定サービス	IPv6 自動設定のサービスを「SLAAC+ ステートレス DHCPv6」「DHCPv6（ステートフル）」「SLAAC+RDNSS」「無効」から選択します。
キャプティブポータル	キャプティブポータルの有効 / 無効を設定します。有効にした場合、キャプティブポータルを選択します。 キャプティブポータルの設定については「ネットワーク - キャプティブポータル」を参照してください。
LAN からの ping を許可	有効にした場合、LAN からの Ping を許可します。

設定後、「保存」をクリックします。

● DHCP サーバの設定

「DHCP モード」で「DHCP サーバ」を選択した場合の設定項目について説明します。

図 9-28　DHCP サーバの設定

項目	説明
ドメイン名	ドメイン名を入力します。
割り当て先頭アドレス	割り当てる IP アドレス範囲の先頭 IP アドレスを入力します。
割り当て末端アドレス	割り当てる IP アドレス範囲の末端 IP アドレスを入力します。
デフォルトゲートウェイ	デフォルトゲートウェイを入力します。
リースタイム (分)	IP アドレスがクライアントにリースされる（割り当てられる）期間（単位：分）を入力します。
DNS プロキシ	DNS リクエストに対しプロキシとして機能させ、ISP の DNS サーバと通信するかどうかを有効 / 無効で指定します。
DNS プライベートアドレスルックアップフィルタ	プライベート IP 範囲のルックアップにフィルタをかけるかどうかを有効 / 無効で指定します。 有効にすると、プライベート IP 範囲のルックアップを拒否します。
DNS サーバ	DNS サーバを「DNS from ISP」「Static DNS」から選択します。 「Static DNS」を選択した場合は手動で DNS サーバを指定します。

● IPv6 割り当ての設定

「IPv6 アサインメント」を有効にした場合の設定項目について説明します。

図 9-29　IPv6 アサインメント

項目	説明
IPv6 アサインメントプレフィックス長	IPv6 割り当てのプレフィックス長を入力します。
IPv6 アサインメントヒント	IPv6 割り当てのヒントを入力します。
IPv6 サフィックス	IPv6 サフィックスの設定方法を「EUI-64」「ランダム」「Manual」から選択します。
手動サフィックス (オプション)	本項目は「Manual」を選択した場合のみ表示されます。サフィックスを手動で入力します。

ネットワーク - アドレッシング - IP 管理リスト

IP 管理リストでは、IP プールの設定を行います。

ゲートウェイの DHCP サーバは、クライアントの MAC アドレスと IP アドレスを DHCP サーバのデータベースに追加することで、ネットワーク上のクライアントに IP 設定を割り当てます。ゲートウェイがクライアントから DHCP 要求を受信すると、そのクライアントの MAC アドレスがデータベース内の MAC アドレスリストと比較され、対応する IP アドレスがクライアントに割り当てられます。

また、本画面では IP-MAC バインディングの設定が可能です。IP-MAC バインディングは、IP アドレスと MAC アドレスの組み合わせを登録し、登録内容と一致した場合にアウトバウンドトラフィック（LAN から WAN へのトラフィック）を許可します。
トラフィックの「送信元 IP アドレス」と「送信元 MAC アドレス」が登録された内容と一致していない場合、パケットはドロップされます。

次の画面は IP 管理リストの設定内容を表示します。また、設定の編集、削除、追加を実行できます。

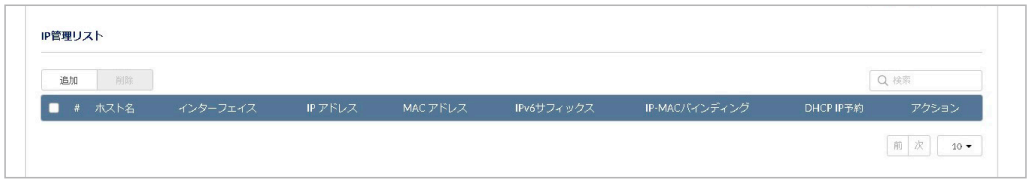


図 9-30　IP 管理リスト

■ IP プール構成の追加

「追加」をクリックし、次の画面で IP プールを設定します。

図 9-31　IP プール構成の追加

本画面には以下の項目が含まれます。

項目	説明
ホスト名	IP アドレスと MAC アドレスのペアを設定するホスト名を入力します。 **注意** ホスト名には、半角英数字と記号「-」「.」のみを使用することができます。
インターフェイス	インターフェイスを選択します。
IP アドレス	割り当てる IP アドレスを入力します。 **注意** 入力する IP アドレスは、選択したインターフェイスの「DHCP モード」設定の開始 / 終了 IP アドレス（「割り当て先頭アドレス」「割り当て末端アドレス」）と同じ範囲内にある必要があります。
MAC アドレス	LAN に接続可能なホストの MAC アドレス（xx:xx:xx:xx:xx:xx 形式）を入力します。 IP アドレスを予約する必要があります。
IPv6 サフィックス (オプション)	IPv6 サフィックスを入力します。本項目はオプションです。
IP-MAC バインディング	IP/MAC バインディングを有効 / 無効に設定します。 有効にすると、ホストの情報が IP/MAC バインディングに関連付けられます。
DHCP IP 予約	DHCP サーバの IP アドレス予約を有効 / 無効に設定します。

設定後、「保存」をクリックします。

ネットワーク - ルーティング

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**ルーティング**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「ネットワーク」を選択 →「**ルーティング**」タブを選択

以下ではルーティングの設定について説明します。
ルーティングの設定により、異なるネットワークにパケットを送信するときに、最適な経路で送信することができます。

本製品は、スタティックルート、ポリシールートをサポートしています。

- スタティックルート：手動で設定した経路を使用します。何らかの変更が発生した場合は経路を手動で再設定します。
- ポリシールート：送信元 / 宛先ネットワーク、送信元 / 宛先ポートなど、特定のパラメータに基づいてルーティングポリシーを設定します。
- RIP※（Routing Information Protocol）の設定：宛先までの距離（ホップ数）をカウントし、ホップ数が少ない経路を選択します。
- OSPF の設定：ネットワーク情報をネットワーク上のルーターから収集し、ネットワークのトポロジーマップを生成します。

※ RIP は未サポートです。

本画面には以下の項目が表示されます。

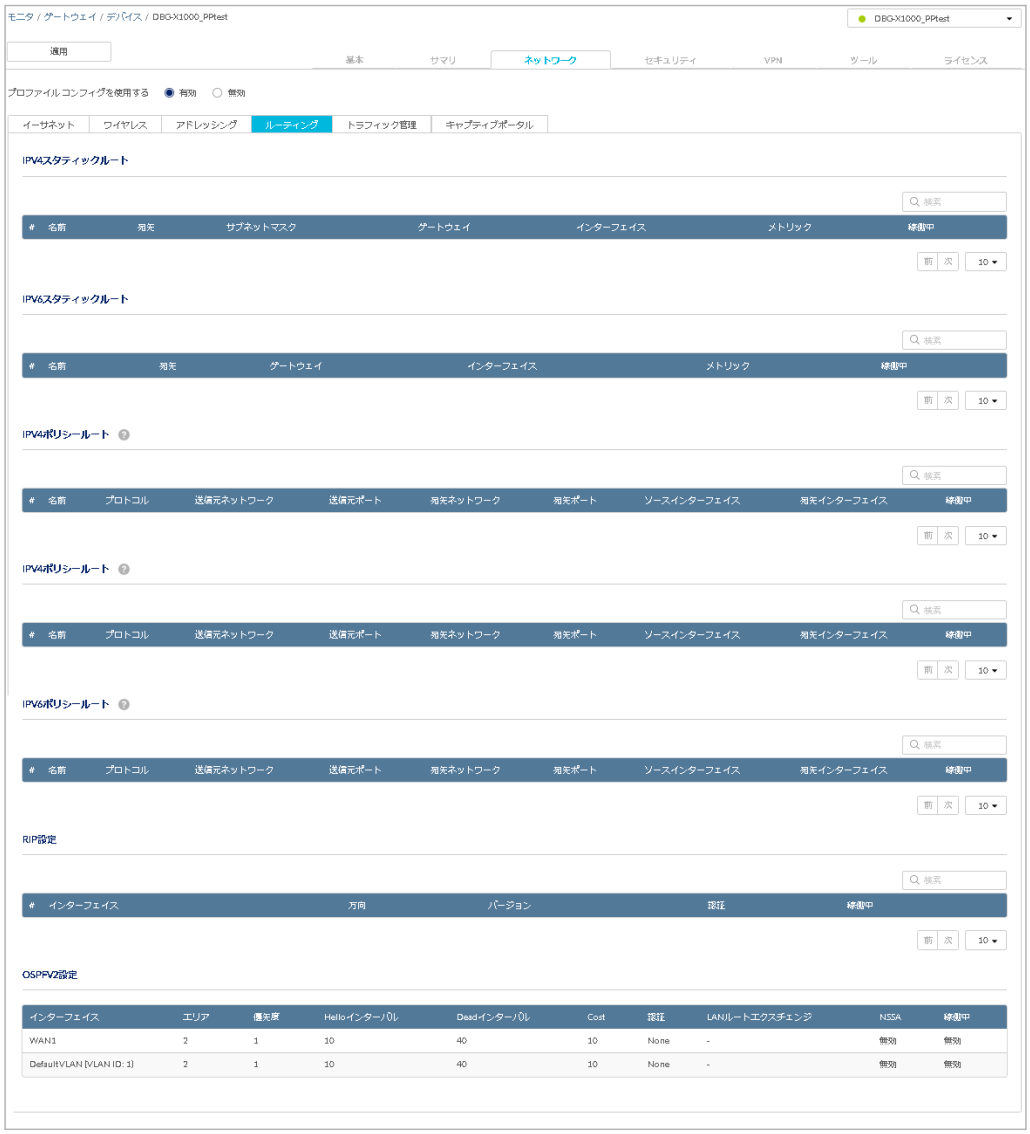


図 9-32　ルーティング

設定内容については、以下を参照してください。

- 「ネットワーク - ルーティング - スタティックルート」
- 「ネットワーク - ルーティング - ポリシールート」
- 「ネットワーク - ルーティング - RIP 設定」
- 「ネットワーク - ルーティング - OSPFV2 設定」

設定後、画面上部の「適用」をクリックします。

ネットワーク - ルーティング - スタティックルート

スタティックルートでは、異なるネットワークへパケットを送信する際の経路を手動で設定します。
設定したスタティックルート以外の経路でパケットを送信することはありません。スタティックルートの設定を完了すると、その経路がアクティブになり、ネットワークが変更されるまで使用されます。

次の画面はスタティックルートの設定内容を表示します。また、設定の編集、削除、追加を実行できます。
「稼働中」では各ルートの有効 / 無効を設定できます。

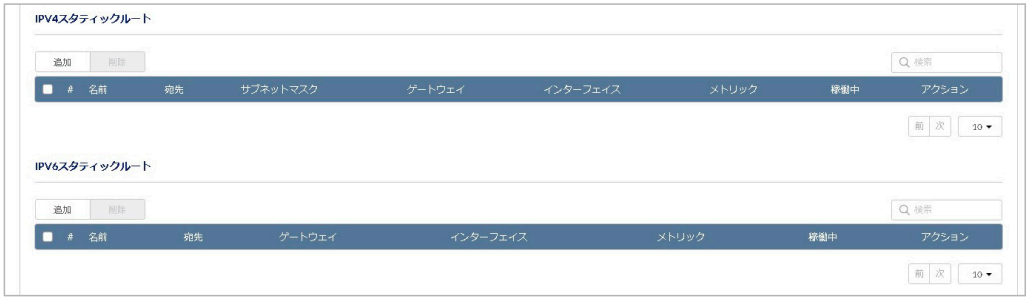


図 9-33　スタティックルート

■ IPv4 スタティックルートの追加

「IPV4 スタティックルート」で「追加」をクリックし、次の画面でスタティックルートを設定します。

図 9-34　IPv4 スタティックルートの追加

本画面には以下の項目が含まれます。

項目	説明
名前	スタティックルートの名前を設定します。
宛先 IP アドレス	スタティックルートの宛先 IPv4 アドレスを設定します。
サブネットマスク	スタティックルートのサブネットマスクを設定します。
ゲートウェイ IP アドレス	スタティックルートのゲートウェイ IPv4 アドレスを設定します。
インターフェイス	このルートにアクセスできる物理ネットワークインターフェイスを選択します。
メトリック	メトリック（2 ～ 15）を設定します。メトリックは、ルートの優先順位を決定します。 同じ宛先へのルートが複数存在する場合は、メトリックが最も小さいルートが選択されます。
プライベート	ルートをプライベートにするには、本項目を有効にします。

設定後、「保存」をクリックします。

■ IPv6 スタティックルートの追加

「IPV6 スタティックルート」で「追加」をクリックし、次の画面でスタティックルートを設定します。

図 9-35　IPv6 スタティックルートの追加

本画面には以下の項目が含まれます。

項目	説明
名前	スタティックルートの名前を設定します。
宛先 IP アドレス	スタティックルートの宛先 IPv6 アドレスを設定します。
IPv6 ゲートウェイ	スタティックルートのゲートウェイ IPv6 アドレスを設定します。
インターフェイス	このルートにアクセスできる物理ネットワークインターフェイスを選択します。
メトリック	メトリック（2 ～ 15）を設定します。メトリックは、ルートの優先順位を決定します。 同じ宛先へのルートが複数存在する場合は、メトリックが最も小さいルートが選択されます。

設定後、「保存」をクリックします。

ネットワーク - ルーティング - ポリシールート

ポリシールートでは、送信元 / 宛先ネットワーク、送信元 / 宛先ポートなどの情報を基に経路を決定し、パケットを送信します。
この機能を使用すると、特定の WAN リンクにサービスを割り当てて、優先度の高いサービスがより信頼性の高い、またはより安価な ISP に送信されるようにすることができます。

次の画面はポリシールートの設定内容を表示します。また、設定の編集、削除、追加を実行できます。
「稼働中」では各ルートの有効 / 無効を設定できます。

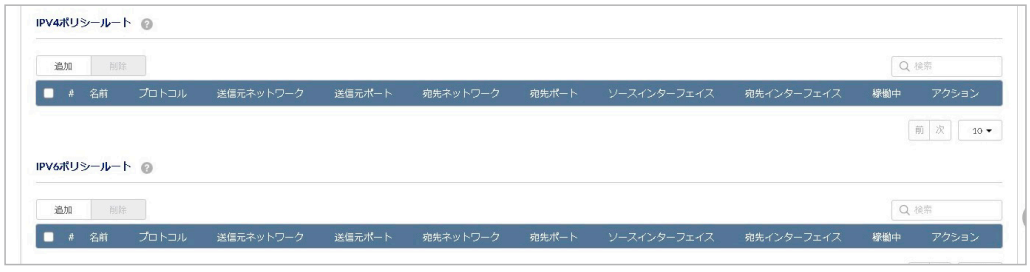


図 9-36　ポリシールート

■ IPv4 ポリシールートの追加

「IPV4 ポリシールート」で「追加」をクリックし、次の画面でポリシールートを設定します。

図 9-37　IPv4 ポリシールートの追加

本画面には以下の項目が含まれます。

項目	説明
名前	ポリシールートの名前を設定します。
ソースインターフェイス	送信元インターフェイスを選択します。
プロトコル	トランスポート層のプロトコルを選択します。
宛先インターフェイス	このルートにアクセスできる物理ネットワークインターフェイスを選択します。
送信元ネットワーク	送信元ネットワークの IP アドレス、IP アドレス範囲を入力します。 IP アドレス範囲を入力する場合は、ハイフンを使用して入力します。（例：192.168.200.101-192.168.200.120） 複数の IP アドレスはカンマ「,」で区切って入力します。（例：192.168.200.101,192.168.200.200） すべての送信元ネットワークを指定する場合は「Any」と入力します。
送信元ポート	送信元ポート番号（1-65535）を入力します。 ポート範囲を入力する場合は、ハイフンを使用して入力します。（例：1-65535） 複数のポートはカンマ「,」で区切って入力します。（例：80,81） すべてのポートを指定する場合は「Any」と入力します。 プロトコルに「Any」「ICMP」を選択した場合、本項目は表示されません。
宛先ネットワーク	宛先ネットワークの IP アドレス、IP アドレス範囲を入力します。 IP アドレス範囲を入力する場合は、ハイフンを使用して入力します。（例：192.168.200.101-192.168.200.120） 複数の IP アドレスはカンマ「,」で区切って入力します。（例：192.168.200.101,192.168.200.200） すべての宛先ネットワークを指定する場合は「Any」と入力します。
宛先ポート	宛先ポート番号（1-65535）を入力します。 ポート範囲を入力する場合は、ハイフンを使用して入力します。（例：1-65535） 複数のポートはカンマ「,」で区切って入力します。（例：80,81） すべてのポートを指定する場合は「Any」と入力します。 プロトコルに「Any」「ICMP」を選択した場合、本項目は表示されません。

設定後、「保存」をクリックします。

■ IPv6 ポリシールートの追加

「IPV6 ポリシールート」で「追加」をクリックし、次の画面でポリシールートを設定します。

図 9-38　IPv6 ポリシールートの追加

本画面には以下の項目が含まれます。

項目	説明
名前	ポリシールートの名前を設定します。
ソースインターフェイス	送信元インターフェイスを選択します。
プロトコル	トランスポート層のプロトコルを選択します。
宛先インターフェイス	このルートにアクセスできる物理ネットワークインターフェイスを選択します。
送信元ネットワーク	送信元ネットワークの IPv6 アドレス、IPv6 アドレス範囲を入力します。 IPv6 アドレス範囲を入力する場合はハイフンを使用して入力します。（例：2001:db8:abcd:64::1234-2001:db8:abcd:64::5678） 複数の IPv6 アドレスはカンマ「,」で区切って入力します。（例：2001:db8:abcd:64::1234,2001:db8:abcd:64::5678） IPv6 アドレスのプレフィックスを入力できます。（例：2001:db8:abcd:64::/64） すべての送信元ネットワークを指定する場合は「Any」と入力します。
送信元ポート	送信元ポート番号（1-65535）を入力します。 ポート範囲を入力する場合は、ハイフンを使用して入力します。（例：1-65535） 複数のポートはカンマ「,」で区切って入力します。（例：80,81） すべてのポートを指定する場合は「Any」と入力します。 プロトコルに「Any」「ICMP」を選択した場合、本項目は表示されません。
宛先ネットワーク	宛先ネットワークの IP アドレス、IP アドレス範囲を入力します。 IPv6 アドレス範囲を入力する場合はハイフンを使用して入力します。（例：2001:db8:abcd:64::1234-2001:db8:abcd:64::5678） 複数の IPv6 アドレスはカンマ「,」で区切って入力します。（例：2001:db8:abcd:64::1234,2001:db8:abcd:64::5678） すべての宛先ネットワークを指定する場合は「Any」と入力します。
宛先ポート	宛先ポート番号（1-65535）を入力します。 ポート範囲を入力する場合は、ハイフンを使用して入力します。（例：1-65535） 複数のポートはカンマ「,」で区切って入力します。（例：80,81） すべてのポートを指定する場合は「Any」と入力します。 プロトコルに「Any」「ICMP」を選択した場合、本項目は表示されません。

設定後、「保存」をクリックします。

ネットワーク - ルーティング - RIP 設定

RIP（Routing Information Protocol）は、ダイナミックルーティングに使用するプロトコルです。
宛先までの距離（ホップ数）をカウントし、ホップ数が少ない経路を選択します。

注意　本機能は未サポートです。

以下の画面は RIP の設定内容を表示します。また、設定の編集、削除、追加を実行できます。
「稼働中」では本項目の有効 / 無効を設定できます。

図 9-39　RIP 設定

■ RIP 設定の追加

「追加」をクリックします。表示される「追加 RIP 設定」画面で RIP を設定します。

図 9-40　「追加 RIP 設定」画面

本画面には以下の項目が含まれます。

項目	説明
インターフェイス	RIP を設定するインターフェイスを選択します。
方向	本製品が RIP パケットを送受信する方法を以下から選択します。 • 「In のみ」：本製品は他のルータからの RIP 情報を受け入れますが、ルーティングテーブルのブロードキャストは行いません。 • 「両方」：本製品はルーティングテーブルをブロードキャストし、他のルータから受信した RIP 情報の処理も行います。RIP 機能を完全に利用するには、「両方」に設定することを推奨します。
バージョン	RIP のバージョンを「RIP-1」「RIP-2M」から選択します。 • 「RIP-1」：サブネット情報を含んでいないクラスベースのルーティングバージョンです。これは最も一般的にサポートされるバージョンです。 • 「RIP-2M」：RIPv1 のすべての機能に加え、サブネット情報をサポートします。ルーティング情報を送る際、マルチキャストアドレスを使って送信します。
認証	認証の有効 / 無効を設定します。初期値は無効です。 本項目はバージョンを「RIP-2M」に設定した場合のみ表示されます。
MD5 キー ID	認証を有効にした場合、MD5 キー ID を入力します。
MD5 認証キー	認証を有効にした場合、MD5 認証キー ID を入力します。

設定後、「保存」をクリックします。

ネットワーク - ルーティング - OSPFV2 設定

OSPFv2 は、内部ゲートウェイプロトコル（IGP）の一つです。OSPFv2 を使用することで、より通信速度の早い経路での通信が可能となります。

ルーティングに OSPFv2 を選択した場合、インターネットプロトコル（IP）パケットの転送経路が、ネットワーク領域の内部で独自に確立されます。まず、ネットワーク領域内に存在する各ルータからリンク状態に関する情報が収集され、その情報をもとにネットワーク全体のトポロジーマップが生成されます。このトポロジーマップを参考にパケットの転送経路が決定されます。

「OSPFV2 設定」欄には、次の画面の内容が表示されます。
「稼働中」欄では、インターフェイスごとに OSPFV2 設定の有効 / 無効を指定できます。また、「アクション」欄から OSPFV2 設定の内容を編集できます。

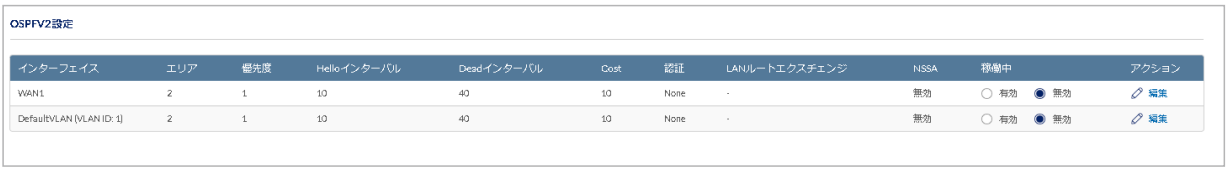


図 9-41　OSPFV2 設定

「OSPFV2 設定」欄に含まれる項目は、以下の通りです。

項目	説明
インターフェイス	OSPFv2 が有効または無効に設定されている、物理ネットワークインターフェイスを表示します。
エリア	インターフェイスが属するエリアを表示します。
優先度	代表ルータ（Designated Router: DR）となる際の、ルータ内での優先度を表示します。
Hello インターバル	Hello パケットを送信する間隔を秒数で表示します。
Dead インターバル	前回の Hello パケットの受信から、本項目で設定した時間（秒）が経過するまでの間 Hello パケットの受信がなかった場合に、その OSPF 隣接ルータはダウンしていると判断されます。
Cost	OSPFv2 インターフェイスへパケットを送信する際のコストを表示します。
認証	認証の種類を表示します。
LAN ルートエクスチェンジ	WAN インターフェイスの LAN ルートエクスチェンジの状態を表示します。
NSSA	OSPF の特殊エリア、Not-So-Stubby Area（NSSA）の有効 / 無効を表示します。
稼働中	各インターフェイスの有効 / 無効を指定できます。
アクション	OSPFv2 の設定を編集できます。

OSPFv2 の設定を編集するには、「編集」をクリックします。表示される次の「編集 OSPFv2」画面から OSPFv2 の設定を編集します。

注意　OSPF におけるルート再配布の対象は kernel、connected、および static に既定されています。
PPPoE、MAP-E などの PPP Interface については、自身の IP Address ではなく Peer の IP Address を広告します。

図 9-42　「編集 OSPFv2」画面

本画面では、以下の項目を設定します。

項目	説明
インターフェイス	OSPFv2 が有効または無効に設定されている、物理ネットワークインターフェイスを表示します。 補足： • L2TP over IPsec インターフェイスの場合は、以下を設定します。 - Nuclias Cloud で、**モニタ** > **ゲートウェイ** > **デバイス**の順にクリックし、「VPN」タブ>「PPTP/L2TP」タブの「サーバモード」欄または「クライアントモード」欄で「追加」をクリックします。 - 表示される画面の「サーバタイプ」または「クライアントタイプ」に「L2TP」を選択し、L2TP over IPsec を有効にします。L2TP over IPsec をサーバ側とクライアント側に設定します。 - 設定を保存します。詳細は「VPN - PPTP/L2TP」を参照してください。
NSSA	OSPF の特殊エリアに外部経路を採用する場合、本項目を有効に設定します。
エリア	インターフェイスが属するエリアを入力します。 2 つのルータ間でセグメントが共通の場合： 両ルータのインターフェイスは、同一セグメント内の同一エリアに属している必要があります。また、両インターフェイスは同じサブネットに属し、また、類似したサブネットマスクを持つ必要があります。
優先度	本項目を設定することで、ネットワークの代表となる OSPFv2 ゲートウェイを選択する手助けをします。 優先度の最も高いゲートウェイが、代表ルータ（DR）として最適であると判断されます。 初期値は「1」に設定されています。設定する値が小さいほど、優先度は高まります。 本項目に設定した値が小さいルータほど、代表ルータとなる可能性が高まります。 本項目に「0」を設定したルータは、代表ルータとなるには不適切であると判断されます。
Hello インターバル	Hello パケットを送信する間隔を秒数で表示します。同一のネットワーク内では、全てのゲートウェイに対して同じ値を本項目に設定します。 初期値は「10（秒）」に設定されています。
Dead インターバル	隣接ルータがダウンしていると判断する際の基準となる、前回の Hello パケットの受信からの経過時間を秒数で入力します。 本項目で設定した時間（秒）Hello パケットの受信がなかった場合に、その OSPF 隣接ルータはダウンしていると判断されます。 初期値は「40（秒）」に設定されています。OSPF を使用する場合、同一ネットワーク内に属する隣接ルータでは、本項目に同じ値を入力する必要があります。本項目に入力した値がルータ間で異なる場合、特定のセグメントにおいて両ルータは隣接ルータにはなりえません。
Cost	OSPFv2 インターフェイスへパケットを送信する際のコストを入力します。
認証タイプ	認証の種類を、プルダウンメニューから選択します。 •「None」：インターフェイスは OSPF パケットの認証を行いません。 •「Simple」：シンプルテキストのキーを使用して、OSPF パケットの認証を行います。 •「MD5」：MD5 認証を使用して、OSPF パケットの認証を行います。
認証キー	本項目は、「認証タイプ」で「Simple」を選択した場合に表示されます。 認証キーとして使用する文字列を、1 ～ 8 文字の範囲で入力します。
MD5 キー ID	本項目は、「認証タイプ」で「MD5」を選択した場合に表示されます。 使用する MD5 キー ID を 1 ～ 255 文字の範囲で入力します。
MD5 認証キー	本項目は、「認証タイプ」で「MD5」を選択した場合に表示されます。 使用する MD5 認証キーを 1 ～ 16 文字の範囲で入力します。
LAN ルートエクスチェンジ	WAN インターフェイスの LAN ルートエクスチェンジを有効 / 無効に設定します。

設定後、「保存」をクリックします。

ネットワーク - トラフィック管理

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**トラフィック管理**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「ネットワーク」を選択 →「**トラフィック管理**」タブを選択

トラフィック管理を設定することで、LAN から WAN へのトラフィック量を制限します。そうすることで、優先度の低い LAN ユーザ（ゲストや HTTP サービスなど）が使用可能な WAN 帯域を独占してしまう事態を回避します。結果、他のユーザの通信速度が遅くなる事象を避けることができます。コスト削減および帯域割り当ての優先度を考慮する際に、トラフィック管理は有効です。

以下では、帯域制御の内容、Web UI からのトラフィック管理の設定方法について説明します。

本製品は、トラフィック管理の手段として、帯域幅シェーピングとセッション制限をサポートしています。

注意　「帯域幅シェーピング」は、現在未サポートですが、今後サポート予定です。

- 帯域幅シェーピング
  特定のトラフィックのトラフィック量を制限してパケットの通信を遅延させることで、通信性能を最適化し、通信可能な帯域幅を確保します。
- セッション制限
  ユーザのセッション数を制限し、特定のユーザのみが帯域を独占し、他のユーザの通信速度が遅くなる事象を防ぎます。

「トラフィック管理」タブには、以下の項目が含まれます。

ネットワーク - トラフィック管理 - 帯域幅シェーピング

注意　「帯域幅シェーピング」は、現在未サポートですが、今後サポート予定です。

帯域幅シェーピングの欄には、次の内容が表示されます。また、設定内容の編集、削除、および追加を実行できます。
「稼働中」欄では、設定の有効 / 無効を指定できます。

図 9-43　「トラフィック管理」タブ（帯域幅シェーピング）

■ IPV4 /IPV6 帯域幅シェーピングの追加

「IPV4 帯域幅シェーピング」欄、または「IPV6 帯域幅シェーピング」欄で、「追加」をクリックします。表示される以下の画面で、追加する帯域幅シェーピングの設定を行います。

図 9-44　「帯域幅シェーピングの追加」画面（IPV4 帯域幅シェーピング）

本画面では、以下の項目の設定を行います。

項目	説明
名前	作成する帯域幅シェーピングルールの名前を入力します。
ポリシータイプ	ポリシータイプをプルダウンメニューの「Outbound」または「Inbound」から選択します。
WAN インターフェイス	本項目は「ポリシータイプ」で「Outbound」を選択した場合のみ表示されます。 帯域幅シェーピングのルールを関連付ける、使用可能な WAN インターフェイスをプルダウンメニューより選択します。
インターフェイス	本項目は「ポリシータイプ」で「Inbound」を選択した場合のみ表示されます。 帯域幅シェーピングのルールを関連付ける、使用可能なインターフェイスをプルダウンメニューより選択します
マネジメントタイプ	管理の基準とする種別をプルダウンメニューの「優先度」または「Rate」より選択します。
優先度	「マネジメントタイプ」で「優先度」を選択した場合、本項目で優先度を「高」「中」「低」より選択し、指定します。
最大帯域幅レート（Kbps）	「マネジメントタイプ」で「Rate」を選択した場合、本項目に最大帯域幅レートを入力します。
最小帯域幅レート（Kbps）	「マネジメントタイプ」で「Rate」を選択した場合、本項目に最小帯域幅レートを入力します。
トラフィックセレクター	
サービス	使用するトラフィックセレクターのサービスの種類をプルダウンメニューより選択します。
トラフィックセレクターマッチタイプ	本項目は「ポリシータイプ」で「Outbound」を選択した場合に表示されます。 トラフィックセレクターを何と関連付けるかを、以下より選択します。 • 「IP アドレス」：トラフィックセレクターを LAN 上のデバイスの IP アドレスと関連付けます。 • 「MAC アドレス」：トラフィックセレクターを LAN 上の特定の MAC アドレスと関連付けます。 • 「インターフェイス」：トラフィックセレクターをインターフェイスと関連付けます。
IP アドレス	ポリシータイプで、「Outbound」を選択し、「トラフィックセレクタマッチタイプ」で「IP アドレス」を選択した場合、もしくはポリシータイプで「Inbound」を選択した場合に表示されます。使用する IP アドレスを入力します。
サブネットマスク	IPV4 の帯域幅シェーピングの追加を行う場合に、上記「IP アドレス」と一緒に表示されます。使用するサブネットマスクを入力します。
MAC アドレス	「トラフィックセレクターマッチタイプ」で「MAC アドレス」を選択した場合に表示されます。使用する MAC アドレスを入力します。
インターフェイス	「トラフィックセレクターマッチタイプ」で「インターフェイス」を選択した場合に、使用するインターフェイスをプルダウンメニューより選択します。
スケジュールポリシー	帯域幅シェーピングのルールを適用するスケジュールをプルダウンメニューより選択します。

設定後、「保存」をクリックします。

ネットワーク - トラフィック管理 - セッション制限

セッション制限の欄には、設定したセッション制限のルールが一覧で表示されます。デバイスを通して、IP アドレス、IP アドレス範囲、インターフェイスごとのセッション数を制限できます。

セッション制限で設定した制限に到達すると、ウェブブラウザより開始されたセッションにおいて、ユーザへの警告メッセージが表示されます。

セッション制限の設定では、セッション制限の名前、送信元タイプ、スケジュール、および最大セッション数を設定します。また、設定内容の編集、削除、および追加を実行できます。

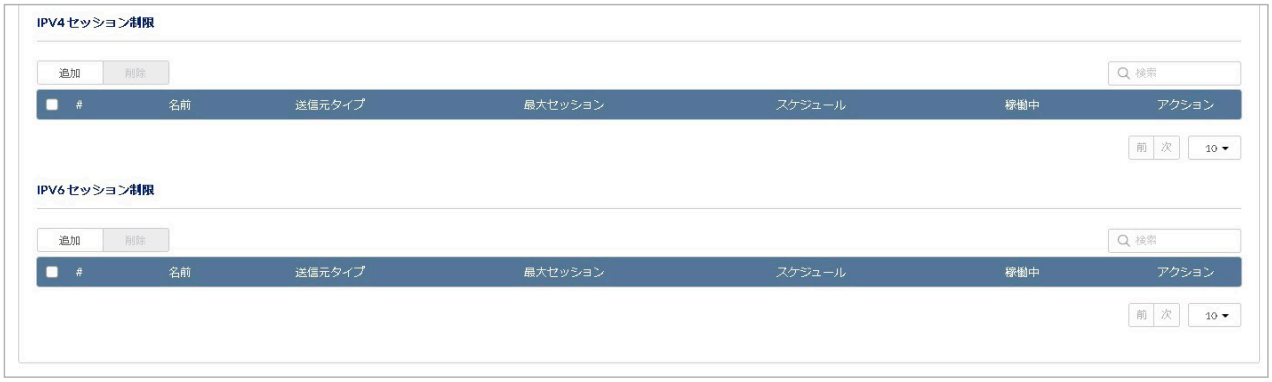


図 9-45　「トラフィック管理」タブ（セッション制限）

セッション制限の欄に含まれる項目は以下の通りです。

項目	説明
名前	特定の送信元タイプに対し設定されたセッション制限ルールの名前を表示します。
送信元タイプ	セッション制限ルールに選択されている送信元の種類を表示します。
最大セッション	セッション数を制限する際に使用する、選択された送信元タイプにおいて許容されるセッションの最大数を表示します。
スケジュール	設定されている、セッション制限ルールを実行するスケジュールを表示します。
稼働中	セッション制限ルールの有効 / 無効を選択できます。
アクション	セッション制限の内容の編集、および削除を行います。

■ IPV4 / IPV6 セッション制限の追加

「IPV4 セッション制限」欄、または「IPV6 セッション制限」欄から、セッション制限の一覧へルールを追加するには、「追加」をクリックします。表示される以下の「セッション制限の追加」画面で、追加するセッション制限のルールを設定します。ルールの一覧より複数のルールを同時に削除するには、削除するルールの左側に表示されているチェックボックスをチェックした後、「削除」をクリックします。

図 9-46　「セッション制限の追加」画面（IPV4 セッション制限）

本画面では、以下の項目の設定を行います。

項目	説明
名前	特定の送信元タイプに対し設定するセッション制限ルールの名前を入力します。
送信元タイプ	送信元の種類をプルダウンメニューの「IP アドレス」「IP レンジ」「インターフェイス」より選択します。 注意　「IP レンジ」は IPV4 のセッション制限を追加する場合のみプルダウンメニューに表示されます。
IP アドレス	「送信元タイプ」で「IP アドレス」を選択した場合に、セッション制限のルールで制御するクライアント / ホストの IP アドレスを入力します。
先頭 IP アドレス	本項目は「送信元タイプ」で「IP レンジ」を選択した場合に表示されます。 セッション制限のルールで制御するクライアント / ホストの IP アドレスの範囲のうち、先頭となる IP アドレスを入力します。
割り当て末端アドレス	本項目は「送信元タイプ」で「IP レンジ」を選択した場合に表示されます。 セッション制限のルールで制御するクライアント / ホストの IP アドレスの範囲のうち、末尾となる IP アドレスを入力します。
インターフェイス	本項目は「送信元タイプ」で「インターフェイス」を選択した場合に表示されます。 セッション制限のルールで制御するネットワークをプルダウンメニューより選択します。
最大セッション	セッションの数を制限するため、対象となる送信元タイプで許容されるセッション数の上限となる数を入力します。
スケジュールポリシー	セッション制限のルールを適用するスケジュールを指定します。プルダウンメニューの設定済みスケジュールより選択します。

設定後、「保存」をクリックします。

ネットワーク - キャプティブポータル

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**ネットワーク**」タブ >「**キャプティブポータル**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定** > **ゲートウェイ > プロファイル** 画面で「ネットワーク」を選択 →「**キャプティブポータル**」タブを選択

注意 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）の場合にスプラッシュページへ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。

以下ではキャプティブポータルの設定について説明します。

キャプティブポータルは、別名「スプラッシュページ」とも呼ばれます。認証されていないユーザがインターネットにアクセスしようとしたときに表示される Web ページです。

キャプティブポータルが設定されている場合、ユーザは認証された後、インターネットへのアクセスのみが許可されます。
ログイン資格情報を入力するか、サービス条件に同意することによって認証されます。キャプティブポータルは、インターネットの使用状況を監視および制御する際に役立ちます。

本製品では、ユーザがキャプティブポータルページを設定でき、さまざまな認証方法を提供します。

注意 キャプティブポータルのエンコーディングには UTF-8 を使用します。

本画面にはキャプティブポータルの一覧が表示されます。また、設定の編集、削除、追加を実行できます。

図 9-47　キャプティブポータル

設定内容については「ネットワーク - キャプティブポータル - キャプティブポータルの追加」を参照してください。

設定後、画面上部の「適用」をクリックします。

■ ネットワーク - キャプティブポータル - キャプティブポータルの追加

「追加」をクリックし、キャプティブポータルの設定を追加します。

図 9-48　キャプティブポータルの追加（クリックスルー）

図 9-49　「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。

項目	説明
None	キャプティブポータルを使用しません。
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。

項目	説明
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。 • 「認証サーバ：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。 • 「認証サーバ：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行います。 • 「ローカル認証」：ローカル認証 DB 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、新規サーバを作成することができます。 • 「認証サーバリスト」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。 ● 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、新規サーバを作成することができます。 • 「認証サーバリスト」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** 認証サーバの設定については「認証 - 認証サーバ」を参照してください。
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」「Twitter（現「X」）」から 1 つ以上指定します。全て指定することも可能です。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。右側のプルダウンメニューから定義済みのスプラッシュページを選択することができます。 **注意** SNS 認証機能（Facebook、Google、LINE、Weibo、Twitter（現「X」））を使用する場合、「同時ログイン」項目の設定内容に関わらず同時ログインが有効になります。
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	スプラッシュページ上に、ベーシックログインとサードパーティ資格情報でサインオンの両方の項目が表示されます。認証方式をこれらより選択し、サインオンします。 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。 右側のプルダウンメニューから定義済みのスプラッシュページを選択することができます。 **注意** SNS 認証機能（Facebook、Google、LINE、Weibo、Twitter（現「X」））を使用する場合、「同時ログイン」項目の設定内容に関わらず同時ログインが有効になります。
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、およびサードパーティ資格情報の項目が表示されます。 認証方式をこれらより選択し、サインオンします。 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。 E メール認証ではメールアドレスを入力すると、一時的に上位ネットワークとの通信が可能になりますので、その間に認証用メールを受信し、認証を実施します。 E 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選択します。 • 「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選択します。 • 「拒否時間制限」：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、Twitter（現「X」））を使用する場合、「同時ログイン」項目の設定内容に関わらず同時ログインが有効になります。
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。

■ 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」「セッション制限」「アイドルタイムアウト」の項目では、セッションの時間と数を指定します。

項目	説明
セッションタイムアウト	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。
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。本項目は、「キャプティブポータル」で「クリックスルー」を選択した場合は表示されません。 セッション制限を以下から選択し設定します。 • 選択肢：「無制限」「1」「2」「3」「4」「5」
アイドルタイムアウト	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。なお、セッションタイムアウトより大きな数値を入力した場合は、その数値の半数へ修正された値が自動的に入力されます。

ウォ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
ウォールドガーデン (オプション)	ウォールドガーデンを選択します。 ウォールドガーデンを追加する場合は「ウォ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「ウォールドガーデン」を参照してください。 **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。

URL リダイレクトを行う場合は、以下の設定を行います。
「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「1 回目のリダイレクトのみ」「15 分」「30 分」「60 分」「120 分」「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。

「SSID / VLAN」の項目では、使用する SSID、VLAN を選択します。

項目	説明
SSID / VLAN	使用する SSID、VLAN を選択します。 **注意** DBG-2000 の場合、プロファイル設定画面では「SSID/VLAN」、デバイス設定画面では「VLAN」が表示されます。 **注意** 1 つのキャプティブポータルには複数の SSID / VLAN を割り当てることができます。ただしそれぞれの「SSID」「VLAN」には、最大 1 つのキャプティブポータルしか割り当てられません。 既に他のキャプティブポータルに紐づけられている「SSID」「VLAN」を選択し、保存した場合は、先に紐づけられていたキャプティブポータルの紐づけは解除されます。

設定後、「保存」をクリックします。

「セキュリティ」タブ

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**セキュリティ**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル 画面**で「**セキュリティ**」を選択

本製品のセキュリティ設定について説明します。セキュリティ設定には、以下の項目が含まれます。

- ファイアウォール：
  ファイアウォールルールの設定を行います。
- IPS：
  IPS（Intrusion Prevention System/ 不正侵入防止システム) の設定を行います。
- WEB コンテンツフィルター：
  Web コンテンツフィルタリングの設定を行います。
  指定したカテゴリに属する Web サイトへのアクセスを規制できます。
- アプリケーションコントロール：
  指定した基準により、利用可能な Web アプリケーションを制限します。

注意 デバイス設定画面の「セキュリティ」タブでは、「プロファイル コンフィグを使用する」の有効 / 無効を設定できません。
「ネットワーク」タブの「プロファイル コンフィグを使用する」で設定した内容が「セキュリティ」タブにも反映されます。

参照 設定項目の詳細については以下を参照してください。
「セキュリティ - ファイアウォール」
「セキュリティ - IPS」
「セキュリティ - WEB コンテンツフィルター」
「セキュリティ - アプリケーションコントロール」

セキュリティ - ファイアウォール

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**セキュリティ**」タブ >「**ファイアウォール**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「セキュリティ」を選択 →「**ファイアウォール**」タブを選択

以下では、ファイアウォール設定について説明します。

ファイアウォール設定により、安全なネットワーク環境を維持できます。

- IPV4 ファイアウォールルール
  IPv4 ネットワークでのファイアウォールルールを設定できます。
  ファイアウォールルールを定義し、ネットワークの送受信トラフィックを制限します。

- ポートフォワーディング
  ネットワークに入ってくるトラフィックのアクセスを制限できます。
  特定の外部ユーザのみが特定のローカルリソースへのアクセスが可能となります。

- ポートトリガー
  必要に応じて受信トラフィック用に特定の受信ポートを開放できる機能です。

- IPV6 ファイアウォールルール
  IPv6 ネットワークでのファイアウォールルールを設定できます。
  ファイアウォールルールを定義し、ネットワークの送受信トラフィックを制限します。

本画面には以下の項目が表示されます。

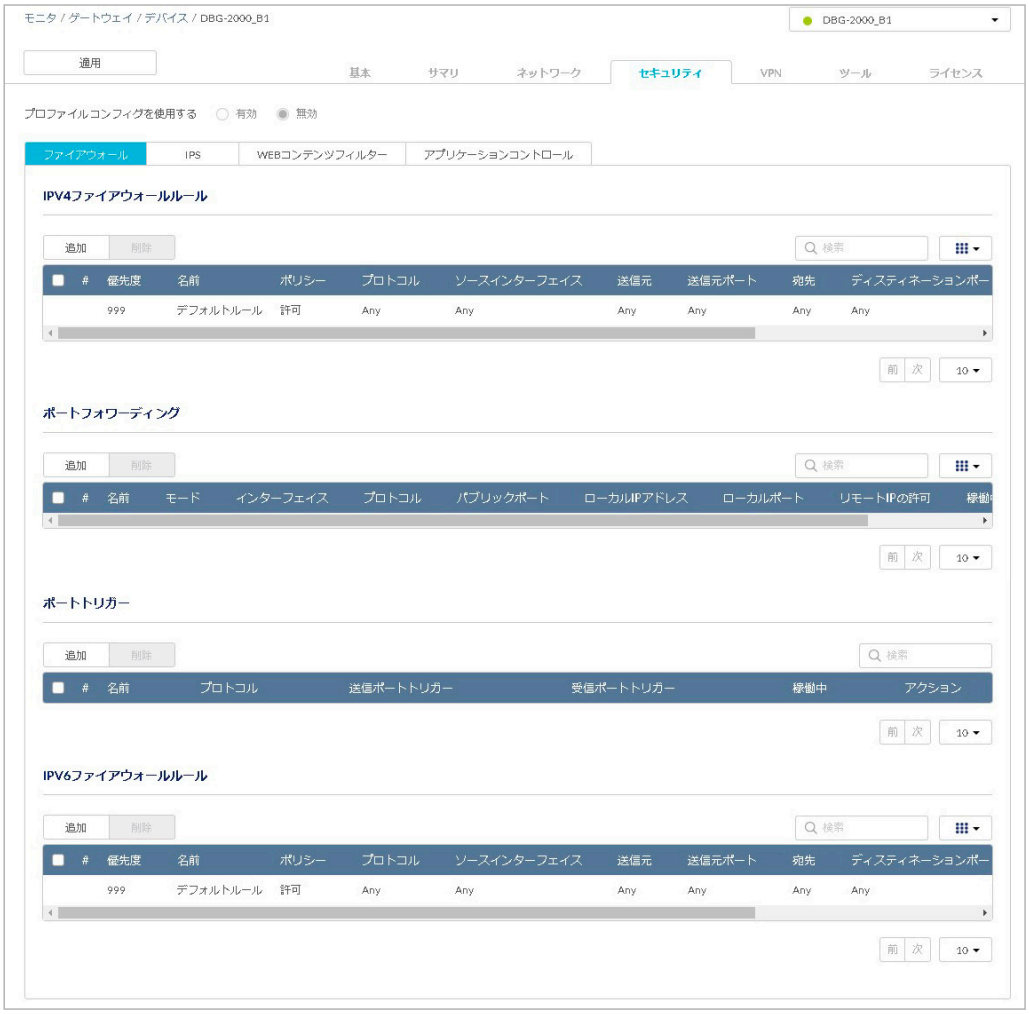


図 9-50　ファイアウォール

設定後、画面上部の「適用」をクリックします。

セキュリティ - ファイアウォール - IPV4 ファイアウォールルール

ファイアウォールルールにより、ネットワークの送受信トラフィックを制限できます。
トラフィックのプロトコル、送信元、宛先を指定し、該当するトラフィックを「許可」または「拒否」するかを指定します。

次の画面に IPV4 ファイアウォールルールの設定が表示されます。また、設定の編集、削除、追加を実行できます。
「稼働中」欄では設定を有効 / 無効にできます。

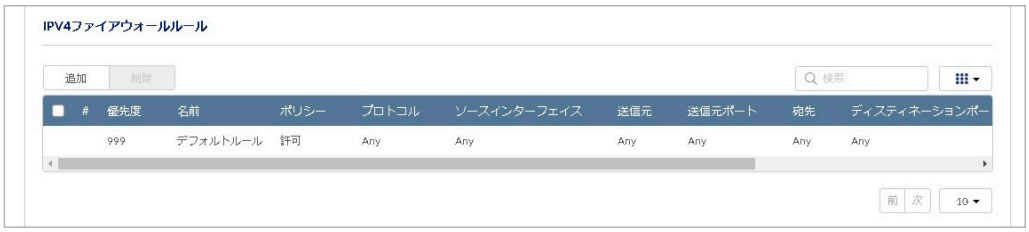


図 9-51　IPV4 ファイアウォールルール

■ セキュリティ - ファイアウォール - IPV4 ファイアウォールルール -IPv4 ファイアウォールルールの追加

「追加」をクリックし、IPv4 ファイアウォールルールを追加します。

図 9-52　IPv4 ファイアウォールルールの追加

本画面には以下の項目が含まれます。

項目	説明
優先度	ルールの優先度を指定します。1 ～ 998 から選択します。値が小さいほど優先度が高くなります。
名前	ファイアウォールルールの名前を入力します。
ポリシー	ポリシータイプを「許可」「拒否」から選択します。
プロトコル	ルールを適用するプロトコルを「Any」「TCP」「UDP」「TCP/UDP」「ICMP」から選択します。
ソースインターフェイス	送信元のインターフェイスを選択します。
送信元	送信元の IP アドレスを指定します。 「Any」を入力した場合はすべての IP アドレスが対象となります。 複数の IP アドレスはカンマ「,」で区切って入力します。（例：192.168.200.101,192.168.200.200） IP アドレス範囲を入力できます。（例：192.168.200.101-192.168.200.200）
送信元ポート	トラフィックの送信元ポートを指定します。 「TCP」「UDP」「TCP/UDP」プロトコルを選択した場合にのみ表示されます。
宛先	宛先の IP アドレスを指定します。 「Any」を入力した場合はすべての IP アドレスが対象となります。 複数の IP アドレスはカンマ「,」で区切って入力します。（例：192.168.200.101,192.168.200.200） ハイフンを使用し、IP アドレス範囲を入力できます。（例：192.168.200.101-192.168.200.200）
ディスティネーションポート	トラフィックの宛先ポートを指定します。 「TCP」「UDP」「TCP/UDP」プロトコルを選択した場合にのみ表示されます。
スケジュール	スケジュールを選択します。

設定後、「保存」をクリックします。

セキュリティ - ファイアウォール - ポートフォワーディング

ポートフォワーディングは、WAN から特定のポート番号宛てに届いたパケットを、あらかじめ設定しておいた LAN 側のデバイスに転送する機能です。
ネットワークに入ってくるトラフィックのアクセスを制限し、特定の外部ユーザのみが特定のローカルリソースへアクセス可能となります。
初期値では、LAN 要求に応答する場合を除き、WAN 側から LAN へのアクセスはすべてブロックされます。
外部デバイスがセキュア LAN 上のサービスにアクセスできるようにするには、サービスごとにポートフォワーディングルールを作成する必要があります。フォワーディング（転送）のほか、トランスレーション（変換）モードもサポートしています。

次の画面にポートフォワーディングの設定が表示されます。また、設定の編集、削除、追加を実行できます。
「稼働中」では本項目を有効 / 無効に設定できます。

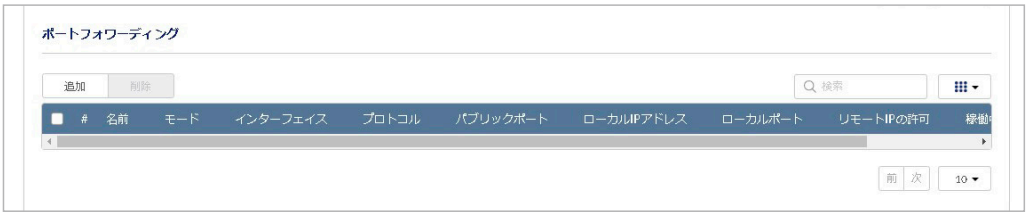


図 9-53　ポートフォワーディング

■ セキュリティ - ファイアウォール - IPV4 ファイアウォールルール - ポートフォワーディングの追加

「追加」をクリックし、ポートフォワーディングの設定を追加します。

図 9-54　ポートフォワーディングの追加

本画面には以下の項目が含まれます。

項目	説明
名前	ルールの名前を入力します。
モード	モードを以下から選択します。 • 「フォワーディング」：トラフィックは WAN ホストから LAN ホストに転送されます。 • 「トランスレーション」：送信（LAN → WAN）、受信（WAN → LAN）トラフィックの送信元 / 宛先ポートを変更するために使用します。 **注意** 「トランスレーション」は、インターフェイス設定でルートモードが NAT に設定されている場合のみ使用できます。
インターフェイス	ルールを適用するインターフェイスを選択します。
プロトコル	ルールを適用するプロトコルを以下から選択します。 • 「TCP」「UDP」「TCP/UDP」
パブリックポート	WAN ホストでアプリケーションが実行されているポート番号を入力します。 ポート番号は整数である必要があります。 ポート範囲を指定する場合はハイフンを使用してください。（例：6880-6889）
ローカル IP アドレス	LAN ホスト IP アドレスを入力します。 トラフィックの発信元または宛先となる IP アドレスです。

項目	説明
ローカルポート	ローカルポート番号を入力します。ポート番号は整数である必要があります。 ポート範囲を指定する場合はハイフンを使用してください。（例：6880-6889） パブリック範囲のマッピングポートをローカルポートの範囲に接続する場合、範囲は同じ長さである必要があります。 「モード」に「トランスレーション」を選択した場合に設定します。 **注意**　本項目は、インターフェイス設定でルートモードが NAT に設定されている場合のみ使用できます。
リモート IP の許可	許可するリモート IP を入力します。 ここで設定されるリモート IP は、「フォワーディング」「トランスレーション」が許可されます。 複数の IP アドレスはカンマ「,」で区切って入力します。（例：192.168.200.101,192.168.200.200） ハイフンを使用し、IP アドレス範囲を入力できます。（例：192.168.200.101-192.168.200.200）

設定後、「保存」をクリックします。

セキュリティ - ファイアウォール - ポートトリガー

ポートフォワーディングと同様、WAN から特定のポート番号宛てに届いたパケットを、あらかじめ設定しておいた LAN 側のデバイスに転送します。ポートトリガーを使用すると、必要に応じて受信トラフィック用に特定の受信ポートを開放できます。使用していないときはポートは閉じられた状態となるため、ポートフォワーディングよりも安全性が高くなります。

注意　本機能は、「ネットワーク」タブ>「イーサネット」タブの「インターフェイス設定」で設定する「ルートモード」で「NAT」を設定した場合のみ使用できます。

以下の画面にポートトリガーの設定が表示されます。また、設定の編集、削除、追加を実行できます。「稼働中」欄では設定を有効 / 無効にできます。

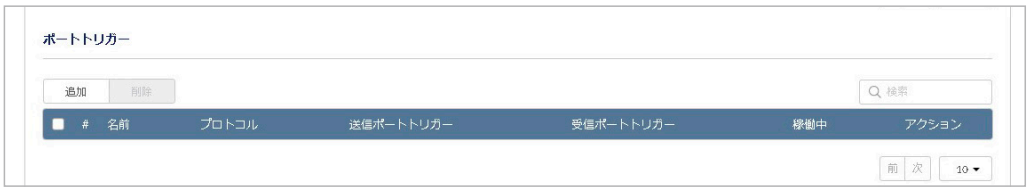


図 9-55　ポートトリガー

■ セキュリティ - ファイアウォール - ポートトリガー - ポートトリガーの追加

「追加」をクリックし、ポートトリガーの設定を追加します。

図 9-56　ポートトリガーの追加

本画面には以下の項目が含まれます。

項目	説明
名前	ルールの名前を入力します。
プロトコル	ルールを適用するプロトコルを以下から選択します。 • 「TCP」「UDP」「TCP/UDP」
送信ポートトリガー	トリガーポートの範囲を入力します。
受信ポートトリガー	トラフィックを受信するために開いているポート範囲を入力します。

設定後、「保存」をクリックします。

セキュリティ - ファイアウォール - IPV6 ファイアウォールルール

ファイアウォールルールにより、ネットワークの送受信トラフィックを制限できます。
トラフィックのプロトコル、送信元、宛先を指定し、該当するトラフィックを「許可」または「拒否」するかを指定します。

以下の画面に IPV6 ファイアウォールルールの設定が表示されます。また、設定の編集、削除、追加を実行できます。
「稼働中」欄では設定を有効 / 無効にできます。

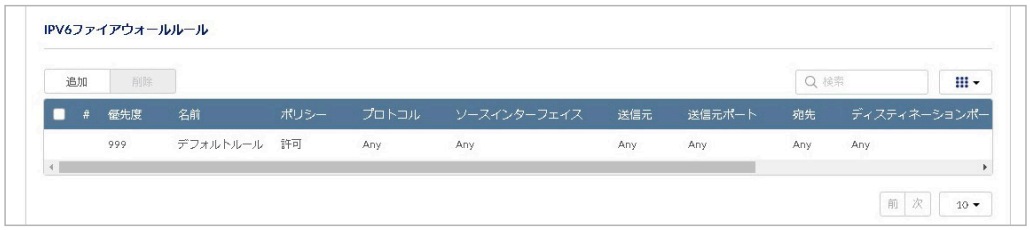


図 9-57　IPV6 ファイアウォールルール

■ セキュリティ - ファイアウォール - IPv6 ファイアウォールルール -IPv6 ファイアウォールルールの追加

「追加」をクリックし、IPv6 ファイアウォールルールを追加します。

図 9-58　IPv6 ファイアウォールルールの追加

本画面には以下の項目が含まれます。

項目	説明
優先度	ルールの優先度を指定します。1-998 から選択します。値が小さいほど優先度が高くなります。
名前	ファイアウォールの名前を入力します。
ポリシー	ポリシータイプを「許可」「拒否」から選択します。
プロトコル	ルールを適用するプロトコルを「Any」「TCP」「UDP」「TCP/UDP」「ICMP」から選択します。
ソースインターフェイス	送信元のインターフェイスを選択します。
送信元	送信元の IPv6 アドレスを指定します。 「Any」を入力した場合はすべての IPv6 アドレスが対象となります。 複数の IPv6 アドレスはカンマ「,」で区切って入力します。（例：2001:db8:abcd:64::1234,2001:db8:abcd:64::5678） IPv6 アドレスのプレフィックスを入力できます。（例：2001:db8:abcd:64::/64）
送信元ポート	トラフィックの送信元ポートを指定します。 「TCP」「UDP」「TCP/UDP」プロトコルを選択した場合にのみ表示されます。
宛先	宛先の IPv6 アドレスを指定します。 「Any」を入力した場合はすべての IPv6 アドレスが対象となります。 複数の IPv6 アドレスはカンマ「,」で区切って入力します。（例：2001:db8:abcd:64::1234,2001:db8:abcd:64::5678） IPv6 アドレスのプレフィックスを入力できます。（例：2001:db8:abcd:64::/64）
ディスティネーションポート	トラフィックの宛先ポートを指定します。 「TCP」「UDP」「TCP/UDP」プロトコルを選択した場合にのみ表示されます。
スケジュール	スケジュールを選択します。

設定後、「保存」をクリックします。

セキュリティ - IPS

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**セキュリティ**」タブ >「**IPS**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「セキュリティ」を選択 →「**IPS**」タブを選択

以下で、IPS（Intrusion Prevention System/ 不正侵入防止システム) の設定を行います。
IPS（Intrusion Prevention System）/ 不正侵入防止システムは、インターネットからの悪意ある攻撃がプライベートネットワークにアクセスすることを防ぎます。本製品にロードされたスタティックな攻撃シグニチャにより、一般的な攻撃を検出して防止することが可能です。

本画面には以下の項目が表示されます。

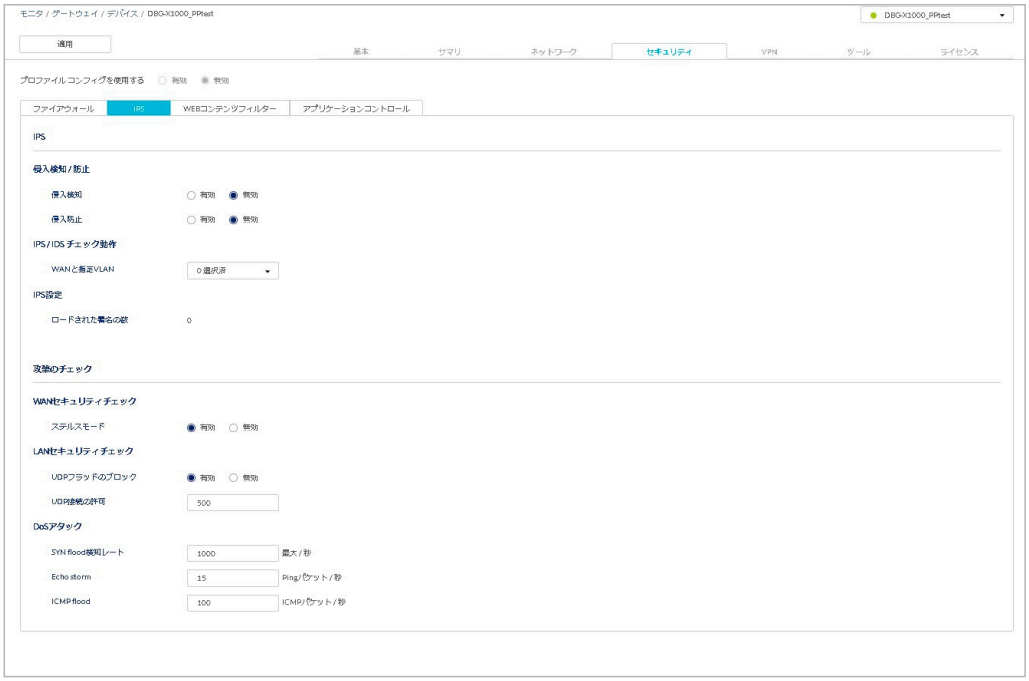


図 9-59　IPS

設定後、画面上部の「適用」をクリックします。

セキュリティ - IPS - IPS

IPS（Intrusion Prevention System/ 不正侵入防止システム) の設定を行います。
侵入検知と防止の有効 / 無効、「WAN」と「LAN/VLAN」間のチェックの有効 / 無効を設定できます。

図 9-60　IPS

本画面には以下の項目が含まれます。

項目	説明
侵入検知 / 防止	
侵入検知	侵入検知を有効 / 無効に設定します。
侵入防止	侵入防止を有効 / 無効に設定します。
IPS / IDS チェック動作	
WAN と指定 VLAN	選択した VLAN と WAN の間の侵入を検知します。
IPS 設定（デバイス設定のみ表示）	
ロードされた署名の数	本製品にロードされた署名（シグネチャ）の数が表示されます。 シグネチャには検出パターンや検出のルールが記述されており、シグネチャに基づいて検出が行われます。

設定後、画面上部の「適用」をクリックします。

セキュリティ - IPS - 攻撃のチェック

攻撃（アタック）とは、悪意あるセキュリティ違反、または意図的ではないネットワークの問題を意味します。
攻撃のチェックを行うことにより、連続する Ping リクエストや ARP スキャンを経由するディスカバリなど、WAN におけるセキュリティの脅威を管理できます。また、TCP フラッド、UDP フラッドなど、帯域幅を消費し通常のネットワークサービスの動作を妨げる攻撃をブロックできます。

本製品は DoS 攻撃をブロックする機能があります。DoS 攻撃（Denial of Service attack）」は、過剰なアクセスや大量のデータを送付するサイバー攻撃です。DoS 攻撃を受けた場合、処理能力と帯域幅が不足し、通常のネットワークサービスが妨げられる可能性があります。SYN フラッド、エコーストーム、ICMP パケットフラッディングのしきい値を設定し、しきい値を超えたトラフィックを DoS 攻撃の可能性があると判断できます。

図 9-61　攻撃のチェック

本画面には以下の項目が含まれます。

項目	説明
WAN セキュリティチェック	
ステルスモード	ステルスモードの使用の有無を、有効 / 無効で指定します。
LAN セキュリティチェック	
UDP フラッドのブロック	有効にした場合、UDP フラッドをブロックします。 LAN 上の単一コンピュータからの、設定した数を超えたアクティブな UDP 接続を受け付けません。
UDP 接続の許可	LAN 上の 1 台のコンピュータから本製品が同時に受け入れる UDP 接続の数を入力します。 「UDP フラッドのブロック」を有効にした場合に表示されます。 • 設定可能範囲：25 - 500
DoS アタック	
SYN flood 検知レート	SYN フラッドを検出するレートを入力します。
Echo storm	WAN からのエコーストーム攻撃を検出するしきい値（1 秒あたりの Ping パケット数）を入力します。 しきい値以上の Ping トラフィックを外部アドレスから受信した場合、エコーストーム攻撃として検出され、当該アドレスからのそれ以上の Ping トラフィック送信を防止します。
ICMP flood	WAN からの ICMP フラッド攻撃を検出するしきい値（1 秒あたりの ICMP パケット数）を入力します。 しきい値以上の ICMP トラフィックを外部アドレスから受信した場合、ICMP フラッド攻撃として検出され、当該アドレスからのそれ以上の ICMP トラフィック送信を防止します。

設定後、画面上部の「適用」をクリックします。

セキュリティ - WEB コンテンツフィルター

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**セキュリティ**」タブ >「**WEB コンテンツフィルター**」タブを選択
- 画面の表示手順（プロファイル設定時）：**設定 > ゲートウェイ > プロファイル** 画面で「セキュリティ」を選択 →「**WEB コンテンツフィルター**」タブを選択

以下で、WEB コンテンツフィルタリングの設定を行います。

「WEB コンテンツフィルター」では、Web ページをフィルタリングできます。
WEB コンテンツフィルターにより、LAN と WAN の間にインターネットアクセスポリシーを作成できます。
ファイアウォールルールではトラフィックのタイプに基づいてポリシーを作成しますが、WEB コンテンツフィルターではウェブベースのコンテンツ自体を使用して、トラフィックを許可 / 拒否します。

本画面には以下の項目が表示されます。

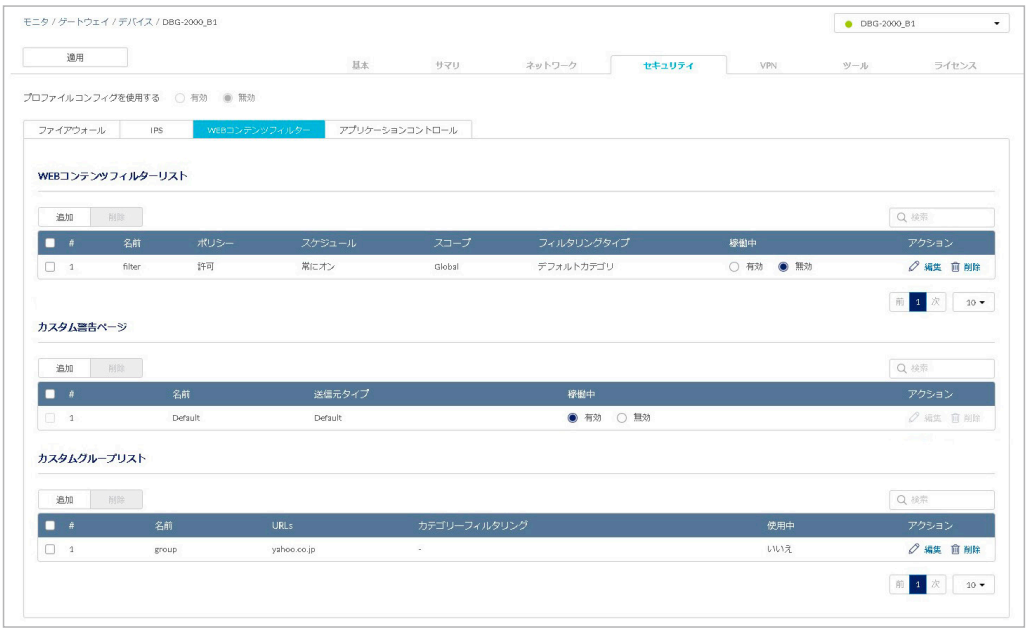


図 9-62　WEB コンテンツフィルター

設定後、画面上部の「適用」をクリックします。

セキュリティ - WEB コンテンツフィルター - WEB コンテンツフィルターリスト

WEB コンテンツフィルターのリストを設定します。

次の画面はコンテンツフィルターの設定内容を表示します。
「稼働中」ではフィルタを有効 / 無効に設定できます。また、設定の編集、削除、追加を実行できます。

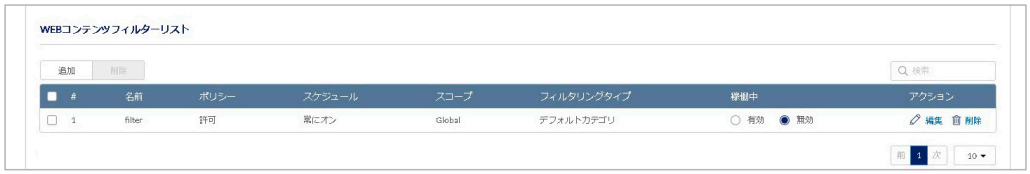


図 9-63　WEB コンテンツフィルターリスト

■ セキュリティ - WEB コンテンツフィルター - WEB コンテンツフィルターリスト - WEB コンテンツフィルターの追加

「追加」をクリックし、フィルタの設定を追加します。

図 9-64　WEB コンテンツフィルターの追加

本画面には以下の項目が含まれます。

項目	説明
名前	フィルタの名前を入力します。
ポリシールールの設定	
ポリシー	ポリシールールを「許可」「拒否」から選択します。 「拒否」を選択した場合、管理対象外に対するアクションとオーバーライドの設定を行います。
スケジュール	フィルタを適用するスケジュールを選択します。 スケジュール設定は**設定 > スケジュールポリシー**画面から行います。
非管理アクション	管理対象外のサイトに対して実行するアクションを「許可」「拒否」から選択します。 • 初期値：「許可」
オーバーライド許可	「有効」にした場合、ブロックするカテゴリに分類されたサイトを許可します。
オーバーライドタイムアウト（秒）	ブロック対象のカテゴリが「オーバーライド許可」によって接続が許可される時間（秒）を指定します。
アクセス時の更新	ブロック対象のカテゴリへの新しいアクセス毎に オーバーライド（上書き）タイマを再起動します。タイムアウトするまで接続は許可されます。
ポリシースコープの設定	
ポリシースコープ	ポリシースコープを「Global」「機能別」から選択します。 「Global」を選択した場合、選択した WEB コンテンツに一致するすべてのタイプのトラフィックを対象とします。 「機能別」を選択した場合、以降に表示される項目を設定します。 プロファイル設定画面では本項目を設定できません。

項目	説明
ネットワーク	ネットワークプロファイルを以下から選択します。 • 「シングル」: IP アドレスを入力します。 • 「レンジ」: IP アドレス範囲を入力します。 • 「インターフェイス」: インターフェイスを選択します。
コンテンツフィルタリング	
フィルタリングタイプ	フィルタリングタイプを以下から選択します。 • 「デフォルトカテゴリ」: フィルタリングするカテゴリを選択します。 • 「URL」: 画面右下に表示される「次」をクリックし、URL を追加します。 • 「デフォルトカテゴリ + URL」: フィルタリングするカテゴリを選択します。また、画面右下に表示される「次」をクリックし、URL を追加します。 • 「カスタムグループ」: 作成したグループを使用してフィルタリングを行います。詳細は「セキュリティ - WEB コンテンツフィルター - カスタムグループリスト - カスタムグループリストの追加」を参照してください。 注意 Web コンテンツフィルターは、IP アドレスを基準に動作します。そのため、IP アドレスが同一である URL は、「フィルタリングタイプ」に「URL」を選択しフィルタリング対象として指定していない場合でもフィルタリングの対象となります。
デフォルトカテゴリ	「デフォルトカテゴリ」「デフォルトカテゴリ + URL」を選択した場合、カテゴリを選択します。
カスタムグループ	「カスタムグループ」を選択した場合、カスタムグループを選択します。

設定後、「保存」をクリックします。

■ セキュリティ - WEB コンテンツフィルター - WEB コンテンツフィルターリスト - URL の追加

フィルタリングタイプに「URL」「デフォルトカテゴリ + URL」を選択した場合、次の画面で URL を追加します。

図 9-65　URL の追加

本画面には以下の項目が含まれます。

項目	説明
URL/ キーワードの追加	URL、ドメイン名またはキーワードを入力します。 「追加」をクリックし、複数の URL/ キーワードを追加できます。 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。
一括インポート	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ます。 最大 512 個の URL を追加できます。

設定後、「保存」をクリックします。
前の画面に戻る場合は「前」をクリックします。

セキュリティ - WEB コンテンツフィルター - カスタム警告ページ

インターネットサーフィンのポリシーに違反しているクライアント対し、通知を行う警告画面を設定します。

次の画面に警告画面の設定が表示されます。また、設定の編集、削除、追加を実行できます。
「稼働中」欄では設定を有効 / 無効にできます。

図 9-66　カスタム警告ページ

■ 警告画面の追加

「追加」をクリックし、警告画面の設定を追加します。

図 9-67　警告画面の追加

本画面には以下の項目が含まれます。

項目	説明
名前	警告画面の名前を入力します。
警告ページ	警告画面を選択します。警告画面は**設定 > スプラッシュページ**画面から追加、編集できます。

設定後、「保存」をクリックします。

セキュリティ - WEB コンテンツフィルター - カスタムグループリスト

フィルタリングに使用するグループを設定します。URL やカテゴリをグループ化して管理することができます。

次の画面はカスタムグループリストの設定内容を表示します。また、設定の編集、削除、追加を実行できます。

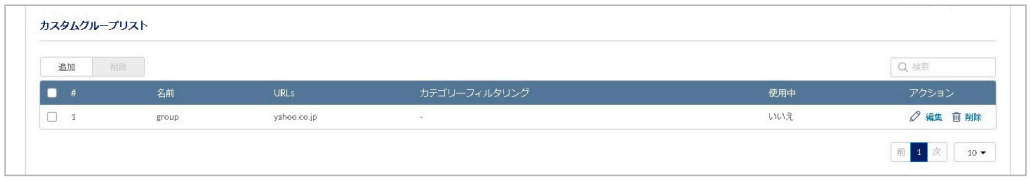


図 9-68　カスタムグループリスト

■ セキュリティ - WEB コンテンツフィルター - カスタムグループリスト - カスタムグループリストの追加

「追加」をクリックし、グループの設定を追加します。

図 9-69　グループ設定の追加（URL）

図 9-70　グループ設定の追加（カテゴリベース）

本画面には以下の項目が含まれます。

項目	説明
グループ名	グループ名を入力します。
カスタムフィルタリングタイプ	フィルタリングタイプを以下から選択します。選択した項目によって表示される画面が異なります。 • 「URL」：URL を追加します。 • 「カテゴリーベース」：フィルタリングするカテゴリを選択します。 • 「URL+ カテゴリーベース」：URL を追加します。また、画面右下に表示される「次」をクリックし、フィルタリングするカテゴリを選択します。
URL フィルタリング	
URL/ キーワードの追加	URL、ドメイン名またはキーワードを入力します。 「追加」をクリックし、複数の URL/ キーワードを追加できます。 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。
一括インポート	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ます。 最大 512 個の URL を追加できます。
カテゴリベースフィルタリング	
サポートアイテム	フィルタリングするカテゴリのチェックボックスにチェックをいれます。 「>>」ボタンをクリックして「選択アイテム」のボックスに移動させます。 本項目は「カテゴリーベース」または「URL+ カテゴリーベース」を選択した場合に設定します。
選択アイテム	「サポートアイテム」から選択したアイテムを表示します。 選択したアイテム欄からアイテムを削除するには、カテゴリを選択して「<<」ボタンをクリックします。 本項目は「カテゴリーベース」または「URL+ カテゴリーベース」を選択した場合に表示されます。

設定後、「保存」をクリックします。

注意 WEB コンテンツフィルターにおいて、対象の URL がどのカテゴリに分類されるかは、下記サイトで確認できます。
https://www.clavister.com/web-content-filtering/

セキュリティ - アプリケーションコントロール

- 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**セキュリティ**」タブ >「**アプリケーションコントロール**」タブを選択
- 画面の表示手順（プロファイル設定時）:**設定 > ゲートウェイ > プロファイル** 画面で「セキュリティ」を選択 →「**アプリケーションコントロール**」タブを選択

以下で、アプリケーションコントロールの設定を行います。

アプリケーションコントロールを使用すると、特定のアプリケーション（YouTube、Facebook など）のトラフィックを許可または拒否できます。

本画面には以下の項目が表示されます。
「稼働中」ではアプリケーションコントロールの有効 / 無効を選択できます。また、設定の編集、削除、追加を実行できます。

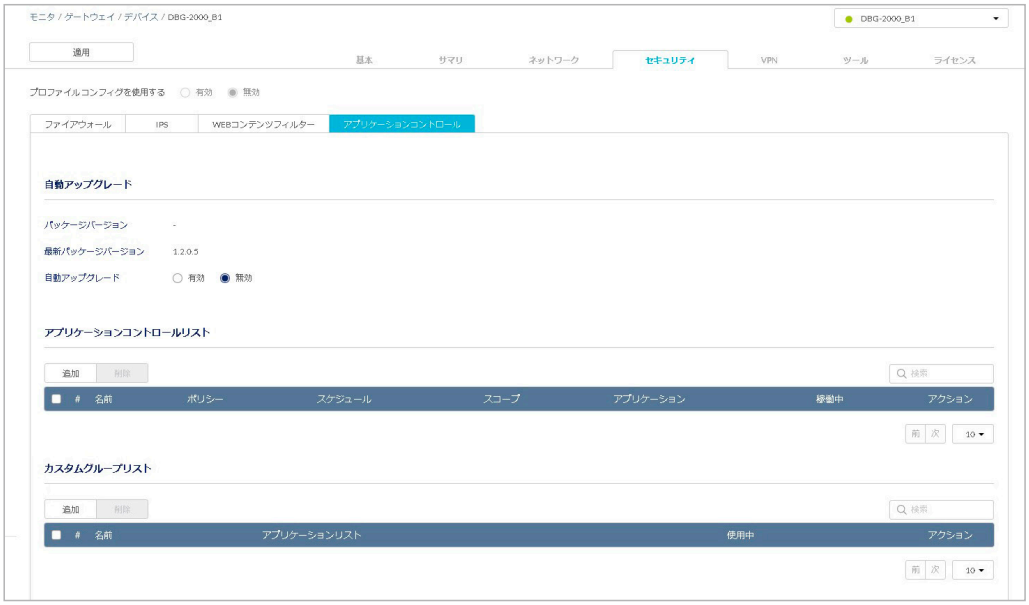


図 9-71　アプリケーションコントロール

設定項目の詳細については以下を参照してください。
「セキュリティ - アプリケーションコントロール - 自動アップグレード」
「セキュリティ - アプリケーションコントロール - アプリケーションコントロールリスト」
「セキュリティ - アプリケーションコントロール - カスタムグループリスト」

設定後、画面上部の「適用」をクリックします。

セキュリティ - アプリケーションコントロール - 自動アップグレード

現在実行しているパッケージのバージョンを表示します。
サーバ上の更新されたパッケージの有無をデバイスが自動的にチェックする時間間隔、またはスケジュールを設定します。

図 9-72　自動アップグレード

本画面には以下の項目が含まれます。

項目	説明
パッケージバージョン	実行中のパッケージバージョンを表示します。
最新パッケージバージョン	最新のパッケージバージョンを表示します。
自動アップグレード	自動アップグレードの有効 / 無効を設定します。
時間	本項目は、「自動アップグレード」欄で「有効」を選択した場合のみ表示されます。 サーバ上の更新されたパッケージの有無をチェックする時間を設定します。 • 「インターバル」：本製品が更新されたパッケージの有無をチェックする間隔（単位：分）を入力します。 • 「スケジュール」:設定した日時に更新されたパッケージの有無をチェックします。曜日と時刻を選択します。

設定後、画面上部の「適用」をクリックします。

セキュリティ - アプリケーションコントロール - アプリケーションコントロールリスト

アプリケーションコントロールリストを設定します。
特定のアプリ、またはグループを選択して、そのグループに関連付けられているアプリケーションを管理できます。

本画面には以下の項目が表示されます。
「稼働中」ではアプリケーションコントロールの有効 / 無効を選択できます。また、設定の編集、削除、追加を実行できます。

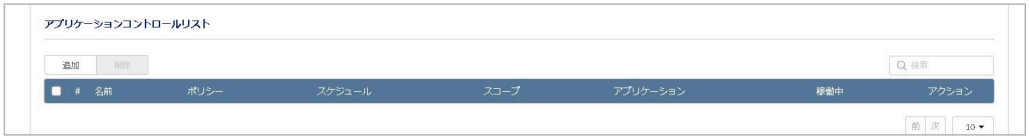


図 9-73　アプリケーションコントロールリスト

■ セキュリティ - アプリケーションコントロール - アプリケーションコントロールリスト - アプリケーションコントロールリストの追加

「追加」をクリックし、アプリケーションコントロールリストの設定を追加します。

図 9-74　アプリケーションコントロールリストの追加

本画面には以下の項目が含まれます。

項目	説明
ポリシー名	ポリシーの名前を入力します。
ポリシールールの設定	
ポリシー	ポリシールールを「許可」「拒否」から選択します。
スケジュール	ポリシールールを適用するスケジュールを選択します。 スケジュール設定は**設定 > スケジュールポリシー**画面から行います。
ポリシースコープの設定	
ポリシースコープ	ポリシースコープを「Global」「機能別」から選択します。 「Global」ポリシーは、選択したアプリケーションに一致するすべてのタイプのトラフィックを対象とします。 「機能別」を選択した場合、以降に表示される項目を設定します。 プロファイル設定画面では本項目を設定できません。
ネットワーク	ネットワークプロファイルを以下から選択します。 • 「シングル」: IP アドレスを入力します。 • 「IP レンジ」: IP アドレス範囲を入力します。 • 「インターフェイス」: インターフェイスを選択します。

項目	説明
アプリケーションコントロール	
アプリケーションタイプ	アプリケーションタイプを以下から選択します。 • 「デフォルトグループ」: 初期値で設定されているグループを使用してフィルタリングを行います。「デフォルトグループ」のドロップダウンリストからグループを選択します。 • 「単一アプリケーション」: カテゴリを選択後、アプリケーションを選択します。 • 「カスタムグループ」:作成したグループを使用してフィルタリングを行います。「カスタムグループの追加」からグループを作成できます。詳細は「セキュリティ - アプリケーションコントロール - カスタムグループリスト - グループ設定の追加」を参照してください。
デフォルトグループ	「アプリケーションタイプ」に「デフォルトグループ」を選択した場合に表示されます。初期値で設定されているグループを「デフォルトグループ」のドロップダウンリストから選択します。
カテゴリ	アプリケーションタイプに「単一アプリケーション」を選択した場合に表示されます。カテゴリを指定します。
アプリケーション	本項目は、アプリケーションタイプに「単一アプリケーション」を選択した場合に表示されます。アプリケーションを指定します。
カスタムグループ	本項目は、アプリケーションタイプに「カスタムグループ」を選択した場合に表示されます。カスタムグループを指定します。

設定後、「保存」をクリックします。

セキュリティ - アプリケーションコントロール - カスタムグループリスト

アプリケーションコントロールに使用するグループリストを設定します。

本画面にはカスタムグループリストの設定内容が表示されます。また、設定の編集、削除、追加を実行できます。
「使用中」ではグループがアプリケーションコントロールに使用されているかどうかを確認できます。

図 9-75　カスタムグループリスト

■ セキュリティ - アプリケーションコントロール - カスタムグループリスト - グループ設定の追加

「追加」をクリックし、グループの設定を追加します。

図 9-76　グループ設定の追加

本画面には以下の項目が含まれます。

項目	説明
グループ名	グループ名を入力します。
サポート APP	フィルタリングするアプリケーションのチェックボックスにチェックを入れます。 「>>」ボタンをクリックして「選択 APP」のボックスに移動します。
選択 APP	「サポート APP」から選択した項目を表示します。 「選択 APP」欄から項目を削除するには、アプリケーションを選択して「<<」ボタンをクリックします。

設定後、「保存」をクリックします。

「VPN」タブ

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VP**N」タブを選択

本製品の VPN 設定について説明します。

VPN（Virtual Private Network）は、インターネット上で仮想のプライベートネットワークを作成し、安全な通信を可能とする技術です。

本製品はサイト間 VPN、リモートアクセス VPN をサポートしています。
サイト間 VPN はオフィスなどの拠点同士を接続します。リモートアクセス VPN は、リモートクライアント（PC などのデバイス）から拠点に接続します。
また、本製品は PPTP/L2TP による VPN 接続をサポートしています。

参照 設定項目の詳細については以下を参照してください。
「VPN - SITE TO SITE VPN」
「VPN - CLIENT TO SITE VPN」
「VPN - PPTP/L2TP」
「VPN - OPEN VPN」
「VPN - GRE トンネル」

VPN - SITE TO SITE VPN

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VP**N」タブ >「**SITE TO SITE VPN**」タブを選択

サイト間 VPN は、インターネット上に IPsec トンネルを設定し、オフィスなどの拠点同士を接続します。通信を暗号化するため、最も安全性の高い VPN 接続方式です。本機能を使用すると、トンネルのエンドポイントの詳細とローカル / リモートネットワークを手動で入力することなく、VPN トンネルを確立できます。

次の画面にサイト間 VPN の設定が表示されます。また、VPN の有効 / 無効、追加、削除を実行できます。

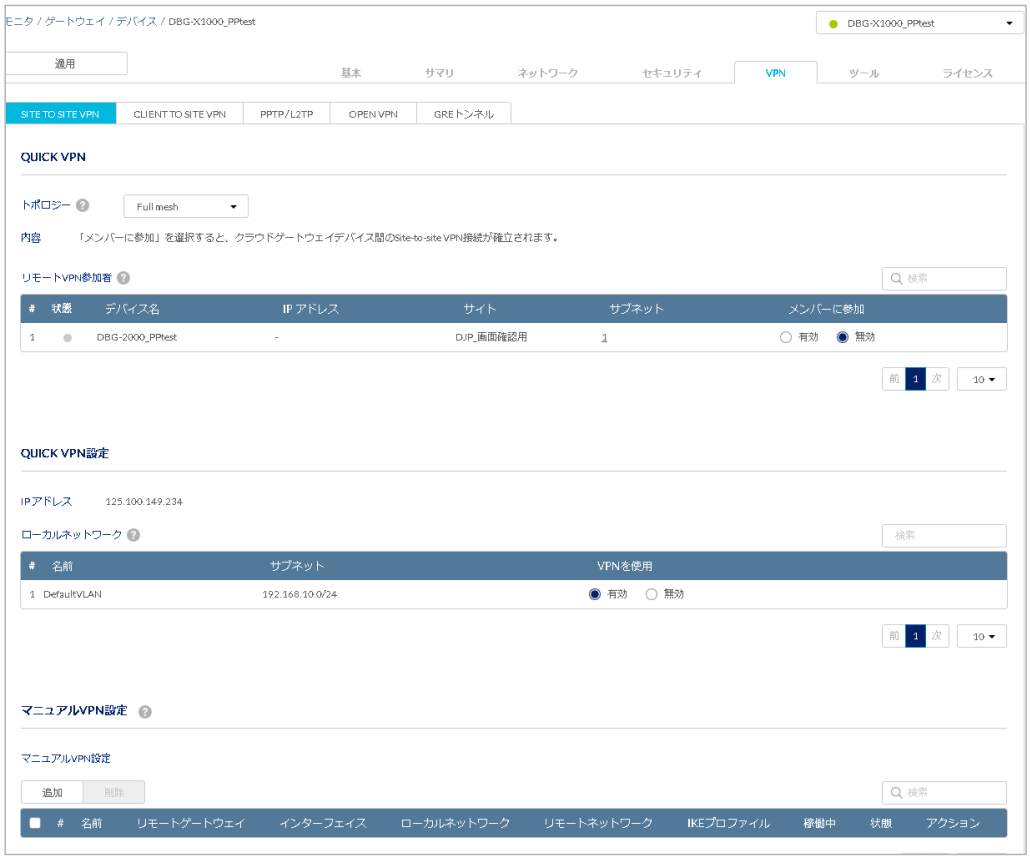


図 9-77　SITE TO SITE VPN

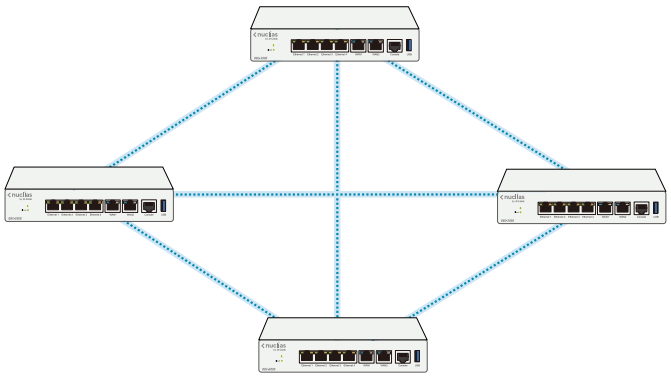
設定の詳細については以下を参照してください。
「VPN - SITE TO SITE VPN（Full mesh）」
「VPN - SITE TO SITE VPN（ハブアンドスポーク）」
「VPN - SITE TO SITE VPN - QUICK VPN 設定（Full mesh/ ハブアンドスポーク）」
「VPN - SITE TO SITE VPN - マニュアル VPN 設定（Full mesh/ ハブアンドスポーク）」

設定後、画面上部の「適用」をクリックします。
クライアントとネットワークが IPsec トンネルを介してどのように接続されるかを設定します。
Nuclias クラウドの同じ組織に展開されている Nuclias ゲートウェイデバイス間に VPN トンネルを構築できます。

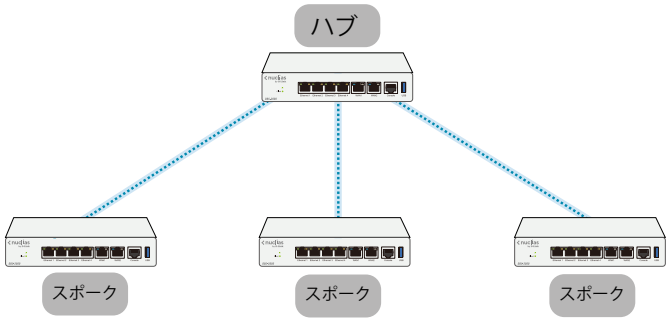
図 9-78　トポロジー

「トポロジー」には、次の 2 つのモードがあります。

- **Full mesh**
  Nuclias ゲートウェイ同士のサイト間 VPN 接続は、全てのサイト間で自動的に確立されます。



- **ハブアンドスポーク**
  1 つのサイトをハブとして設定し、ハブとその他のサイト（スポーク）間で VPN 接続を確立します。
  ハブアンドスポークを選択した場合、「ハブアンドスポークタイプ」で「HUB」または「スポーク」を選択します。



「トポロジー」で「Full mesh」または「ハブアンドスポーク」を選択すると、参加している Nuclias ゲートウェイは自動的に次の機能を実行します。

- VPN に参加しているローカルサブネットをアドバタイズ
- 使用可能な WAN ポートの WAN IP アドレスをアドバタイズ
- グローバル VPN ルートテーブルを適用
- VPN トンネルとトラフィック暗号化を確立するために必要な設定を適用

VPN - SITE TO SITE VPN（Full mesh）

「トポロジー」で「Full mesh」を選択した場合の設定について説明します。

トポロジを「Full mesh」モードに設定すると、同じモードに設定されたすべての Nuclias ゲートウェイ（リモート VPN 参加者）が表示されます。

特定のリモートデバイスとのトンネルを確立するには、「メンバーに参加」を有効にします。
トンネル設定がリモートピアにプッシュされると、リモートピアとの間にトンネルが確立されます。

図 9-79　SITE TO SITE VPN 設定（Full mesh）

「リモート VPN 参加者」には以下の項目が含まれます。

項目	説明
状態	リモートデバイスのステータスを表示します。 緑色はオンラインであることを示し、赤色はオフラインであることを示します。
デバイス名	Full mesh モードに設定されているリモートデバイスの名前を表示します。
IP アドレス	リモートゲートウェイデバイスの WAN IP アドレスを表示します。
サイト	リモートゲートウェイデバイスのサイトを表示します。
サブネット	リモートゲートウェイデバイスのサブネットの数を表示します。 カーソルをあてると、リモートデバイスのサブネットとサブネットマスクを表示できます。
メンバーに参加	有効にした場合、トンネルを確立するために必要なトンネル設定がリモートピアにプッシュされます。

「QUICK VPN 設定（クイック設定）」と「マニュアル VPN 設定（手動設定）」の詳細については、以下を参照してください。

- 「VPN - SITE TO SITE VPN - QUICK VPN 設定（Full mesh/ ハブアンドスポーク）」
- 「VPN - SITE TO SITE VPN - マニュアル VPN 設定（Full mesh/ ハブアンドスポーク）」

VPN - SITE TO SITE VPN（ハブアンドスポーク）

「トポロジー」で「ハブアンドスポーク」を選択した場合の設定について説明します。
1 つのサイトをハブとして設定し、ハブとその他のサイト（スポーク）間で VPN 接続を確立します。

Nuclias ゲートウェイデバイス間のサイト間 VPN 接続は、同じ組織内のすべての Site to Site 対応ピア間で自動的に確立されます。この場合、リモートのサイト間に不要な IPsec トンネルを確立し、ネットワークの性能を低下させる可能性があります。このような場合は、1 つの Nuclias ゲートウェイをハブとして指定し、その他すべてのリモートサイトをスポークとして指定する、「ハブアンドスポーク」が推奨されます。
また、「ハブアンドスポーク」モードは、複数の拠点から本社への接続がある場合などにも適しています。

ハブアンドスポークを選択した場合、タイプを「HUB」「スポーク」から選択します。

■ VPN - SITE TO SITE VPN（ハブアンドスポーク）-「HUB」に設定した場合

「HUB」モードを選択した場合、すべての HUB とスポークで VPN トンネルを確立します。

同じ組織内の別の Nuclias ゲートウェイがハブとして構成されている場合は、「既存の HUB」として追加できます。「リモート VPN ピア接続」で既存のハブへのサイト間トンネルの有効 / 無効を設定できます。また、「バックアップハブ」を有効にすることでバックアップハブとして使用することもできます。

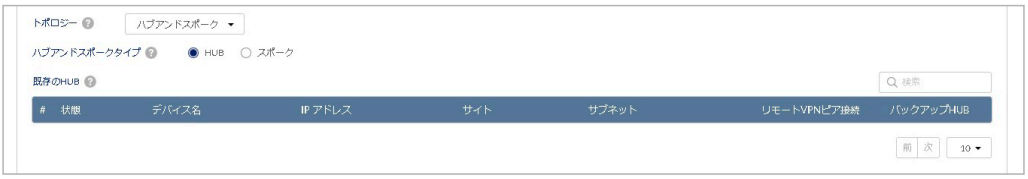


図 9-80　SITE TO SITE VPN 設定（ハブアンドスポーク - HUB 選択時）

「既存の HUB」には以下の項目が含まれます。

項目	説明
状態	リモートデバイスのステータスを表示します。 緑色はオンラインであることを示し、赤色はオフラインであることを示します。
デバイス名	ハブに設定されているリモートデバイスの名前を表示します。
IP アドレス	リモートゲートウェイデバイスの WAN IP アドレスを表示します。
サイト	リモートゲートウェイデバイスのサイトを表示します。
サブネット	リモートゲートウェイデバイスのサブネットの数を表示します。 カーソルを置くと、リモートデバイスのサブネットとサブネットマスクを表示できます。
リモート VPN ピア接続	既存のハブへのサイト間トンネルの有効 / 無効を設定します。
バックアップ HUB	別のハブを現在のハブのバックアップハブとして選択できます。

■ VPN - SITE TO SITE VPN（ハブアンドスポーク）-「スポーク」に設定した場合

「スポーク」モードを選択した場合、選択したハブと VPN トンネルを確立します。

Nuclias ゲートウェイがスポークとして設定されている場合、その Nuclias ゲートウェイに対して複数のハブを設定できます。
スポークである Nuclias ゲートウェイは、すべてのサイト間トラフィックを設定されたハブに送信します。スポーク同士はトラフィックの送受信は行いません。

「スポーク」を選択すると、「既存の HUB」のリストが表示されます。
「プライマリ HUB」を有効にすると、選択したハブがスポークのプライマリハブになり、このハブと接続しているすべてのスポークと通信できます。同時に有効化できるプライマリハブは 1 つのみです。

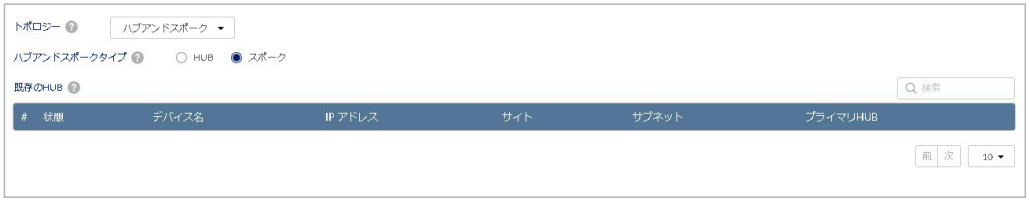


図 9-81　SITE TO SITE VPN 設定（ハブアンドスポーク - スポーク選択時）

「既存の HUB」には以下の項目が含まれます。

項目	説明
状態	ハブのステータスを表示します。 ハブがオンラインの場合は緑色の点が表示され、ハブがオフラインの場合は赤色の点が表示されます。
デバイス名	トンネルを確立するハブデバイスの名前を表示します。
IP アドレス	トンネルを確立するハブの WAN IP アドレスを表示します。
サイト	ハブデバイスを識別するために設定されたサイト名を参照します。
サブネット	リモートデバイスで共有されているローカル / プライベートネットワークの数を表示します。 カーソルをあてると、リモートデバイスのサブネットとサブネットマスクが表示されます。
プライマリ HUB	有効にした場合、プライマリハブとして設定されます。

「QUICK VPN 設定（クイック設定）」と「マニュアル VPN 設定（手動設定）」の詳細については、以下を参照してください。

- 「VPN - SITE TO SITE VPN - QUICK VPN 設定（Full mesh/ ハブアンドスポーク）」
- 「VPN - SITE TO SITE VPN - マニュアル VPN 設定（Full mesh/ ハブアンドスポーク）」

VPN - SITE TO SITE VPN - QUICK VPN 設定（Full mesh/ ハブアンドスポーク）

「QUICK VPN 設定」では、同一の Nuclias クラウド組織内に登録されている DBG デバイス間に VPN トンネルを確立するための設定を行います。

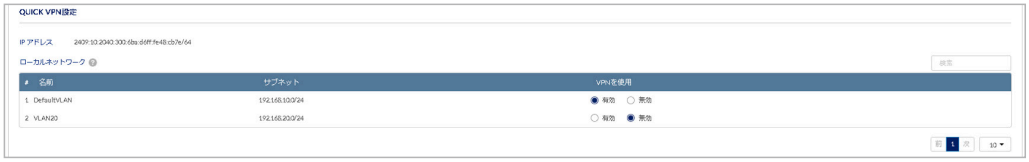


図 9-82　QUICK VPN 設定

「QUICK VPN 設定」には以下の項目が含まれます。

「ローカルネットワーク」では、複数のサブネットがある場合は、VPN に参加するサブネットを指定するオプションがあります。
有効なサブネットからのトラフィックは IPsec VPN によって暗号化されます。
すべてのローカルサブネットは、VPN トポロジ内で一意である必要があります。

項目	説明
IP アドレス	デバイスの現在の WAN IP アドレスが表示されます。
ローカルネットワーク	
名前	ローカルサブネットの LAN/VLAN インターフェイスの名前が表示されます。
サブネット	サブネット IP アドレスが表示されます。
VPN を使用	IPsec VPN でトラフィックを暗号化する場合は、「有効」を選択します。

VPN - SITE TO SITE VPN - マニュアル VPN 設定（Full mesh/ ハブアンドスポーク）

「マニュアル VPN 設定」では、VPN を手動で設定し、IPsec VPN トンネルを構築できます。

マニュアル VPN 設定は、以下のようなケースで使用します。
- 異なる Nuclias クラウド組織に登録されている 2 つの Nuclias ゲートウェイデバイス間にトンネルを確立する場合
- Nuclias ゲートウェイとサードパーティ製ゲートウェイの間にトンネルを確立する場合

本画面には「マニュアル VPN 設定」と「IKE プロファイル」の項目があります。
「稼働中」では VPN の有効 / 無効を選択できます。
また、設定の編集、削除、追加を実行できます。

図 9-83　マニュアル VPN 設定

■ VPN - SITE TO SITE VPN - マニュアル VPN 設定 - マニュアル VPN 設定の追加

「追加」をクリックし、手動で VPN の設定を追加します。

図 9-84　マニュアル VPN 設定の追加

本画面には以下の項目が含まれます。

項目	説明
接続名	VPN 接続の名前を入力します。
IKE プロファイル	ドロップダウンリストから設定済みの IKE プロファイルを選択します。
サイト IP アドレスタイプ	使用する IP アドレスの種類を「IPv4」または「IPv6」から選択します。
ローカルサイトの設定	
ローカルネットワーク	IPsec トンネル経由で提供するネットワークアクセスタイプを選択します。 • 「サブネット」：サブネット全体が VPN に接続できます。IP アドレスとサブネットマスクを入力します。 • 「Single IP」：1 つのホストが VPN に接続できます。VPN の一部となるホストの IP アドレスを入力します。 • 「Any」：指定したローカルエンドポイントからの任意のトラフィックが VPN に接続できます。
IP アドレス	VPN 接続を行うローカルサイトの IP アドレスを入力します。
リモートサイトの設定	
リモートネットワーク	IPsec トンネル経由で提供するネットワークアクセスタイプを選択します。 • 「サブネット」：サブネット全体が VPN に接続できます。IP アドレスとサブネットマスクを入力します。 • 「Single IP」：1 つのホストが VPN に接続できます。VPN の一部となるホストの IP アドレスを入力します。 • 「Any」：指定したリモートエンドポイントからの任意のトラフィックが VPN に接続できます。
IP アドレス	VPN 接続を行うリモートサイトの IP アドレスを入力します。
送信インターフェイス	データの送信に使用するインターフェイスを指定します。
リモートゲートウェイ	接続に使用するゲートウェイを「Static IP」または「FQDN」から選択します。
IP アドレスタイプ	使用する IP アドレスの種類を「IPv4」または「IPv6」から選択します。
IP アドレス	「リモートゲートウェイ」で「Static IP」を選択した場合は、IP アドレスを入力します。
ホスト名	「リモートゲートウェイ」で「FQDN」を選択した場合は、ホスト名を入力します。
キープアライブ	キープアライブ機能の有効 / 無効を設定します。有効にした場合、以下の項目を設定します。 • 「送信元 IP アドレス」：Ping をトリガする送信元 IP を指定します。 • 「宛先 IP アドレス」：Ping を受信するリモートホストを指定します。 • 「検知時間（秒）」：Ping パケットの送信間隔を指定します。 • 「失敗後再接続」：Ping が指定回数失敗すると、トンネルを再試行します。
アイドルタイムアウト	アイドルタイムアウト機能の有効 / 無効を設定します。本項目は「キープアライブ」に「無効」を選択した場合のみ設定可能となります。 有効にした場合、以下の項目を設定します。 • 「アイドルタイムアウト（秒）」：アイドル時に接続が切断されるまでの時間（単位：秒）を入力します。
デッドピア検知	デッドピア検知機能の有効 / 無効を設定します。 有効にした場合、リモートピアが到達可能かどうかを検出できます。到達できない場合はトンネルをダウンさせます。 有効にした場合、以下の項目を設定します。 • 「検知間隔（秒）」：リモートピアにピア検出パケットを送信し、パケットが到達可能かどうかのチェックを実施する間隔を秒数で入力します。 • 「切断する連続失敗回数」：リモートピアへの接続の失敗回数を設定します。接続を指定した回数失敗した場合、リモートピアはダウンしていると判断されます。
バックアップトンネル	「デッドピア検知」を有効にした場合、VPN トンネルバックアップ機能の有効 / 無効を設定します。 有効にした場合、以下の項目を設定します。 • 「送信バックアップインターフェイス」：バックアップの送信インターフェイスを選択します。 • 「リモートバックアップゲートウェイ」：バックアップのゲートウェイを「Static IP」「FQDN」から選択します。 • 「IKE バックアッププロファイル」：バックアップの IKE プロファイルを選択します。 • 「IP アドレス」：リモートバックアップゲートウェイを「Static IP」に設定した場合は、IP アドレスを入力します。 • 「ホスト名」：リモートバックアップゲートウェイを「FQDN」に設定した場合は、ホスト名を入力します。
NetBIOS ブロードキャスト	有効にすると、NetBIOS ブロードキャストが VPN トンネルを通過できるようになります。

設定後、「保存」をクリックします。

■ VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加

IKE プロファイル（IKEv1、IKEv2）は、プロトコル、アルゴリズム、SA ライフタイム、キー管理プロトコルなどの IPsec パラメータを定義します。IKE プロファイルには、自動モードでのフェーズ 1/ フェーズ 2 ネゴシエーションの暗号化、認証、DH グループなどのアルゴリズムに関連する情報も含まれています。
VPN トンネルの両端を構成するときは、必ず同じ設定を入力してください。

「追加」をクリックし、IKE プロファイルを追加します。IKE phase-1 の設定後、IKE phase-2 の設定を行います。

図 9-85　IKE プロファイル設定の追加（IKE phase-1）

本画面には以下の項目が含まれます。

項目	説明
プロファイル名	IKE プロファイル名を入力します。
IKE バージョン	IKE のバージョンを「IKEv1」「IKEv2」から選択します。
IKE phase-1 設定	
Exchange モード	本項目は、「IKE バージョン」で「IKEv1」を選択した場合に、表示されます。 Exchange モードを「Aggressive」「Main」から選択します。
ローカル識別子タイプ	ローカル識別子タイプを「ローカル WAN IP」「FQDN」「User-FQDN」から選択します。 「FQDN」「User-FQDN」を選択した場合は、「ローカル識別子」に FQDN 名を入力します。 「ローカル WAN IP」を選択した場合、WAN インターフェイスのローカル IP アドレスが使用されます。
リモート識別子タイプ	ローカル識別子タイプを「リモート WAN IP」「FQDN」「User-FQDN」から選択します。 「FQDN」「User-FQDN」を選択した場合は、「リモート識別子」に FQDN 名を入力します。 「リモート WAN IP」を選択した場合、VPN ポリシーのリモート IP アドレスが使用されます。
DH グループ	DH（Diffie-Hellman）グループを選択します。鍵交換プロセスにおいて使われる鍵の強度を指定します。
暗号化アルゴリズム	鍵交換時に従う暗号化アルゴリズムを選択します。複数のアルゴリズムを選択できます。
認証アルゴリズム	認証アルゴリズムを選択します。複数のアルゴリズムを選択できます。
SA ライフタイム（秒）	SA（セキュリティアソシエーション）の有効期間を設定します。 • 設定可能範囲：300 - 604800（秒）
認証方法	認証方法を「事前共有鍵」または「RSA- 署名（証明書）」から選択します。
事前共有鍵	「認証方法」で「事前共有鍵」選択した場合、事前共有鍵を入力します。
証明書	「認証方法」で「RSA- 署名（証明書）」を選択した場合、証明書を選択します。
拡張認証	拡張認証機能の有効 / 無効を設定します。

項目	説明
拡張認証タイプ	拡張認証機能を有効にした場合、使用する認証タイプを以下から選択します。 • 「IPsec ホスト（イニシエータ）」：ユーザ名とパスワードを入力します。 • 「ローカル認証」：ローカルサーバに保存されているローカル認証のいずれかを選択します。 • 「認証サーバ」：RADIUS サーバを選択します。

設定後、「次」をクリックします。

IKE phase-2 の設定を行います。

図 9-86　IKE プロファイルの追加（IKE phase-2 設定）

本画面には以下の項目が含まれます。

項目	説明
IKE phase-2 設定	
プロトコル選択	IKE phase-2 のプロトコルを選択します。
暗号化アルゴリズム	使用する暗号化アルゴリズムを選択します。複数のアルゴリズムを選択できます。
認証アルゴリズム	認証アルゴリズムを選択します。複数のアルゴリズムを選択できます。
SA ライフタイム（秒）	SA（セキュリティアソシエーション）の有効期間を設定します。 • 設定可能範囲：300 - 604800（秒）
Perfect forward secrecy	有効にした場合、同じ鍵を使用せずに新たに DH 鍵交換が行われます。
DH グループ	DH グループを選択します。 「Perfect forward secrecy」を有効にした場合に設定します。

設定後、「保存」をクリックします。

VPN - CLIENT TO SITE VPN

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VPN**」タブ >「**CLIENT TO SITE VPN**」タブを選択

「CLIENT TO SITE VPN」タブでは、IPsec VPN サーバの設定を行います。

次の画面に IPsec VPN サーバと IKE プロファイルの設定が表示されます。設定の有効 / 無効、追加、削除を実行できます。

図 9-87　CLIENT TO SITE VPN

■ VPN - CLIENT TO SITE VPN - IPsec VPN サーバの追加

「追加」をクリックし、IPsec VPN サーバを追加します。

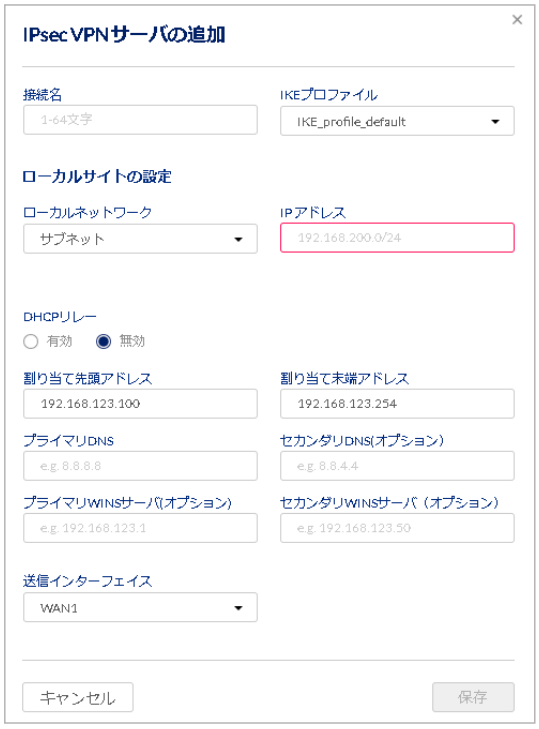


図 9-88　IPsec VPN サーバの追加

本画面には以下の項目が含まれます。

項目	説明
接続名	VPN 接続の名前を入力します。
IKE プロファイル	ドロップダウンリストから設定済みの IKE プロファイルを選択します。
ローカルサイトの設定	
ローカルネットワーク	IPsec トンネル経由で提供するネットワークアクセスタイプを選択します。 • 「サブネット」：サブネット全体が VPN に接続できます。IP アドレスを入力します。 • 「Any」：指定したローカルエンドポイントからの任意のトラフィックが VPN に接続できます。
IP アドレス	VPN に接続するための IP アドレスを入力します。
DHCP リレー	DHCP リレーの有効 / 無効を設定します。
リレーゲートウェイ	DHCP リレーを有効にした場合、リレーゲートウェイを入力します。
割り当て先頭アドレス	DHCP リレーを無効にした場合、割り当てる IP アドレス範囲の先頭 IP アドレスを入力します。
割り当て末端アドレス	DHCP リレーを無効にした場合、割り当てる IP アドレス範囲の末端 IP アドレスを入力します。
プライマリ DNS	プライマリ DNS の IP アドレスを入力します。「DHCP リレー」で「有効」を選択した場合、本項目はオプションです。
セカンダリ DNS（オプション）	セカンダリ DNS の IP アドレスを入力します。本項目はオプションです。
プライマリ WINS サーバ（オプション）	プライマリ WINS サーバの IP アドレスを入力します。本項目はオプションです。
セカンダリ WINS サーバ（オプション）	セカンダリ WINS サーバの IP アドレスを入力します。本項目はオプションです。
送信インターフェイス	データの送信に使用するインターフェイスを指定します。

設定後、「保存」をクリックします。

■ VPN - CLIENT TO SITE VPN -IKE プロファイルの追加

IP Sec VPN サーバの設定に使用する IKE プロファイルを設定します。
IKE プロファイルの設定項目については、「VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加」を参照してください。

VPN - PPTP/L2TP

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VPN**」タブ >「**PPTP/L2TP**」タブを選択

Nuclias ゲートウェイは、PPTP/L2TP VPN を確立できます。
本項目で設定を「有効」にすると、PPTP/L2TP サーバが Nuclias ゲートウェイで利用可能になり、LAN および WAN PPTP/L2TP クライアントユーザがアクセスできるようになります。さらに、PPTP/L2TP サーバ（トンネルエンドポイント）によって認証されると、PPTP/L2TP クライアントは Nuclias ゲートウェイが管理する LAN ネットワークにアクセスできます。

PPTP/L2TP クライアントに割り当てる IP アドレスの範囲は、LAN サブネットと一致しないようにしてください。
PPTP/L2TP サーバは、初期値ではローカル PPTP/L2TP ユーザ認証を使用しますが、外部 RADIUS 認証サーバを使用することもできます。

次の画面に PPTP/L2TP「サーバモード」「クライアントモード」の設定が表示されます。「稼働中」では設定の有効 / 無効を選択できます。
また、設定の編集、追加、削除を実行できます。

図 9-89　PPTP/L2TP

設定内容の詳細については「VPN - PPTP/L2TP - サーバモード」「VPN - PPTP/L2TP - クライアントモード」を参照してください。
設定後、画面上部の「適用」をクリックします。

VPN - PPTP/L2TP - サーバモード

PPTP/L2TP サーバの設定について説明します。

PPTP/L2TP「サーバモード」の設定が表示されます。「稼働中」では設定の有効 / 無効を選択できます。
また、設定の追加、編集、削除を実行できます。

図 9-90　PPTP/L2TP サーバモード

■ **VPN - PPTP/L2TP - サーバモード - PPTP サーバの追加**

「追加」をクリックし、PPTP サーバを追加します。

図 9-91　PPTP サーバの追加

本画面には以下の項目が含まれます。

項目	説明
サーバタイプ	サーバタイプとして「PPTP」を選択します。
名前	PPTP サーバの名前を入力します。
ルーティングモード	ルーティングモードを「NAT」「ルータ」から選択します。
割り当て先頭アドレス	PPTP クライアントに割り当てる IP アドレス範囲の、開始 IP アドレスを入力します。
割り当て末端アドレス	PPTP クライアントに割り当てる IP アドレス範囲の、終了 IP アドレスを入力します。
認証サーバ	使用可能な認証サーバを選択します。 ・「ローカル認証」「RADIUS」「認証なし」 選択した内容に応じて、ローカル認証データベースまたは RADIUS サーバを指定します。
ローカル認証	本項目は「認証サーバ」で「ローカル認証」を選択した場合に表示されます。 ローカル認証データベースをプルダウンメニューより選択します。
RADIUS サーバ	本項目は「認証サーバ」で「RADIUS」を選択した場合に表示されます。 RADIUS サーバをプルダウンメニューより選択します。
認証プロトコル	認証タイプを以下から選択します（複数選択可）。 ・「全て」「PAP」「CHAP」「MS-CHAP」「MS-CHAPv2」
暗号化	認証プロトコルとして「MS-CHAP」「MS-CHAPv2」が選択されている場合に暗号化オプションを選択します。 ・「全て」：すべての暗号化オプションを選択します。 ・「MPPE 40 bit」：MPPE 40 ビット暗号化を有効にします。 ・「MPPE 128 bit」：MPPE 128 ビット暗号化を有効にします。 ・「ステートフル MPPE」：ステートフル MPPE 暗号化を有効にします。このモードの MPPE 暗号化は安全性が低く、互換性のために使用できます。
アイドルタイムアウト（秒）	アイドル時に接続が切断されるまでの時間（単位：秒）を入力します。 **注意**　本項目は未サポートです。
Netbios	有効に設定した場合、NetBIOS ブロードキャストが VPN トンネルを通過できるようになります。
WINS サーバ	「Netbios」を有効にした場合、NetBIOS の WINS サーバアドレスを入力します。

設定後、「保存」をクリックします。

■ VPN - PPTP/L2TP - サーバモード - L2TP サーバの追加

「追加」をクリックし、L2TP サーバを追加します。

図 9-92　L2TP サーバの追加

本画面には以下の項目が含まれます。

項目	説明
サーバタイプ	サーバタイプとして「L2TP」を選択します。
名前	L2TP サーバの名前を入力します。
ルーティングモード	ルーティングモードを「NAT」「ルータ」から選択します。
割り当て先頭アドレス	L2TP クライアントに割り当てる IP アドレス範囲の、開始 IP アドレスを入力します。
割り当て末端アドレス	L2TP クライアントに割り当てる IP アドレス範囲の、終了 IP アドレスを入力します。
認証サーバ	使用可能な認証サーバをから選択します。 ・「ローカル認証」「RADIUS」「認証なし」 選択した内容に応じて、ローカル認証データベースまたは RADIUS サーバを指定します。
ローカル認証	本項目は「認証サーバ」で「ローカル認証」を選択した場合に表示されます。 使用するローカル認証データベースをプルダウンメニューより選択します。
RADIUS サーバ	本項目は「認証サーバ」で「RADIUS」を選択した場合に表示されます。 使用する RADIUS サーバをプルダウンメニューより選択します。
暗号化	本項目は、認証プロトコルとして「MS-CHAP」または「MS-CHAPv2」が選択されている場合に表示されます。 使用する暗号化の方式を選択します。 ・「全て」：すべての方式の暗号化を使用します。 ・「MPPE 40 bit」：標準的な強度の MPPE 40 ビット暗号化を使用します。 ・「MPPE 128 bit」：強力な強度の MPPE 128 ビット暗号化を使用します。 ・「ステートフル MPPE」:ステートフル MPPE 暗号化を使用します。この方式の MPPE 暗号化を選択した場合、互換性は向上しますが安全性は低くなります。
認証プロトコル	認証タイプを以下から選択します（複数選択可）。 ・「全て」「PAP」「CHAP」「MS-CHAP」「MS-CHAPv2」
シークレットキーを有効にする	シークレットキーを追加する場合は「有効」を選択します。
シークレットキー	使用するシークレットキーを入力します。
アイドルタイムアウト（秒）	アイドル時に接続が切断されるまでの時間（単位：秒）を入力します。
L2TP Over IPsec	L2TP over IPsec の有効 / 無効を設定します。 有効にした場合は「次」をクリックし、IKE プロファイルの設定を行います。 IKE プロファイルの設定については、「VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加」を参照してください。

設定後、「保存」をクリックします。

VPN - PPTP/L2TP - クライアントモード

PPTP/L2TP クライアントの設定について説明します。

PPTP/L2TP「クライアントモード」の設定が表示されます。「稼働中」では設定の有効 / 無効を選択できます。
また、設定の追加、編集、削除を実行できます。

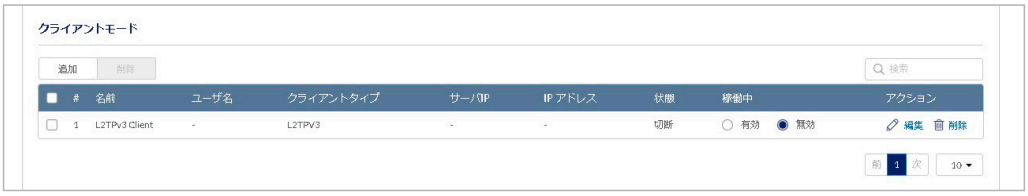


図 9-93　PPTP/L2TP クライアントモード

■ VPN - PPTP/L2TP - クライアントモード - PPTP クライアントの追加

「追加」をクリックし、PPTP クライアントを追加します。

図 9-94　PPTP クライアントの追加

本画面には以下の項目が含まれます。

項目	説明
クライアントタイプ	クライアントタイプとして「PPTP」を選択します。
名前	PPTP クライアントの名前を入力します。
VPN サーバ	接続先の PPTP サーバの IP アドレスまたはドメイン名を入力します。
トンネルタイプ	トンネルタイプを選択します。 • 「フルトンネル」: PPTP サーバ経由で、サーバデバイスに接続されているインターネットと LAN ホストにアクセスします。 • 「スプリットトンネル」: 選択したリモートネットワークにのみ VPN 接続を行います。
リモートネットワーク	「スプリットトンネル」を選択した場合、リモートネットワークのアドレスを入力します。 このアドレスは PPTP サーバのローカルアドレスです。
リモートネットマスク	「スプリットトンネル」を選択した場合、リモートネットワークのサブネットマスクを入力します。
ユーザ名 (オプション)	VPN サーバに接続するためのユーザ名を入力します。本項目はオプションです。
パスワード (オプション)	VPN サーバに接続するためのパスワードを入力します。本項目はオプションです。
MPPE	MPPE（Microsoft Point-to-Point Encryption）の有効 / 無効を設定します。
アイドルタイムアウト（秒）	アイドル時に PPTP サーバから切断されるまでの時間（単位：秒）を入力します。 注意　本項目は未サポートです。

設定後、「保存」をクリックします。

■ VPN - PPTP/L2TP - クライアントモード - L2TP クライアントの追加

「追加」をクリックし、L2TP クライアントを追加します。

図 9-95　L2TP クライアントの追加

本画面には以下の項目が含まれます。

項目	説明
クライアントタイプ	クライアントタイプとして「L2TP」を選択します。
名前	L2TP クライアントの名前を入力します。
VPN サーバ	接続先の L2TP サーバの IP アドレスまたはドメイン名を入力します。
トンネルタイプ	トンネルタイプを以下から選択します。 • 「フルトンネル」：L2TP サーバ経由で、サーバデバイスに接続されているインターネットと LAN ホストにアクセスします。 • 「スプリットトンネル」：選択したリモートネットワークにのみ VPN 接続を行います。
リモートネットワーク	「スプリットトンネル」を選択した場合、リモートネットワークのアドレスを入力します。 このアドレスは L2TP サーバのローカルアドレスです。
リモートネットマスク	「スプリットトンネル」を選択した場合、リモートネットワークのサブネットマスクを入力します。
ユーザ名 (オプション)	VPN サーバに接続するためのユーザ名を入力します。本項目はオプションです。
パスワード (オプション)	VPN サーバに接続するためのパスワードを入力します。本項目はオプションです。
シークレットキーを有効にする	シークレットキーを追加する場合は「有効」を選択します。
シークレットキー	シークレットキーを入力します。本項目は「シークレットキーを有効にする」で「有効」を選択した場合のみ表示されます。
MPPE	MPPE（Microsoft Point-to-Point Encryption）の有効 / 無効を設定します。
L2TP Over IPsec	L2TP over IPsec の有効 / 無効を設定します。 有効にした場合は「次」をクリックし、IKE プロファイルの設定を行います。 IKE プロファイルの設定については、「VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加」を参照してください。

項目	説明
デッドピア検知	本項目は「L2TP over IPsec」を「有効」にした場合に表示されます。デッドピア検知機能の有効 / 無効を設定します。 有効を選択した場合、以下の項目を設定します。 • 「検知間隔（秒）」：リモートピアにピア検出パケットを送信し、パケットが到達可能かどうかのチェックを実施する間隔を秒数で入力します。 • 「失敗後再接続」：リモートピアがダウンしていると判断する際の基準となる、リモートピアへの接続の失敗回数を指定します。指定した回数、接続に失敗した場合、VPN トンネルを切断します。その後、トンネルの確立を再試行します。

設定後、「保存」をクリックします。

■ VPN - PPTP/L2TP - クライアントモード - L2TPv3 クライアントの追加

注意 L2TPv3 クライアント、および L2TPv3 サーバは未サポートです。

「追加」をクリックし、L2TPv3 クライアントを追加します。

図 9-96　L2TPv3 クライアントの追加

本画面には以下の項目が含まれます。

項目	説明
クライアントタイプ	クライアントタイプとして「L2TPv3」を選択します。
名前	L2TPv3 クライアントの名前を入力します。
インターフェイス	トンネルを確立するインターフェイスを選択します。
Pseudowire クラス	「ダイナミックトンネル」または「スタティックトンネル」を選択します。 • 「ダイナミックトンネル」：L2TPv3 クライアントはサーバから情報を取得します。 • 「スタティックトンネル」：手動で設定を行います。

「Pseudowire クラス」で「ダイナミックトンネル」を選択した場合は、以下の項目が表示されます。

項目	説明
LNS アドレス	LNS アドレスを入力します。

項目	説明
ホスト名	ホスト名または IP アドレスを入力します。
リモートエンド ID	L2TPv3 の Remote End ID を入力します。
ローカルルータ ID	L2TPv3 の接続先に通知する Router ID を設定します。
リモートルータ ID	L2TPv3 の接続先の Router ID を設定します。
自動ダイヤル	有効にした場合、設定が適用されている間は自動的にサーバに接続します。
リダイヤル	有効にした場合、トンネルが切断されると自動的に再接続します。
リダイヤルタイムアウト	「リダイヤル」を「はい」に設定した場合、再接続のタイムアウト値を設定します。
最大リダイヤル数	「リダイヤル」を「はい」に設定した場合、再接続の最大回数を設定します。
Pseudowire インターフェイス IP (オプション)	Pseudowire インターフェイス IP を入力します。本項目はオプションです。
Pseudowire インターフェイスサブネットマスク (オプション)	Pseudowire インターフェイスのサブネットマスクを入力します。本項目はオプションです。
ピア Pseudowire インターフェイス IP (オプション)	接続先の Pseudowire インターフェイス IP を入力します。本項目はオプションです。
L2TPv3 Over IPsec	L2TPv3 over IPsec の有効 / 無効を設定します。 有効にした場合は「次」をクリックし、IKE プロファイルの設定を行います。 IKE プロファイルの設定については、「VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加」を参照してください。
デッドピア検知	L2TPv3 over IPsec を有効にした場合、デッドピア検知機能の有効 / 無効を設定します。 有効にした場合、以下の項目を設定します。 • 「検知間隔（秒）」：リモートピアにピア検出パケットを送信し、パケットが到達可能かどうかをチェックを実施する間隔を秒数で入力します。 • 「失敗後再接続」：リモートピアがダウンしていると判断する際の基準となる、リモートピアへの接続の失敗回数を指定します。指定した回数、接続に失敗した場合、VPN トンネルを切断します。その後、トンネルの確立を再試行します。

「Pseudowire クラス」で「スタティックトンネル」を選択した場合は、以下の項目が表示されます。

項目	説明
ローカル IP アドレス	L2TPv3 のローカル IP アドレスを入力します。
リモート IP	L2TPv3 のリモート IP アドレスを入力します。
トンネル ID	L2TPv3 のトンネル ID を指定します。
ピアトンネル ID	L2TPv3 の接続先トンネル ID を指定します。
セッション ID	L2TPv3 のセッション ID を指定します。
ピアセッション ID	L2TPv3 の接続先セッション ID を指定します。
カプセル化	L2 フレームのカプセル化方式として、「UDP」または「IP」を選択します。
送信元ポート	「カプセル化」で「UDP」を選択した場合、L2TPv3 で使用する送信元ポートを指定します。
宛先ポート	「カプセル化」で「UDP」を選択した場合、L2TPv3 で使用する宛先ポートを指定します。
IPv4 チェックサム	「カプセル化」で「UDP」を選択した場合、IPv4 チェックサムの有効 / 無効を設定します。
IPv6 チェックサム (TX)	「カプセル化」で「UDP」を選択した場合、IPv6 チェックサム（TX）の有効 / 無効を設定します。
IPv6 チェックサム (RX)	「カプセル化」で「UDP」を選択した場合、IPv6 チェックサム（RX）の有効 / 無効を設定します。
Cookie（オプション）	L3TPv3 の Cookie を入力します。本項目はオプションです。
ピア Cookie（オプション）	L3TPv3 の接続先の Cookie を入力します。本項目はオプションです。
レイヤ 2 Specific ヘッダ	セッションの Layer-2 Specific Header タイプを指定します。
シーケンス	パケットが不正な順序となることを防止、検出するためのシーケンス番号について設定します。 「送信」を選択した場合、各送信パケットのデフォルト Layer-2 Specific Header にシーケンス番号をセットします。「受信」を選択した場合、不正な順序となっている受信パケットを調整します。
Pseudowire インターフェイス IP (オプション)	Pseudowire インターフェイス IP を入力します。本項目はオプションです。
Pseudowire インターフェイスサブネットマスク (オプション)	Pseudowire インターフェイスのサブネットマスクを入力します。本項目はオプションです。
ピア Pseudowire インターフェイス IP (オプション)	接続先の Pseudowire インターフェイス IP を入力します。本項目はオプションです。
L2TPv3 Over IPsec	L2TPv3 over IPsec の有効 / 無効を設定します。 有効にした場合は「次」をクリックし、IKE プロファイルの設定を行います。 IKE プロファイルの設定については、「VPN - SITE TO SITE VPN - マニュアル VPN 設定 - IKE プロファイルの追加」を参照してください。

項目	説明
デッドピア検知	L2TPv3 over IPsec を有効にした場合、デッドピア検知機能の有効 / 無効を設定します。 有効にした場合、以下の項目を設定します。 • 「検知間隔（秒）」：リモートピアにピア検出パケットを送信し、パケットが到達可能かどうかのチェックを実施する間隔を秒数で入力します。 • 「失敗後再接続」：リモートピアがダウンしていると判断する際の基準となる、リモートピアへの接続の失敗回数を指定します。指定した回数、接続に失敗した場合、VPN トンネルを切断します。その後、トンネルの確立を再試行します。

設定後、「保存」をクリックします。

VPN - OPEN VPN

● 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VPN**」タブ >「**OPEN VPN**」タブを選択

注意　以下はデバイス画面からのみ設定できます。プロファイルには含まれません。

OpenVPN では、証明書やユーザ名 / パスワードを使用したピアの相互認証が可能です。
マルチクライアント - サーバ設定で利用した場合、サーバは署名と CA（認証局）を使用して、すべてのクライアントに対して認証証明書をリリースすることができます。OpenVPN は、本製品を介して確立することができます。

OpenVPN のモードは「サーバ」モード、または「クライアント」モードから選択します。

注意　OpenVPN クライアントとして OpenVPN Connect のみをサポートします。

注意　VPN クライアントはクライアント画面に表示されません。

次の画面で OpenVPN の有効 / 無効を設定します。

図 9-97　OpenVPN（無効）

有効にすると、設定項目が追加表示されます。設定項目は選択したモードによって異なります。

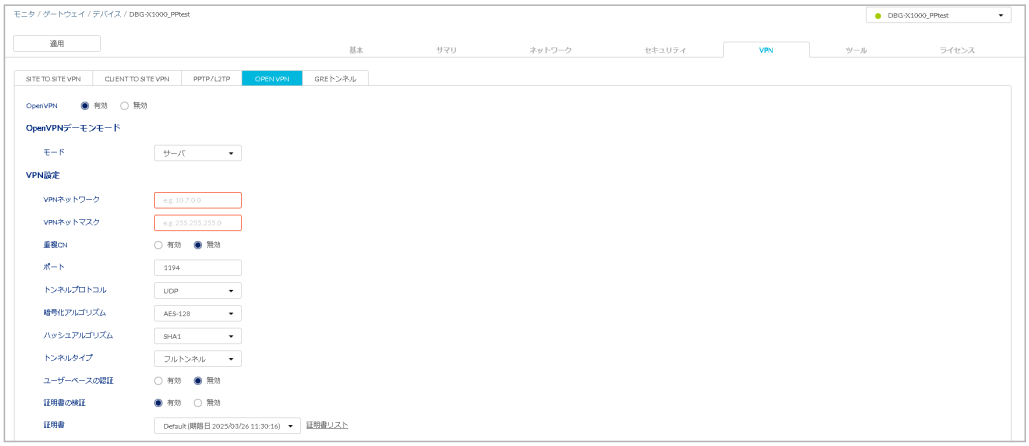


図 9-98　OPEN VPN（サーバモード）

それぞれのモードの設定内容については以下を参照してください。
「VPN - OPEN VPN（サーバモード）」
「VPN - OPEN VPN（クライアントモード）」

設定後、画面上部の「適用」をクリックします。

VPN - OPEN VPN（サーバモード）

OpenVPN のサーバモード設定について説明します。

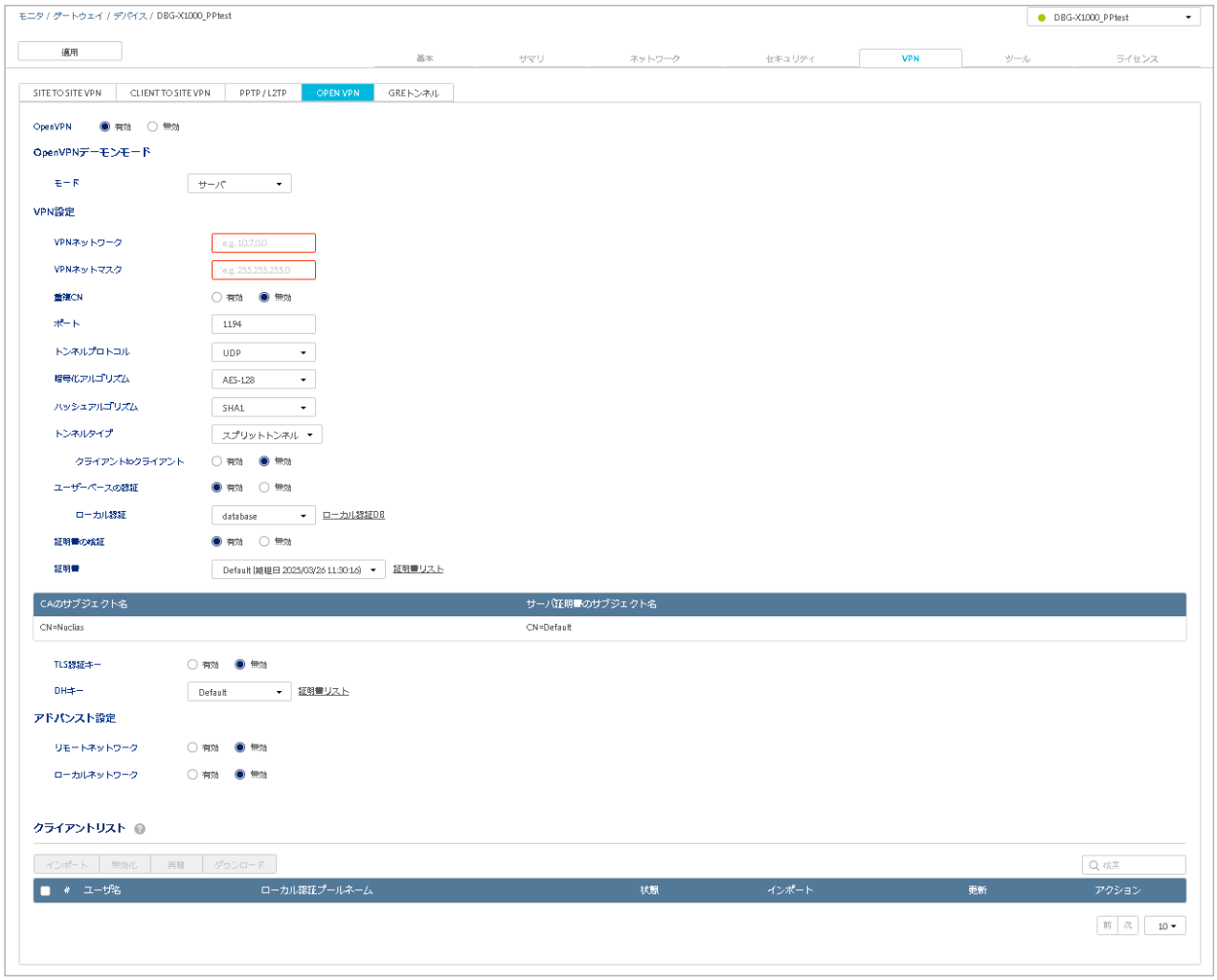


図 9-99　OPEN VPN（サーバモード）

本画面には以下の項目が含まれます。

項目	説明
OpenVPN	OpenVPN 機能を有効に設定します。
OpenVPN デーモンモード	
モード	モードを「サーバ」に設定します。 選択したモードによって、画面に表示される項目が異なります。
VPN 設定	
VPN ネットワーク	VPN の IP ネットワークを入力します。
VPN ネットマスク	ネットマスクを入力します。
重複 CN	有効にすると、複数のクライアントに同じ認証を使用することが可能になります。
ポート	使用するポート番号を入力します。初期値：1194
トンネルプロトコル	「UDP」または「TCP」を選択します。
暗号化アルゴリズム	暗号化方式を以下から選択します。 「AES-128」「BF-CBC」「AES-192」「AES-256」
ハッシュアルゴリズム	ハッシュアルゴリズムを以下から選択します。 「SHA1」「SHA256」「SHA512」
トンネルタイプ	トンネルタイプを以下から選択します。 • 「フルトンネル」：トンネルを通じてすべてのトラフィックをリダイレクトします。 • 「スプリットトンネル」：トンネルを通じて、事前定義されたクライアントルートに基づくプライベート LAN のみにトラフィックをリダイレクトします。
クライアント to クライアント	本項目は、「トンネルタイプ」で「スプリットトンネル」を選択した場合のみ表示されます。 有効を選択した場合、スプリットトンネルにおいて OpenVPN クライアント同士の相互通信が可能になります。
ユーザーベースの認証	ユーザ名 / パスワードを使用した追加の認証方式を有効化 / 無効化します。

項目	説明
ローカル認証	ローカルサーバに保存されている設定済みのローカル認証を選択します。 ローカル認証データベースの追加については「認証 - ローカル認証 DB」を参照してください。
証明書の検証	本項目を有効にした場合、クライアント証明書が必要になります。 無効にした場合、クライアントはユーザ名 / パスワードのみを使用して認証を行います。
証明書	ドロップダウンリストから証明書を選択します。
TLS 認証キー	有効にすると、認証のレイヤーを追加する TLS 認証が追加されます。 TLS キーがアップロードされている場合にのみ表示されます。初期値では無効です。
TLS キー	TLS 認証キーを有効にした場合、TLS キーを選択します。
DH キー	DH キーを選択します。
アドバンスト設定	
リモートネットワーク	リモートネットワーク機能の有効 / 無効を設定します。 有効に設定した場合は、追加表示された項目でリモートネットワークの設定を行います。
ローカルネットワーク	ローカルネットワーク機能の有効 / 無効を設定します。 有効に設定した場合は、追加表示された項目でローカルネットワークの設定を行います。 本項目は「トンネルタイプ」として「スプリットトンネル」を選択した場合に表示されます。

設定後、画面上部の「適用」をクリックします。

■ VPN - OPEN VPN（サーバモード）- クライアントリスト

「クライアントリスト」では、OpenVPN のクライアントの設定を行います。

次の画面には OpenVPN クライアントのリストが表示されます。
また、クライアントの詳細表示、インポート、無効化、再開、ダウンロードを実行できます。

図 9-100　OPEN VPN（サーバモード）- クライアントリスト

本画面には以下の項目が含まれます。

項目	説明
ユーザ名	クライアント名を表示します。
ローカル認証プールネーム	クライアントが属するローカル認証プールの名前を表示します。
状態	証明書のステータスを表示します。
インポート	ユーザの証明書が最初にインポートされた日時を表示します。
更新	ユーザの証明書が最後に更新された日時を表示します。
アクション	クライアントの詳細を表示できます。 クライアントのステータスが保留中の場合は、クライアントの詳細を表示することはできません。
インポート	クライアントリストをインポートします。
無効化	クライアントを無効にします。
再開	クライアントが無効化されている場合、「再開」をクリックしてクライアントを再開できます。
ダウンロード	選択した証明書をダウンロードします。

設定後、「保存」をクリックします。

■ VPN - OPEN VPN（サーバモード）- リモートネットワーク

「アドバンスト設定」で「リモートネットワーク」を有効にした場合は、リモートネットワークの設定を行います。
設定された IP アドレスは、OpenVPN トンネルを介してサーバにリモートでアクセスできます。

次の画面にリモートネットワークの設定が表示されます。設定の編集、削除、追加を実行できます。

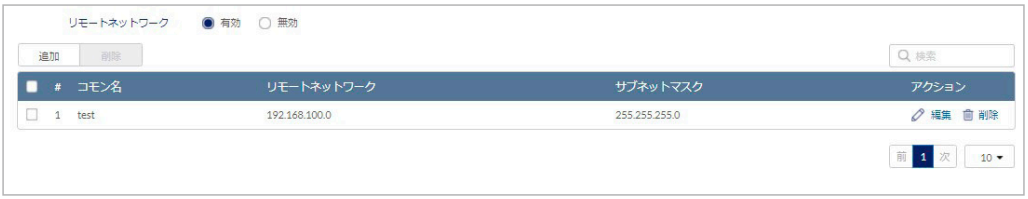


図 9-101　OPEN VPN（サーバモード）- リモートネットワーク

■ VPN - OPEN VPN（サーバモード）- openVPN リモートネットワークの追加

「追加」をクリックし、次の画面でリモートネットワークを追加します。

図 9-102　openVPN リモートネットワークの追加

本画面には以下の項目が含まれます。

項目	説明
コモン名	リモートネットワークの名前を入力します。
リモートネットワーク	リモートネットワークの IP アドレスを入力します。
サブネットマスク	リモートネットワークの IP アドレスのサブネットマスクを入力します。

設定後、「保存」をクリックします。

■ VPN - OPEN VPN（サーバモード）- ローカルネットワーク

OpenVPN のトンネルタイプに「スプリットトンネル」が選択されている場合にのみ設定できます。

本画面には設定された OpenVPN ローカルネットワークのリストが表示されます。
クライアントは、これらの設定済みローカルネットワークにのみアクセスできます。

次の画面にローカルネットワークの設定が表示されます。設定の編集、削除、追加を実行できます。

図 9-103　OPEN VPN（サーバモード）- ローカルネットワーク

■ VPN - OPEN VPN（サーバモード）- openVPN ローカルネットワークの追加

「追加」をクリックし、次の画面でローカルネットワークを追加します。

図 9-104　openVPN ローカルネットワークの追加

本画面には以下の項目が含まれます。

項目	説明
ローカルネットワーク	ローカルネットワークの IP アドレスを入力します。
サブネットマスク	ローカルネットワークの IP アドレスのサブネットマスクを入力します。

設定後、「保存」をクリックします。

VPN - OPEN VPN（クライアントモード）

OpenVPN のクライアントモード設定について説明します。

注意　OpenVPN クライアントとして OpenVPN Connect をサポートします。

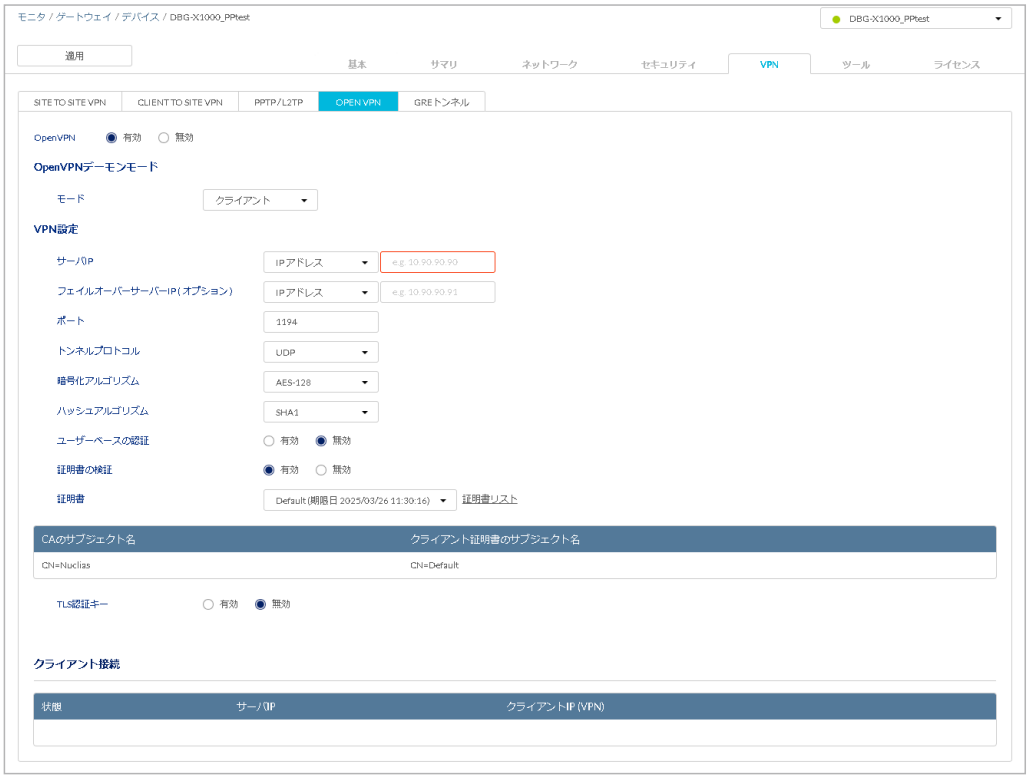


図 9-105　OPEN VPN（クライアントモード）

本画面には以下の項目が含まれます。

項目	説明
OpenVPN	OpenVPN 機能を有効に設定します。
OpenVPN デーモンモード	
モード	モードを「クライアント」に設定します。 選択したモードによって、画面に表示される項目が異なります。
VPN 設定	
サーバ IP	OpenVPN サーバの IP アドレス /FQDN を入力します。
フェイルオーバーサーバー IP（オプション）	フェイルオーバーメカニズムの識別子タイプを「IP アドレス」「FQDN」から選択します。 この機能を使用すると、クライアントに追加の OpenVPN サーバを設定できます。このサーバは、プライマリサーバがダウンしたときに使用されます。クライアントモードでのみ適用されます。
ポート	OpenVPN サーバ（またはアクセスサーバ）を実行するポート番号を入力します。
トンネルプロトコル	「TCP」または「UDP」を選択します。
暗号化アルゴリズム	暗号化方式を以下から選択します。 「AES-128」「BF-CBC」「AES-192」「AES-256」
ハッシュアルゴリズム	ハッシュアルゴリズムを以下から選択します。 「SHA1」「SHA256」「SHA512」
ユーザーベースの認証	ユーザ名 / パスワードを使用した追加の認証方式の有効 / 無効を指定します。初期値は無効です。
ユーザー名	本項目は「ユーザーベースの認証」を有効に設定した場合に表示されます。使用するユーザ名を入力します。
パスワード	「ユーザーベースの認証」を有効に設定した場合、使用するパスワードを入力します。

項目	説明
証明書の検証	本項目を有効に設定した場合、クライアント証明書が必要になります。 無効にした場合、クライアントはユーザ名 / パスワードのみを使用して認証を行います。
証明書	証明書を選択します。
TLS 認証キー	有効にすると、認証のレイヤーを追加する TLS 認証が追加されます。 TLS キーがアップロードされている場合にのみ有効化できます。初期値は無効です。
TLS キー	本項目は「TLS 認証キー」で有効を選択した場合に表示されます。使用する TLS キーを選択します。
クライアント接続	
状態	VPN の接続状態を表示します。
サーバ IP	クライアントが接続されているサーバの IP アドレスを表示します。
クライアント IP（VPN）	接続しているクライアントの IP アドレスを表示します。

設定後、画面上部の「適用」をクリックします。

VPN - GRE トンネル

● 画面の表示手順（デバイス設定時）：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**VPN**」タブ >「**GRE トンネル**」タブを選択

注意　以下はデバイス画面からのみ設定できます。プロファイル画面からは設定できません。

GRE（Generic Routing Encapsulation）は、トンネルプロトコルの 1 つです。パケットを別のプロトコルでカプセル化して伝送を行います。
GRE トンネルを作成すると、トンネルを介してマルチキャストパケットの送受信が可能となります。

以下の手順で GRE トンネルを確立します。
① GRE トンネルを作成します。
② GRE トンネルを使用して、リモートローカルネットワーク用のスタティックルートを設定します。

GRE トンネルを作成する場合、GRE トンネルのエンドポイントに固有の IP アドレスを設定します。
この IP アドレスは、もう一方のルータのスタティックルートでゲートウェイ IP アドレスとして参照されます。
「GRE トンネルの追加」画面の「リモート IP」には、エンドポイントルータの WAN IP アドレスを入力します。

GRE トンネル名に対して設定されたインターフェイスを使用し、ゲートウェイ上にスタティックルートを作成します。
スタティックルートの宛先 IP アドレスはリモート LAN のサブネットです。
スタティックルートのゲートウェイ IP アドレスは、終端ゲートウェイ（リモート LAN サブネットを管理しているゲートウェイ）の GRE トンネル IP になります。

次の画面に GRE トンネルの設定が表示されます。「稼働中」では設定の有効 / 無効を選択できます。
また、設定の追加、編集、削除を実行できます。

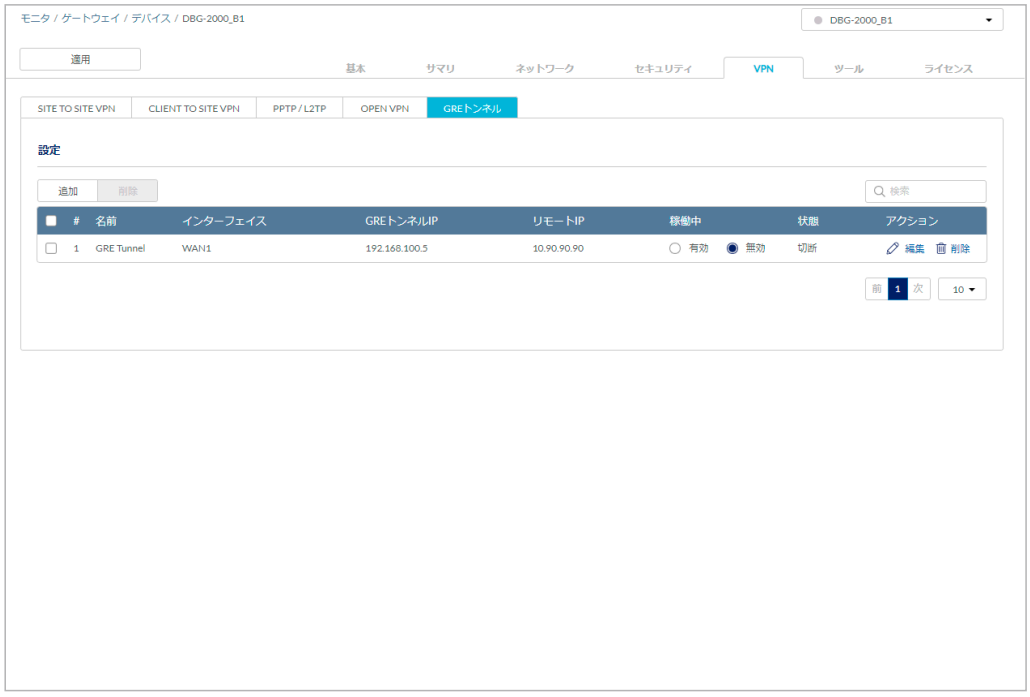


図 9-106 GRE トンネル

設定後、画面上部の「適用」をクリックします。

■ VPN - GRE トンネル - GRE トンネルの追加

「追加」をクリックし、次の画面で GRE トンネルを追加します。

図 9-107 GRE トンネルの追加

本画面には以下の項目が含まれます。

項目	説明
GRE トンネル名	GRE トンネルの名前を入力します。
インターフェイス	このトンネルを作成するインターフェイスを選択します。
IP アドレスタイプ	使用する IP アドレスの種類を選択します。
GRE トンネル IP	このエンドポイントの IP アドレスを選択します。
サブネットマスク	本項目は、「IP アドレスタイプ」に「IPv4」を選択した場合のみ表示されます。サブネットマスクを入力します。
リモート IP	エンドポイントゲートウェイの WAN IP アドレスを入力します。
スタティックルート設定	
IP アドレス	リモート LAN サブネットからのスタティックルートの宛先 IP アドレスを入力します。
サブネットマスク	本項目は、「IP アドレスタイプ」に「IPv4」を選択した場合のみ表示されます。サブネットマスクを入力します。
ゲートウェイ IP アドレス	終端となるゲートウェイ（リモート LAN サブネットを管理しているゲートウェイの GRE トンネル IP）の IP アドレスを入力します。

設定後、「保存」をクリックします。

「ツール」タブ

● 画面の表示手順：**設定 > ゲートウェイ > デバイス** 画面でデバイスを選択 →「**ツール**」タブを選択

以下では、デバイスと Nuclias の接続の確認と、デバイスの再起動について説明します。
診断ツール（「PING」「TRACEROUTE」）を使用して、デバイスの接続性、接続経路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。

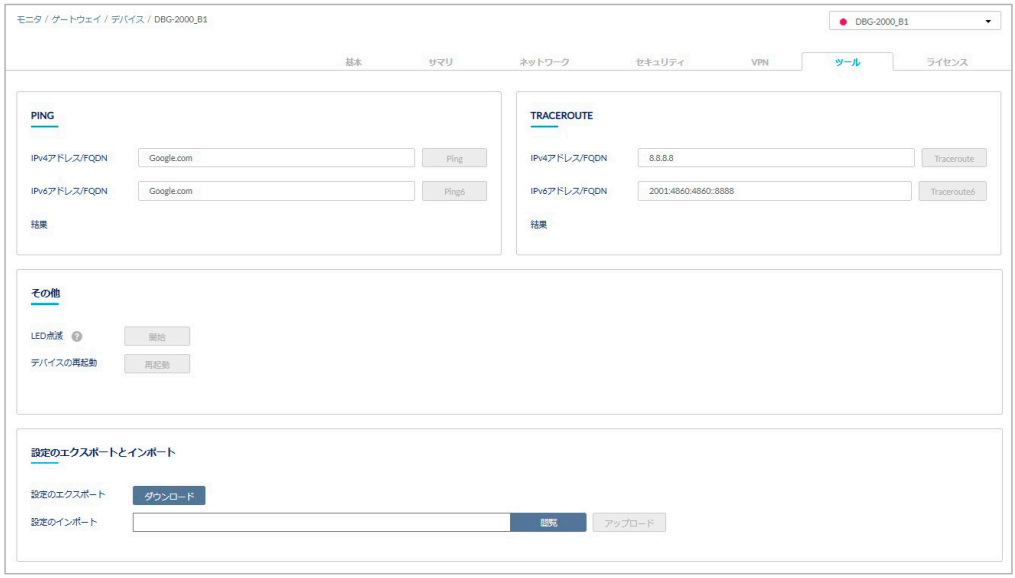


図 9-108　ツール

本画面には以下の項目が含まれます。

項目	説明
PING	接続性を確認する宛先デバイスの IP アドレスまたはドメイン名を入力し、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。 • IPv4 アドレスに Ping を実行する場合： 「IPv4 アドレス /FQDN」に IPv4 アドレスまたはドメイン名を入力し、「Ping」をクリックします。 • IPv6 アドレスに Ping を実行する場合： 「IPv6 アドレス /FQDN」に IPv6 アドレスまたはドメイン名を入力し、「Ping6」をクリックします。 注意 「PING」または「TRACEROUTE」診断ツールを使用する場合、DBG-2000/DBG-X1000 と接続するルータやファイアウォール側で、事前に「ICMP プロトコル」の使用を許可してください。
TRACEROUTE	経路を確認する宛先デバイスの IP アドレスまたはドメイン名を入力し、トレースルートを実行します。 • IPv4 アドレスにトレースルートを実行する場合： 「IPv4 アドレス /FQDN」に IPv4 アドレスまたはドメイン名を入力し、「Traceroute」をクリックします。 • IPv6 アドレスにトレースルートを実行する場合： 「IPv6 アドレス /FQDN」に IPv6 アドレスまたはドメイン名を入力し、「Traceroute6」をクリックします。 注意 「PING」または「TRACEROUTE」診断ツールを使用する場合、DBG-2000/DBG-X1000 と接続するルータやファイアウォール側で、事前に「ICMP プロトコル」の使用を許可してください。
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。 ● 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。
設定のエクスポートとインポート	● 設定のエクスポート 「ダウンロード」をクリックすると、設定の内容を CSV 形式でダウンロードできます。 ● 設定のインポート 「閲覧」をクリックし、CSV ファイルを選択します。「アップロード」をクリックすると、設定の内容をインポートできます。

「ライセンス」タブ

● 画面の表示手順：**設定** > **ゲートウェイ** > **デバイス** 画面でデバイスを選択 →「**ライセンス**」タブを選択

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 9-109「ライセンス」タブ

本画面には以下の項目が含まれます。

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 9-110　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 Nuclias ゲートウェイに 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 Nuclias ゲートウェイに 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 Nuclias ゲートウェイから除外し、別の Nuclias ゲートウェイ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。

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 > 認証サーバを選択します。

図 9-111　認証 - 認証サーバ

本画面には以下の項目が含まれます。

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。 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

1. 「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。
2. 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」
3. 「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。
次の画面で「タイプ」「サーバ名」「IP アドレス」を指定します。

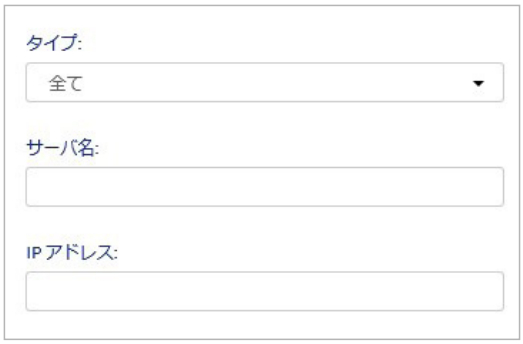


図 9-112　認証サーバの検索

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. 次の画面で設定を行います。

図 9-113　RADIUS サーバの追加

本画面には以下の項目が含まれます。

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」
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。
アカウンティング interim 間隔	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、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。

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. 次の画面で設定を行います。

図 9-114　LDAP サーバの追加

本画面には以下の項目が含まれます。

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。

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. 次の画面で設定を行います。

図 9-115　POP3 サーバの追加

本画面には以下の項目が含まれます。

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。

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. 次の画面で設定を行います。

図 9-116　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含まれます。

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。

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. 次の画面で設定を行います。

図 9-117　NT ドメインサーバの追加

本画面には以下の項目が含まれます。

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

キャプティブポータル ローカルデータベース認証の設定を行います。
キャプティブポータル ローカル DB 認証を有効にすると、以下で設定した「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。

設定 > 認証 > ローカル認証 DB を選択します。

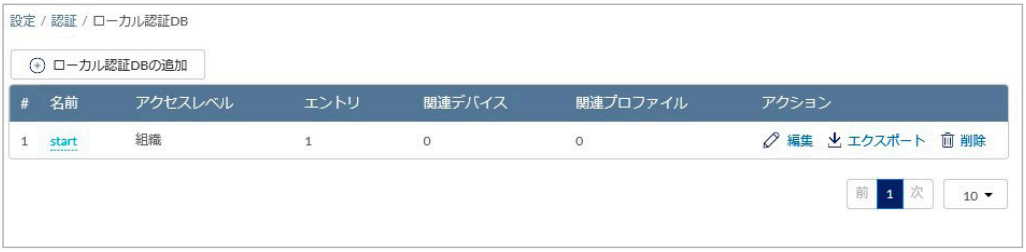


図 9-118　認証 - ローカル認証 DB

本画面には以下の項目が含まれます。

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	データベースの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。 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、次の画面を表示します。

図 9-119　ローカル認証 DB の追加

2. 以下の項目を入力します。

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. 次の画面で「ユーザ名」「パスワード」を編集します。

図 9-120　ローカル認証 DB の編集

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　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

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・管理を行います。
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、次の画面を表示します。

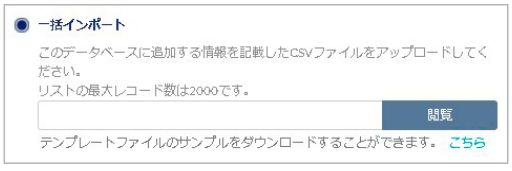
図 9-121　MAC ACL

■ MAC ACL の追加

1. 「MAC ACL の追加」をクリックし、次の画面を表示します。

図 9-122　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。
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。 

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. 次の画面で「MAC アドレス」「ユーザ名」を設定します。エントリを削除する場合は「アクション」欄のごみ箱アイコンをクリックします。

図 9-123　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 > 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 MAC 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 > 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。

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「ネットワーク - キャプティブポータル」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。
次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 9-124　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、次の画面を表示します。

図 9-125　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。
   エントリを削除する場合は「アクション」欄の「削除」をクリックします。

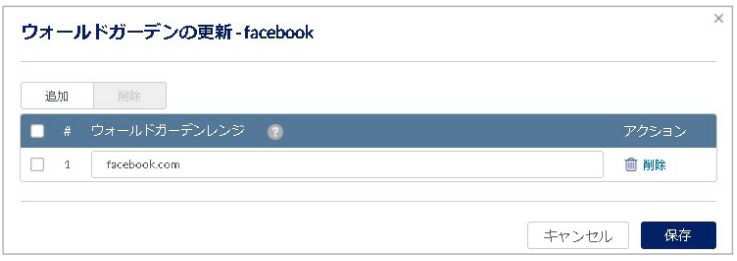


図 9-126　ウォールドガーデンの更新

2. 設定後、「保存」をクリックします。

■ **ウォールドガーデンの削除**

1. **設定 > 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、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 9-127　設定 - スケジュールポリシー

本画面には以下の項目が含まれます。

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。
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。 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、次の画面を表示します。

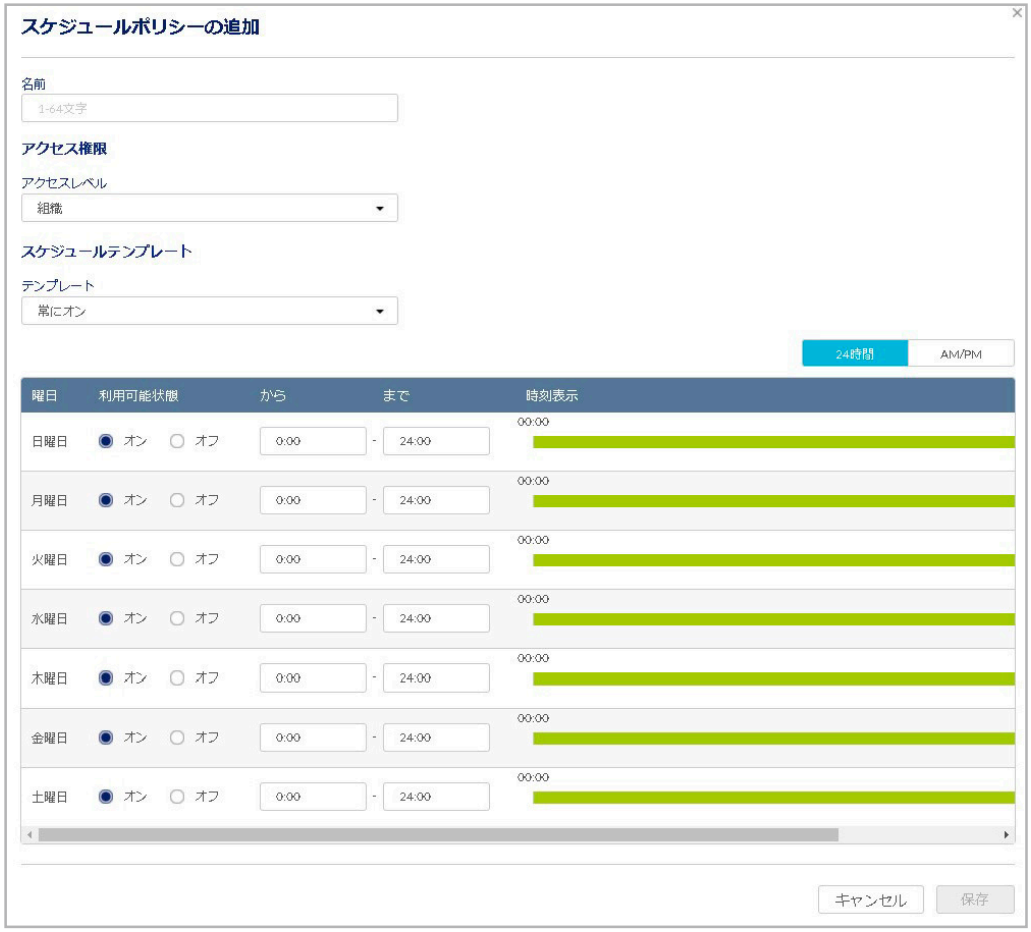


図 9-128　スケジュールポリシーの追加

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。

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　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。

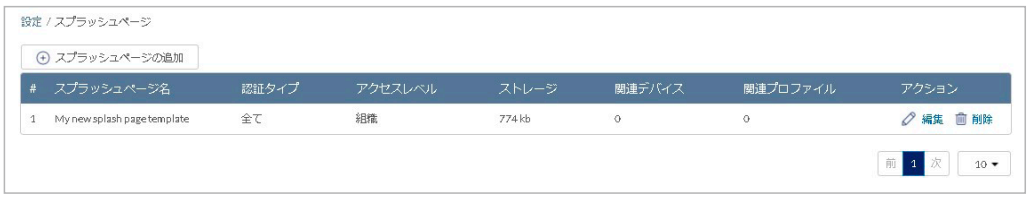


図 9-129　スプラッシュページ

■ 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、次の画面を表示します。

図 9-130　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」「サイトタグ」「サイト」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. 「テンプレート」を選択した場合は「次」、「従来の HTML」を選択した場合は「保存」をクリックし、表示される画面で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「削除」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 9-131　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含まれます。

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 9-132　スプラッシュページ編集（テンプレート）の例

● 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ーの警告ページも選択できます。

図 9-133　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 9-134　複数言語の追加

本画面には以下の項目が含まれます。

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 10 章　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。

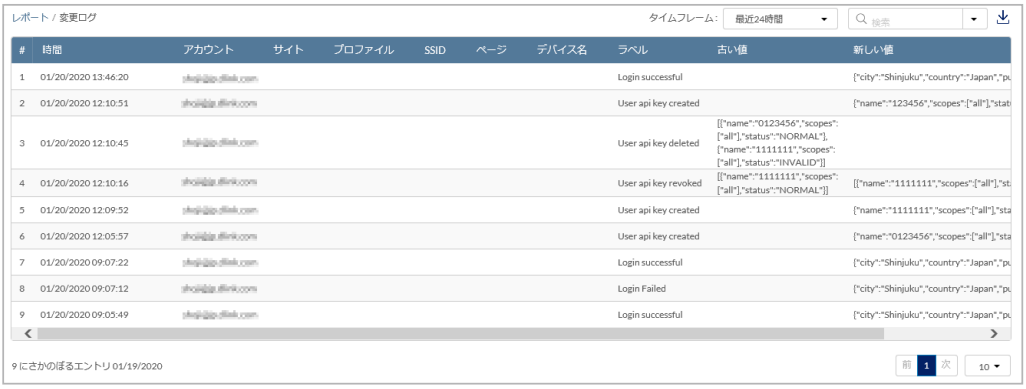


図 10-1　変更ログ

■ 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。 DBG-X1000 の場合、関連するプロファイルはありません。
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。レポートは E メールで送信できます。また、送信スケジュールを指定してレポートを送信することもできます。

レポート > サマリレポートを選択してください。

図 10-2　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	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。

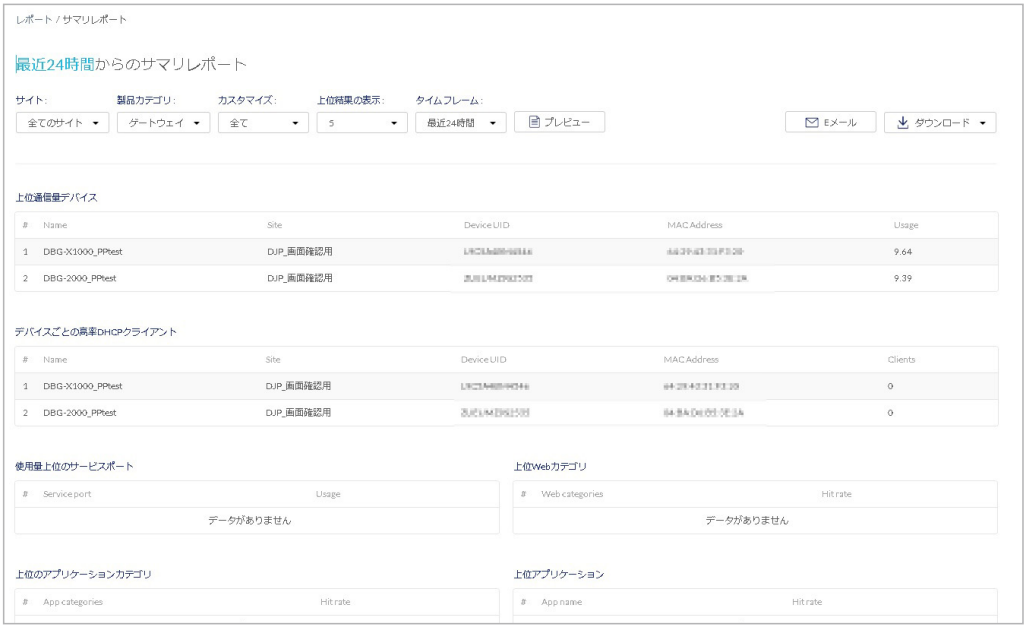


図 10-3　サマリレポート（プレビュー）- ゲートウェイ

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 10-4　アラート

各情報の詳細は下記の通りです。

項目	説明
重大性	アラートの重大性を「警告」「重大」「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 10-5　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	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 11 章　管理

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 11-1　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	ユーザ名が表示されます。クリックして接続レベル、権限の変更ができます。 ただし自身のユーザ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ています。 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。

図 11-2　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。
閲覧者	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、次の画面を表示します。

図 11-3　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 Nuclias 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 11-4　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、次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。

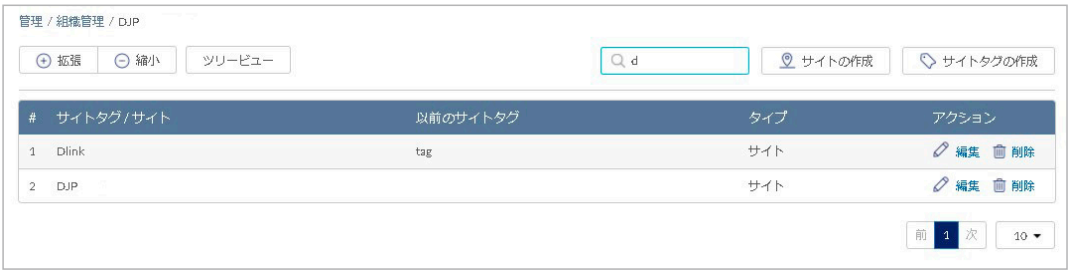


図 11-5　組織管理 - 検索

■ 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、次の画面を表示します。

図 11-6　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、次の画面を表示します。

図 11-7　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の 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. 「保存」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、次の画面を表示します。

図 11-8　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. 「組織」欄の組織名をクリック後、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 11-9　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. 次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。

図 11-10　サイトの編集

図 11-11　サイトタグの編集

3. 設定後、「適用」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 11-12　ライセンス管理（概要）

本画面には「概要」「デバイス」「ライセンス」「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 - 概要」「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 - 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 - 概要

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 11-13　ライセンス管理（概要）

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 11-14　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、次の画面を表示します。

図 11-15　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、次の画面を表示します。

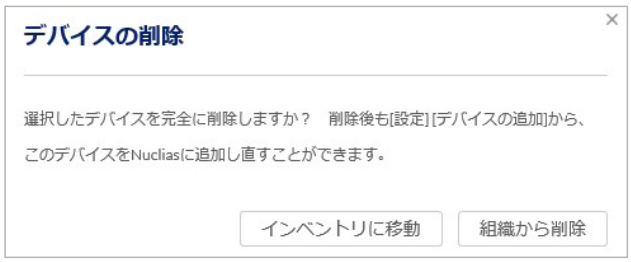


図 11-16　デバイスの削除

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 8 章 モニタ「ゲートウェイ - 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. 次の画面で「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。

図 11-17　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の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。

■ 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。
   次の画面では 2 つのデバイスを選択しています。

図 11-18　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、次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ため、「残り 3」と表示されます。

図 11-19　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。

図 11-20　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 11-21　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 > ゲートウェイ > デバイス**画面、または**設定 > ゲートウェイ > 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 11-22　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	ライセンスの使用状態を表示します。 ・「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。

■ ライセンスヒストリの表示

「ライセンスヒストリ」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 形式でダウンロードできます。

■ 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。

図 11-23　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。
次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。

図 11-24　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。

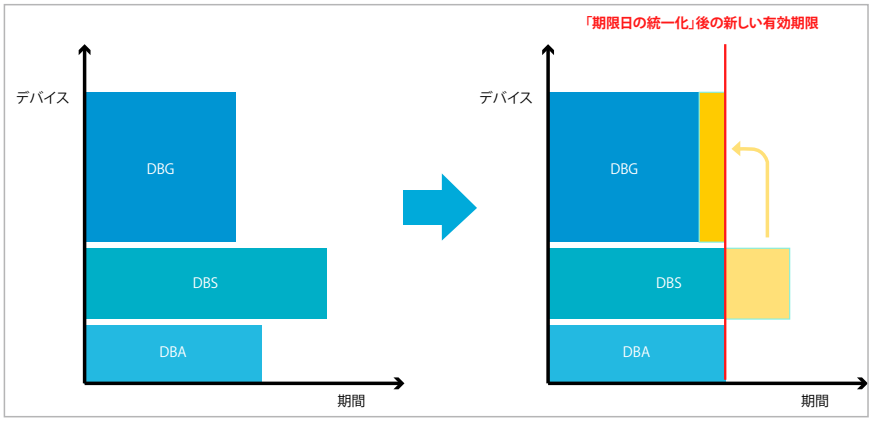


図 11-25 「期限日の統一化」の仕組み

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 11-26　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 11-27　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。

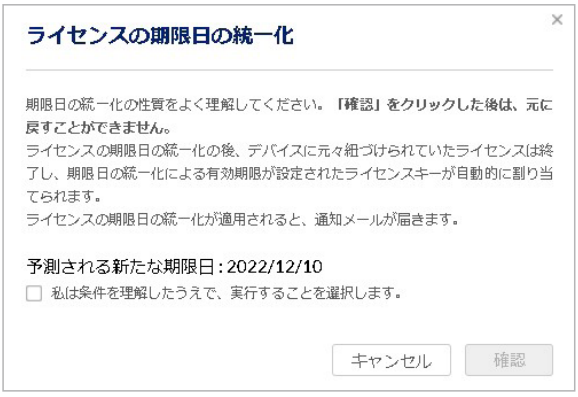


図 11-28　ライセンス期限の計算

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（ウエイト）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

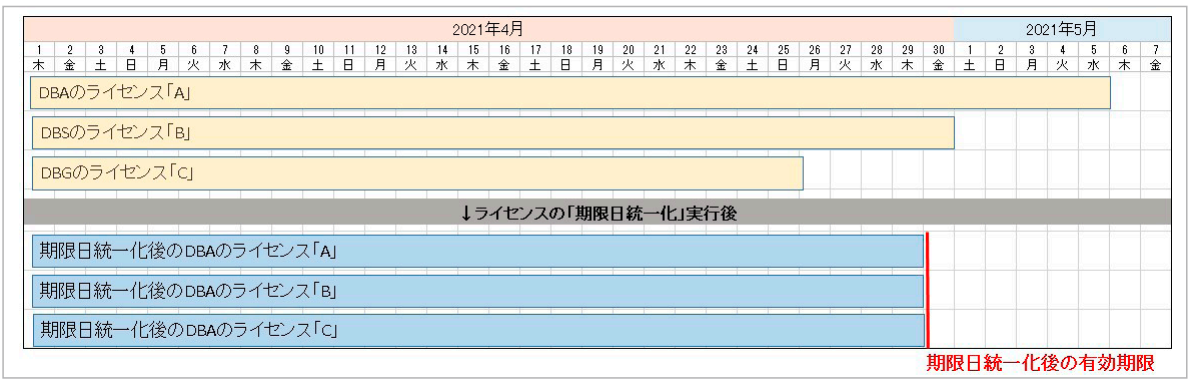


図 11-29　ライセンス期限統一化の例

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 シリーズの 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 シリーズ (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 シリーズの数）× 5（DBG の比重）＝ 1745

デバイスの比重の合計（計算手順の 5）：

(2 DBA x 2) + (1 DBG x 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 11-30　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。
Details	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 形式でダウンロードできます。

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　「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 > インベントリを選択し、次の画面を表示します。

図 11-31　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」
- 「ファームウェアアップグレード」
- 「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

デバイスのモデル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 11-32　ファームウェア

ファームウェア - 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 11-33　ファームウェア - 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	管理デバイスの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当該デバイス一覧が表示されます。
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。
自動アップグレード	ファームウェアの自動アップグレードについて、有効 / 無効を表示します。
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「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、次の画面でスケジュールを設定します。

図 11-34　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。

図 11-35　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。

ファームウェア - ファームウェア管理タブ

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 11-36　ファームウェア - 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 Excel 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。
指定したイベントが発生した場合、図 10-4「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。

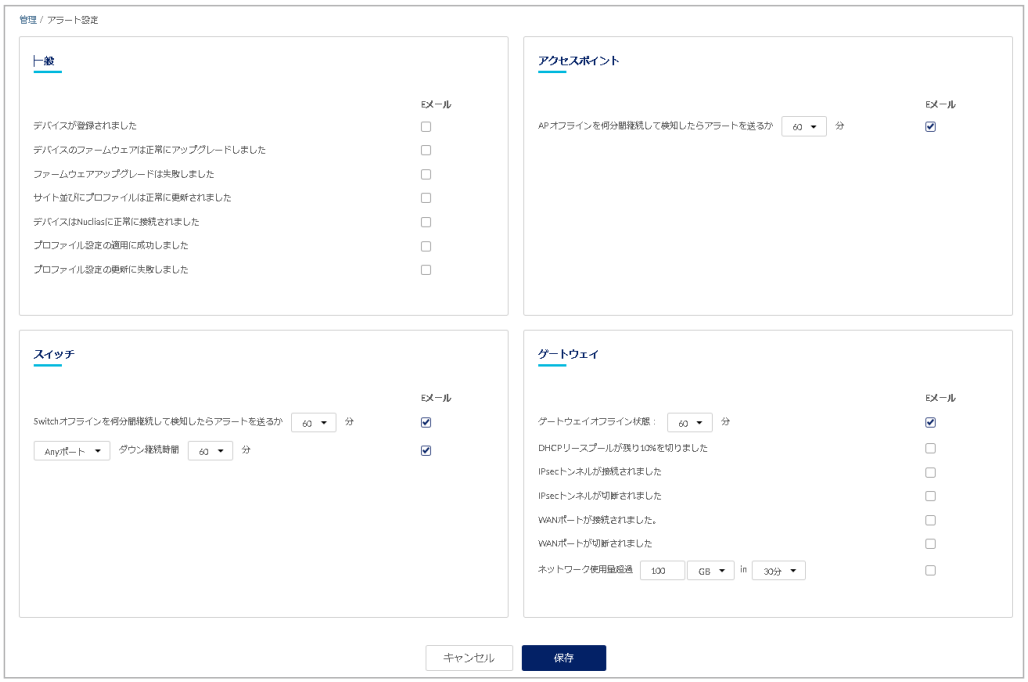


図 11-37　アラート設定

本画面には以下の項目があります。

アラート設定（一般）

項目	説明
デバイスが登録されました	デバイスが Nuclias クラウド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	デバイスへプッシュ設定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	デバイスへのプッシュ設定が失敗した際にアラートを発報します。

アラート設定（ゲートウェイ）

項目	説明
ゲートウェイオフライン状態	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。プルダウンより、「5」「10」「15」「30」「60 」（単位：分）から指定できます。 本製品が実際に 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。 例：本項目で「10 分」と設定した場合、実際に本製品が Nuclias から切断されてからアラートが送信されるにはおよそ 15 分以上かかります。
DHCP リースプールが残り 10% を切りました	DHCP リースプールが 10%以下になった場合にアラートを発報します。
IPsec トンネルが接続されました	IPsec トンネルが接続された場合にアラートを発報します。
IPsec トンネルが切断されました	IPsec トンネルが切断された場合にアラートを発報します。
WAN ポートが接続されました	WAN ポートが接続された場合にアラートを発報します。
WAN ポートが切断されました	WAN ポート切断された場合にアラートを発報します。
ネットワーク使用量超過	ネットワーク使用量が設定した量を超過した場合にアラートを発報します。 ネットワークの使用量、単位、時間を指定します。

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。

証明書の管理

管理 > 証明書の管理を選択し、証明書の設定、管理を行う画面を表示します。

図 11-38　証明書の管理

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	証明書とキーのコモンネームを表示します。
コンテンツ	エントリに含まれるコンテンツの種類を表示します。
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	ローカルユーザ証明書の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。

注意　ローカルユーザ証明書は削除できません。

■ 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、次の画面を表示します。

図 11-39　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 Key」「TLS Key」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。

図 11-40　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）の証明書 / 秘密鍵のファイル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、次の画面で SAML の設定を行います。

図 11-41　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、次の画面を表示します。

図 11-42　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、次の画面を表示します。

図 11-43　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」「閲覧者」「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 > アドバンスト設定 > 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 • roleName：Nuclias の**管理 > アドバンスト設定 > 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、次の画面で SMS の設定を行います。

図 11-44　SMS 設定

■ Twilio SMS 設定の追加

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

図 11-45　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いけない時間（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。
許可済電話局番	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。

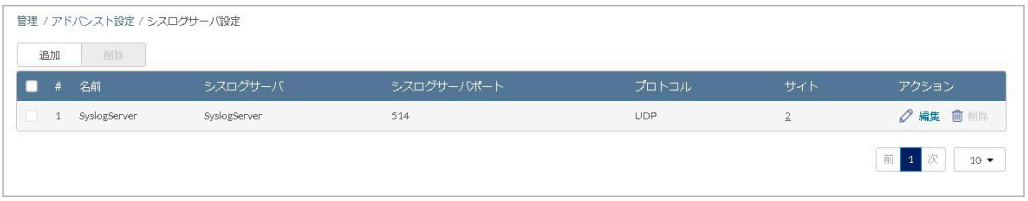


図 11-46　シスログサーバ設定

■ 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**の画面で「追加」をクリックし、次の画面を表示します。

図 11-47　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. 「適用」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**の画面で、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、「適用」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**の画面で、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、次の画面でデバイスを表示します。

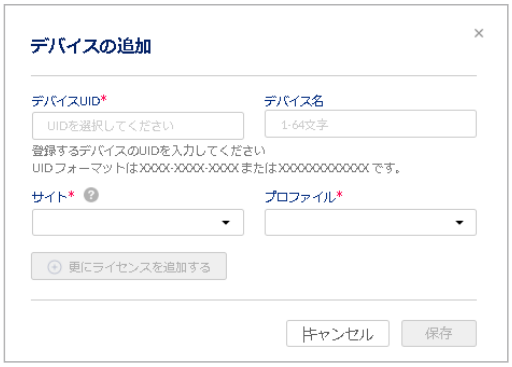


図 11-48　デバイスの追加

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。  **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、次の画面を表示します。

図 11-49　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 12 章　ヘルプ

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。本画面は英語表示のみです。

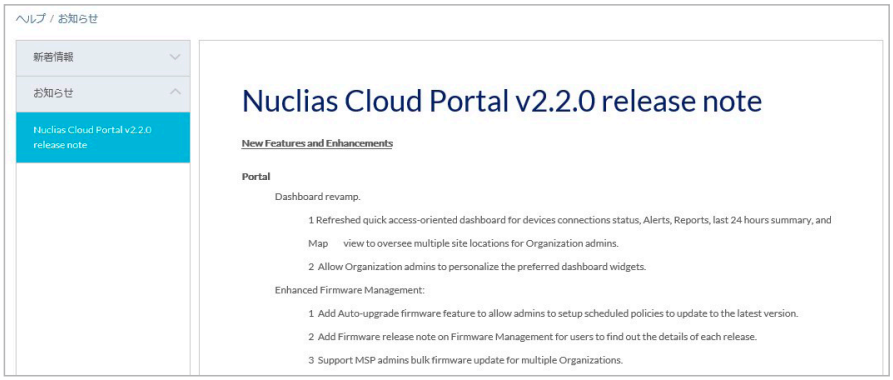


図 12-1　お知らせ

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 12-2　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。 • 選択肢：「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」 「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 2 MB 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 12-3　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。

付録

付録 A　ライセンスの適用や開始等に関する詳細

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。

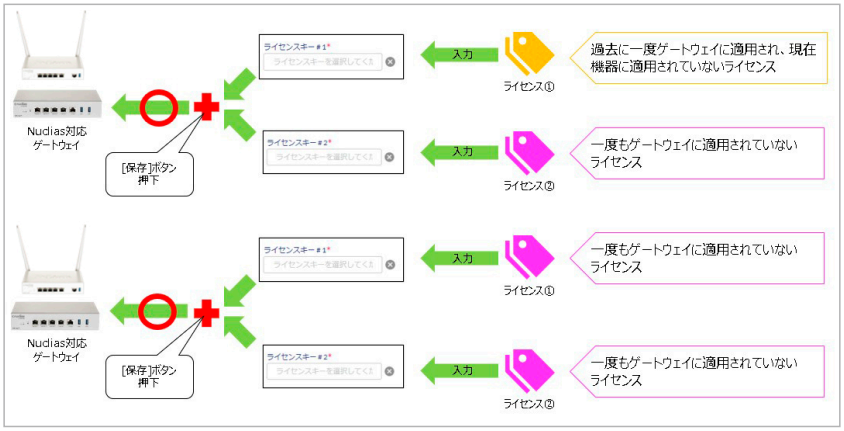
■ ライセンスを複数適用する場合

1 台のデバイスに複数のライセンスを適用する場合、適用した順に #1、#2、・・・と番号が割り振られ、#1 から順に使用されます。
#2 以降のライセンスは、それより若い番号のライセンスが全て消費されるか手動で解除された後にはじめて使用開始されます。
例えば以下のような場合、ライセンスキー「QST・・・」が先に使用されます。

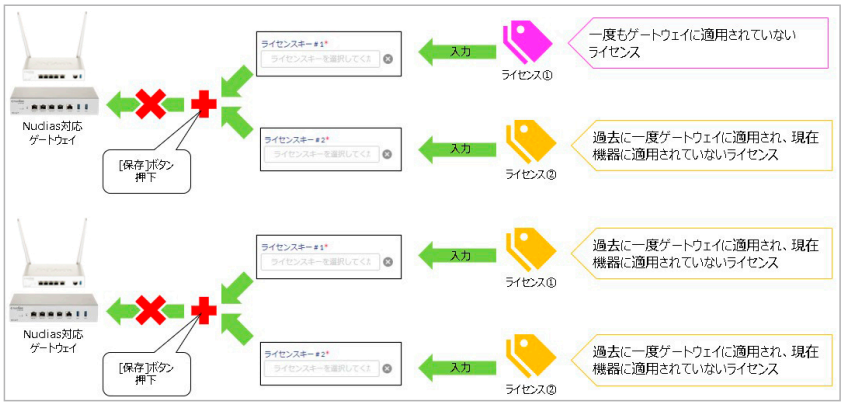
図 13-1　デバイス追加画面

また、「以前デバイスに適用して使用開始したが、現在はデバイスに適用されていないライセンス」は、「ライセンスキー #1」にのみ入力できます。

同時に適用できるライセンスの組み合わせ：



同時に適用できないライセンスの組み合わせ：



■ **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 > ゲートウェイ > 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=XXXXXx xxxxXXXXXxxxxxXXXXXxxxxx==&otp=XXXXXxxxxxXXXXXxxxxxXXXXXxxxxx 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 Nuclias ゲートウェイ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 Nuclias ゲートウェイ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。