

D-Link DNH-100
Nuclias Connect Hub

..... ユーザマニュアル

安全にお使いいただくために

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

安全上のご注意

必ずお守りください

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

 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 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 ぬれた手でさわらない
感電の原因となります。 |  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 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 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 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 電子レンジ、IH 調理器などの加熱調理機、圧力釜など高压容器に入れたり、近くに置いたりしない
火災、やけど、けが、感電、故障の原因となります。 |
|  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。 | |

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。 |  指示 ガソリンスタンドなど引火性ガスが発生する可能性のある場所や粉じんが発生する場所に立ち入る場合は、必ず事前に本製品の電源を切る
引火性ガスなどが発生する場所で使用すると、爆発や火災の原因となります。 |
|  禁止 発煙、焦げ臭い匂いの発生などの異常状態のまま使用しない
感電、火災の原因となります。
使用を止めて、ケーブル/コード類を抜いて、煙が出なくなつてから販売店に修理をご依頼ください。 |  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。 |
|  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。 |  指示 無線製品は病院内で使用する場合は、各医療機関の指示に従って使用する
電子機器や医療電気機器に悪影響を及ぼすおそれがあります。 |
|  禁止 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。 |  禁止 本製品の周辺に放熱を妨げるようなもの（フィルムやシールでの装飾を含む）を置かない
火災、または故障の原因となります。 |
|  指示 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。 |  指示 耳を本体から離してご使用ください
大きな音を長時間連続して聞くと、難聴などの耳の障害の原因となります。 |
|  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。 |  指示 無線製品をご使用の場合、医用電気機器などを装着している場合は、医用電気機器メーカーもしくは、販売業者に、電波による影響について確認の上使用する
医療電気機器に悪影響を及ぼすおそれがあります。 |
|  禁止 ケーブル/コード類や端子を破損させない
無理なねじり、引っ張り、加工、重いもの下敷きなどは、ケーブル/コードや端子の破損の原因となり、火災、感電、または故障の原因となります。 |  指示 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
電子機器が誤動作するなど、悪影響を及ぼすおそれがあります。 |
|  指示 本製品付属の AC アダプタもしくは電源ケーブルを指定のコンセントに正しく接続して使用する
火災、感電、または故障の原因となります。 |  指示 ディスプレイ部やカメラのレンズを破損した際は、割れたガラスや露出した端末内部に注意する
破損部や露出部に触れると、やけど、けが、感電の原因となります。 |
|  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。 |  指示 ペットなどが本機に噛みつかないように注意する
火災、やけど、けがなどの原因となります。 |
|  禁止 各種端子やスロットに導電性異物（金属片、鉛筆の芯など）を接触させたり、ほごりが内部に入ったりしないようにする
火災、やけど、けが、感電または故障の原因となります。 |  禁止 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 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。 |  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。抜かずに行くと、火災、やけど、感電または故障の原因となります。
-  SD や MicroSD カード、USB メモリの使用中は、カードやメモリを取り外したり、本製品の電源を切ったりしない。データの消失、機器本体の故障の原因となります。
-  磁気カードや磁気を帯びたものを本製品に近づけない。磁気カードのデータが消えてしまうおそれもしくは機器本体の誤作動の原因となります。
-  ディーリンクジャパンが販売している無線機器は国内専用のため、海外で使用しない。海外では国によって電波使用制限があるため、本製品を使用した場合、罰せられる場合があります。海外から持ち込んだディーリンク製品や並行輸入品を日本国内で使用する場合も同様に、罰せられる場合があります。

注意

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

電波障害自主規制について

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

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

ご使用上の注意

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

- マニュアルなどに記載されている以外の方法での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製品ラベルや認証ラベルをはがさないでください。はがしてしまうとサポートを受けられなくなります。

静電気障害を防止するために

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

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

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

電源の異常

万一停電などの電源異常が発生した場合は、必ず本スイッチの電源プラグを抜いてください。また、計画停電などが予定されている場合には、事前に本スイッチの電源プラグを抜いてください。電源が再度供給できる状態になってから電源プラグを再度接続します。

このたびは、弊社製品をお買い上げいただきありがとうございます。

本書は、製品を正しくお使いいただくための取扱説明書です。

必要な場合には、いつでもご覧いただけますよう大切に保管してください。

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

製品保証規定は以下を参照ください。

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

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

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

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

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

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

目次

安全にお使いいただくために.....	2
ご使用上の注意.....	4
静電気障害を防止するために.....	4
電源の異常.....	4
本マニュアルの対象者.....	8
表記規則について.....	8
製品名 / 品番について.....	8
第 1 章 本製品のご利用にあたって	9
パッケージの内容.....	9
システム要件.....	9
サポートする機能.....	9
Nuclias Connect 対応機器.....	10
外観について.....	10
前面パネル.....	10
背面パネル.....	10
LED 表示.....	11
第 2 章 機器の設置	12
ネットワーク接続前の準備.....	12
19 インチラックへの取り付け.....	12
ブラケットの取り付け.....	12
19 インチラックにスイッチを取り付ける.....	13
第 3 章 機器の接続	14
コントローラへの接続.....	14
イーサネット経由で接続する.....	14
コンソール経由で接続する (簡易設定のみ).....	15
第 4 章 Nuclias Connect の管理インタフェース	16
Nuclias Connect への接続.....	16
Nuclias Connect 設定ウィザード.....	18
Nuclias Connect 設定ウィザード (初回ログイン時).....	18
Nuclias Connect 設定ウィザード.....	19
ユーザプロフィール.....	22
個人情報.....	22
セキュリティ.....	22
管理インタフェースからのログアウト.....	22
第 5 章 ダッシュボード	23
第 6 章 モニタ	24
アクセスポイント.....	24
アクセスポイント - デバイス詳細.....	25
アクセスポイント - ワイヤレスクライアント.....	26
接続しているクライアント.....	26
ブロックされたクライアント.....	27
アクセスポイント - 隣接 AP.....	28
スイッチ.....	29
スイッチ - デバイス詳細.....	30
基本タブ.....	30
ポートタブ.....	34
IP インタフェースタブ.....	38
ルーティングタブ.....	39
電源タブ.....	40
ツールタブ.....	41
スイッチ - スイッチクライアント.....	44
スイッチ - スイッチポート.....	45
第 7 章 トポロジ	48
第 8 章 フロア計画	51
第 9 章 設定	53
プロフィールの作成.....	53

ネットワークの追加	54
プロファイル設定	56
アクセスポイント - SSID	57
アクセスポイント - VLAN	68
アクセスポイント - 帯域幅の最適化	70
アクセスポイント - RF 最適化	71
アクセスポイント - スケジュール	72
アクセスポイント - デバイス設定	73
アクセスポイント - パフォーマンス設定	74
アクセスポイント - WLAN パーティション	76
アクセスポイント - ワイヤレスリソース	78
スイッチ - 一般 - RADIUS サーバ	81
スイッチ - 一般 - 時間プロファイル	82
スイッチ - 基本	83
スイッチ - IPv4 ACL	88
スイッチ - アクセスポリシー	89
スイッチ - ポート設定	90
スイッチ - SNMP 設定	91
ファームウェアの更新	92
SSL 証明書	93
決済代行システム ※本項目は日本ではサポート対象外となります。	94
第 10 章 レポート	95
アクセスポイントのレポート	95
ピークネットワークアクティビティ	95
時間別ネットワークアクティビティ	96
日別ネットワークアクティビティ	97
最もアクティブな AP	98
スイッチのレポート	99
時間別ネットワークアクティビティ	99
日別ネットワークアクティビティ	100
トップランキング	101
第 11 章 ログ	102
デバイスシスログ	102
システムイベントログ	103
デバイスログ	104
監査ログ	105
アラート	106
第 12 章 システム管理	107
デバイス管理	107
ユーザ管理	108
ユーザステータス	108
ユーザ権限	109
設定	110
一般	110
接続	112
SMTP	113
バックアップ & リストア	114
ファームウェアアップグレード	116
システム設定	117
REST API	118
シングルサインオン (SSO)	119
アラート	122
FOTA	123
リソース	123
Nuclias Connect について	124
【付録 A】 機能別サポート製品 / バージョンについて	125
【付録 B】 Nuclias Connect アプリのセットアップ	127
ネットワークプロファイルのエクスポート	127
Nuclias Connect アプリケーションを使用した AP の検出と設定	128
ネットワークプロファイルの削除	137

本マニュアルの対象者

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

表記規則について

本項では、本マニュアル中での表記方法について説明します。

注意 注意では、使用にあたっての注意事項について説明します。

警告 警告では、ネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

補足 補足では、特長や技術についての詳細情報について説明します。

参照 参照では、別項目での説明へ誘導します。

表1に、本マニュアル中での字体・記号についての表記規則を表します。

表1 字体・記号の表記規則

字体・記号	解説	例
「」	メニュータイトル、ページ名、ボタン名。	「Submit」ボタンをクリックして設定を確定してください。
青字	参照先。	" ご使用になる前に " (13 ページ) をご参照ください。

製品名 / 品番について

本製品の「製品名 / 品番」について一覧を記載します。

■製品名 / 品番一覧

製品名	品番
DNH-100	DNH-100/A1

第1章 本製品のご利用にあたって

- パッケージの内容
- システム要件
- サポートする機能
- Nuclias Connect 対応機器
- 外観について
- LED 表示

パッケージの内容

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

- 本体
- AC 電源ケーブル（100V 用）
- ラックマウントキット
- 壁掛けキット
- ゴム足
- クイックインストールガイド
- GNU GPL ライセンスノート
- PL シート
- 16GB microSD カード

万一、不足しているものや損傷を受けているものがありましたら、ご購入頂いた販売代理店までご連絡ください。

システム要件

コンピュータ要件

- オペレーティングシステム：Windows、macOS、Linux
- イーサネット接続

ブラウザ要件

- Microsoft Edge、Safari、Firefox、Google Chrome

サポートする機能

- AP 集中管理
- プロファイル設定
- モニタ / 統計レポート
- 日本語 GUI
- 最大 100 台までの AP 管理
- サーバ・クライアント型
- チャンネル・出力自動調整
- Syslog サーバ^{※1}
- 外部 Syslog サーバ^{※2}
- Web ベースデザイン

※1 本機が管理しているデバイスから送信されるログを受信する Syslog サーバとしての機能となります。

※2 キャプティブポータルログのみ対応

Nuclias Connect 対応機器

Nuclias Connect では以下のアクセスポイントの管理をサポートしています。

製品名	品番	ファームウェアバージョンの最小要件*
DAP-X2850	DAP-X2850/A1	R1.10r027
DAP-X2810	DAP-X2810/A1	R1.20r032
DAP-2680	DAP-2680/A1	R2.00B08r051
DAP-2610	DAP-2610/A1	R2.01B05r073
DAP-3666	DAP-3666/A1	R1.10b08r068

外観について

前面パネル

前面パネルには、以下のコンポーネントと LED が搭載されています。

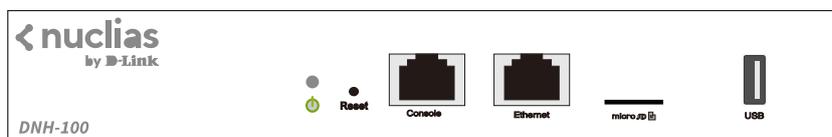


図 1-1 DNH-100 の前面パネル図

コンポーネント	説明
Reset ボタン	電源をオフ、または工場出荷時の設定にリセットします。工場出荷時の設定にリセットするには、Reset ボタンを 6 秒間押下します。
Console (RJ-45) ポート	CLI 管理用の RJ-45 コンソールポートです。RJ-45 コンソールケーブルを使用して接続します。
10BASE-T/100BASE-TX/1000BASE-T ポート	LAN 接続用のギガビット RJ-45 ポートです。
microSD スロット	microSD カードスロットです。(最大 32GB)
USB ポート	USB 3.0 Type-A ポートです。

LED については、「[LED 表示](#)」の項で詳細な動作について説明します。

補足 microSD は FAT32 フォーマットのみサポートされています。

注意 電源を入れたまま microSD カードを抜くと、カードが破損する可能性があります。

注意 電源ケーブルの抜き差しによるシャットダウンを行うと、microSD カードのアンマウント処理が適切に行われず、可能性があります。「[システム設定](#)」を参照して WebUI からシャットダウンを実施してください。

背面パネル

前面パネルには、AC 電源コネクタとセキュリティロックが配置されています。



図 1-2 DNH-100 の背面パネル図

LED 表示

前面パネルには、電源とネットワークの状態を示す LED を搭載しています。

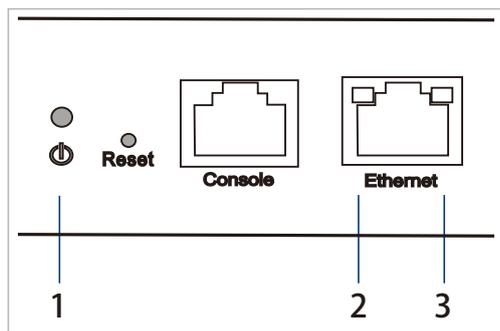


図 1-3 DNH-100 の LED 配置図 (前面パネル)

以下の表にスイッチの LED の状態が意味するスイッチの状態を示します。

#	LED	状態	色	内容
1	Power	点灯	緑	電源が供給され正常に動作しています。スタンダアローンモードで動いています。
		点滅	緑	システムが起動中です。
		点灯	赤	システムを起動することができません。
		消灯	—	スイッチに電源が供給されていません。
2	Link/Act/Speed (10/100Mbps)	点灯	橙	10/100Mbps でリンクが確立しています。
		点滅	橙	10/100Mbps でデータを送受信しています。
		消灯	—	リンクが確立していません。
3	Link/Act/Speed (1000Mbps)	点灯	緑	1000Mbps でリンクが確立しています。
		点滅	緑	1000Mbps でデータを送受信しています。
		消灯	—	リンクが確立していません。

第 2 章 機器の設置

- ネットワーク接続前の準備
- 19 インチラックへの取り付け

ネットワーク接続前の準備

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。

- ・ しっかりとした水平面に設置し、不安定な場所や傾いた場所に設置しないでください。
- ・ 本体の上に重いものを置かないでください。
- ・ 電源ケーブルが電源コンセントにしっかり差し込まれているか確認してください。
- ・ 本製品の周辺で熱の放出と十分な換気ができることを確認してください。換気のためには少なくとも製品の左右 10cm 以上の空間を保つようにしてください。
- ・ 本製品は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。
- ・ 本製品は強い電磁場が発生するような場所（モータの周囲など）や、振動、ほこり、および直射日光を避けて設置してください。
- ・ 本製品上に他の機器を積み重ねて設置、または筐体の側面、天面や底面の換気口からの通気を遮る物体 / 機器の上に本製品を置かないでください。

19 インチラックへの取り付け

以下の手順に従って本スイッチを標準の 19 インチラックに設置します。

ブラケットの取り付け

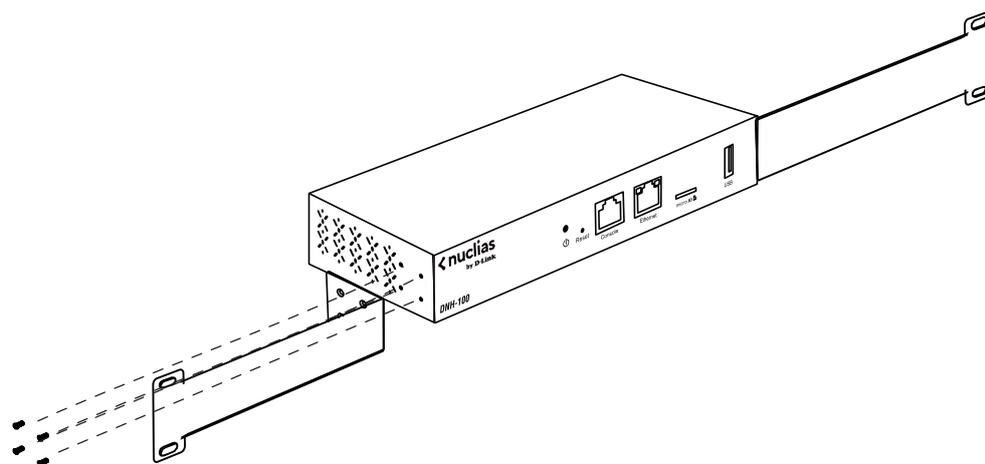


図 2-1 ブラケットの取り付け

ラックマウントキットに付属のネジを使用して、本スイッチにブラケットを取り付けます。

19 インチラックにスイッチを取り付ける

完全にブラケットが固定されていることを確認し、本スイッチを以下の通り標準の 19 インチラックに固定します。

警告 前面、側面にスタビライザを取り付けずに製品を設置すると、ラックが転倒し、場合によっては人身事故を引き起こすことがあります。そのため、ラック内に製品を取り付ける前に必ずスタビライザを取り付けてください。ラックにシステム/コンポーネントを取り付けた後は、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 つだけとしてください。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。

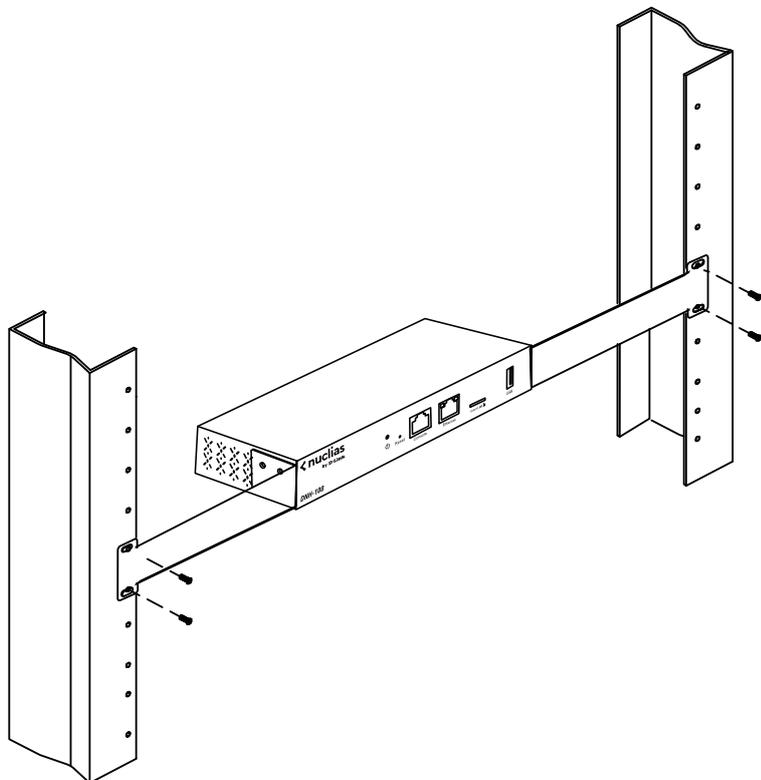


図 2-2 ラックへの設置

第3章 機器の接続

- コントローラへの接続

コントローラへの接続

注意 最初にセットアップを行う際、管理コンピュータと DNH-100 は同じサブネット内に存在する必要があります。

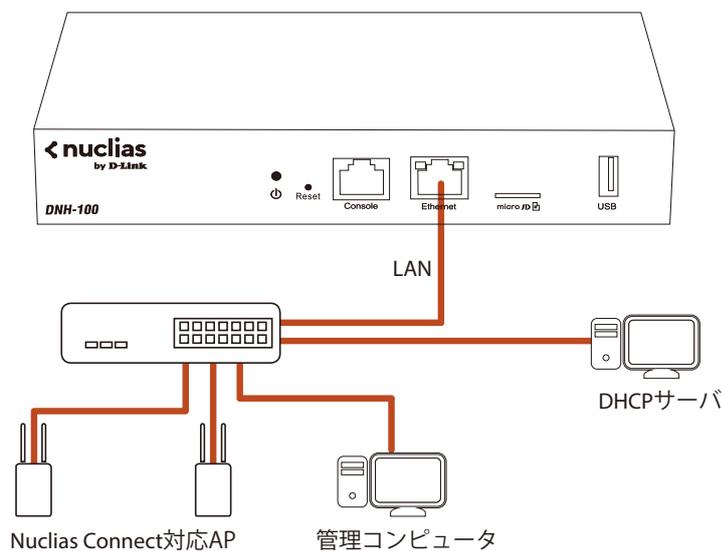


図 3-1 の取り付け

DNH-100 および管理対象のアクセスポイントを、各製品のマニュアルに従い設置します。
以下の方法で管理インターフェースに接続することができます。

イーサネット経由で接続する

WebUI に接続するには以下の機器およびケーブルが必要です。

- ・ RJ-45 イーサネット接続可能な PC
- ・ 標準イーサネットケーブル

1. LAN ケーブルを本製品の Ethernet ポートに接続し、LAN ケーブルのもう一方を LAN ネットワークに繋がるスイッチの RJ-45 ポートに接続します。
2. 電源ケーブルを本製品の電源コネクタに接続し、電源ケーブルのプラグを電源コンセントに接続します。

管理画面への接続

1. コンピュータから管理用画面にアクセスします。Web ブラウザのアドレス入力欄に「https://192.168.0.200」を入力します。
2. 管理インターフェースにログインします。
 - ユーザー名初期値：admin
 - パスワード初期値：admin

コンソール経由で接続する（簡易設定のみ）

コンソールケーブルを使用してスイッチのコンソールポートに接続します。RS-232/RJ-34 変換コネクタケーブルを使用することができます。本製品のコンソールに接続するには、ターミナルエミュレーションプログラムが必要です。

1. RS-232 シリアルインタフェースを管理 PC のシリアルポートに接続します。
2. RJ-45 インタフェースを本製品のコンソールポートに接続します。
3. 管理 PC 上でターミナルエミュレーションプログラムを起動し、プロパティを設定します。
 - スピード：「115200 (bps)」
 - データ：「8 bit」
 - パリティ：「なし (none)」
 - ストップビット：「1 bit」
 - フロー制御：「なし (none)」
4. 本製品に接続し、コマンドラインインタフェースを利用します。

第 4 章 Nuclias Connect の管理インタフェース

- 「Nuclias Connect への接続」
- 「Nuclias Connect 設定ウィザード」
- 「ユーザプロフィール」

Nuclias Connect への接続

DNH-100 には Nuclias Connect がプリロードされています。

1. 管理コンピュータで Web ブラウザを開き、DNH-100 の IP アドレスまたはドメイン名を入力します。デフォルトの IP アドレスは「https://192.168.0.200」です。

注意 最初にセットアップを行う際、管理コンピュータと DNH-100 は同じサブネット内に存在する必要があります。

2. ログインユーザ名、パスワード、CAPTCHA コードを入力し、「ログイン」をクリックして Nuclias Connect にログインします。

図 4-1 Nuclias Connect ログイン画面

補足

- 初期アカウントはユーザ名、パスワードともに admin です。
- 「パスワードを忘れた場合」をクリックすると、現在のパスワードを忘れた場合にパスワードをリセットします。
- インタフェースは多言語オプションをサポートしています。言語を選択するドロップダウンメニューをクリックすると、別の言語を選択できます。

3. ログイン後、パスワード変更画面が表示されます。最初のログイン後に、デフォルトのパスワードを変更する必要があります。

パスワードを割り当てる場合は、強力なパスワードを使用することをお勧めします。新しいパスワードの長さは8~30文字である必要があります。大文字と小文字、数字、記号を組み合わせることで、強力なパスワードを作成できます。

図 4-2 パスワードの変更

注意 一般的な単語や名前は使用しないでください。

現在のパスワードを「Old Password」フィールドに入力し、「New Password」フィールドに新しいパスワードを入力します。「Confirm Password」フィールドに同じパスワードを入力して、入力内容を確認します。「変更」をクリックして処理を完了します。

ログインすると、「システム設定」画面が表示されます。ウィザードに従って設定を行います。

図 4-3 ウィザード - システム設定

Nuclias Connect 設定ウィザード

ウィザードを使用すると、基本的なシステムの設定およびネットワークの作成を行うことができます。

Nuclias Connect 設定ウィザード (初回ログイン時)

1. 「システム情報」画面が表示されます。

図 4-4 ウィザード-システム設定

「LAN 設定」セクションでは、デバイス接続パラメータを設定できます。これらの設定により、管理コンピュータをデバイスに接続できます。

項目	説明
LAN 設定	
IP アドレスの取得	IP インタフェースの IP アドレス取得方法を選択します。 ・ 選択肢：「スタティック IP アドレス (手動)」 「動的 IP アドレス (DHCP)」 注意 DHCP サーバは推奨されません。
IP アドレス	「スタティック IP アドレス」を選択している場合、IP インタフェースの IP アドレスを入力します。
サブネットマスク	IP インタフェースのサブネットマスクを入力します。
ゲートウェイ	IP インタフェースのゲートウェイを入力します。(オプション)
プライマリ DNS	IP インタフェースの優先 DNS アドレスを入力します。(オプション)
セカンダリ DNS	IP インタフェースの優先 DNS アドレスを入力します。(オプション)
デバイスアクセスアドレスの同期	デバイスアクセスアドレスの同期を有効にする場合にチェックします。デバイスアクセスアドレスが LAN IP アドレスと異なり、リモート AP を管理する場合は、この機能を無効にする必要があります。

「日付と時間」セクションでは、デバイスの時刻と日付に関するパラメータを設定できます。NTP サーバを使用することをお勧めします。ログとスケジュールの設定は、正しい時刻と日付の設定に依存します。

項目	説明
日付と時間	
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
NTP	NTP サーバを使用してデバイスの日時を管理する場合は、本項目にチェックを入れます。
NTP サーバ 1	NTP サーバのアドレスを指定します。
NTP サーバ 2	セカンダリ NTP サーバのアドレスを指定します。

「保存」をクリックします。

Nuclias Connect 設定ウィザード

補足 最初の LAN 設定と日時設定が完了した後、WebUI に再度ログインすると、以下のウィザードが表示されます。

補足 ウィザードを途中で終了した場合でも、WebUI の右上の  アイコンから開始することができます。

1. 「システム情報」画面が表示されます。



図 4-5 ウィザード - システム設定

以下の設定項目が表示されます。

項目	説明
デバイスアクセスアドレス	Nuclias Connect サーバアプリケーションの IP アドレスを入力します。リモート AP を管理するには、IP アドレスがパブリック IP アドレスである必要があります。ファイアウォールやルータを介したリモート AP 管理の場合、IP マッピングが必要です。
デバイスアクセスポート	Nuclias Connect サーバアプリケーションのリスニングポート番号を入力します。ファイアウォールやルータを介したリモート AP 管理の場合、受信ポートを開く必要があります。 ・ 初期値：8443
Web アクセスポート	定義済みの Web アクセスポートが表示されます。
国	本システムを利用する国として「Japan」を選択します。

「保存して次へ」をクリックします。

2. 「ネットワークを追加」画面が表示されます。



図 4-6 ネットワークを追加

以下の設定項目が表示されます。

項目	説明
サイト	「サイト」ドロップダウンメニューから既存のサイトを選択するか、新しいサイト (newSite) を選択し、空のフィールドにサイトの名前を入力します。
ネットワーク名	新しいネットワークを識別する名前を入力します。
ネットワーク ID	ネットワーク ID を入力します (オプション)。REST API 機能を使用しない場合は入力不要です。

「次へ」をクリックします。

前の画面に戻るには「戻る」をクリック、ウィザードを中止するには「キャンセル」をクリックします。

第4章 Nuclias Connectの管理インターフェース

3. 「ネットワーク設定」画面が表示されます。「アクセスポイント」にチェックを入れ、ネットワーク設定を定義します。「次へ」をクリックして次に進みます。前の画面に戻るには「戻る」をクリック、ウィザードを中止するには「キャンセル」をクリックします。

補足

スイッチ製品は未サポートです。

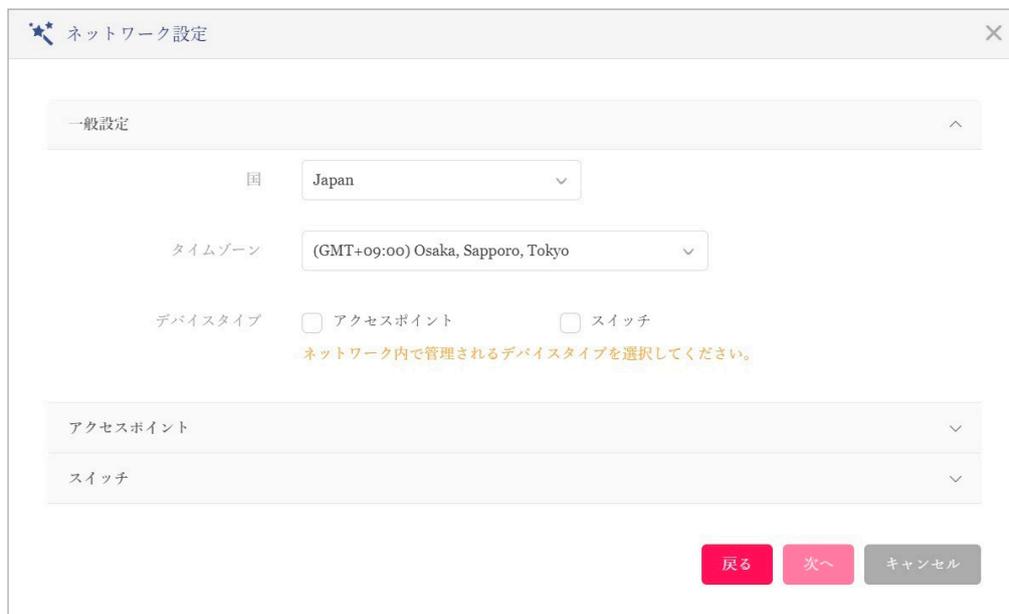


図 4-7 ネットワークの設定



図 4-8 ネットワークの設定

- 「ネットワーク設定を検出」画面が表示されます。データリンクレイヤ（「レイヤ2」または「レイヤ3（IP）」）を選択して、ネットワーク検出を実行するネットワークのタイプを定義します。

レイヤ3が選択されている場合は、ドロップダウンメニューをクリックして、IPまたはプレフィックスセグメンテーションのいずれかを定義します。**+**をクリックして追加のIP/プレフィックスセグメントを追加するか、「次へ」をクリックして続行します。設定プロセスを中止するには「終了」をクリックします。

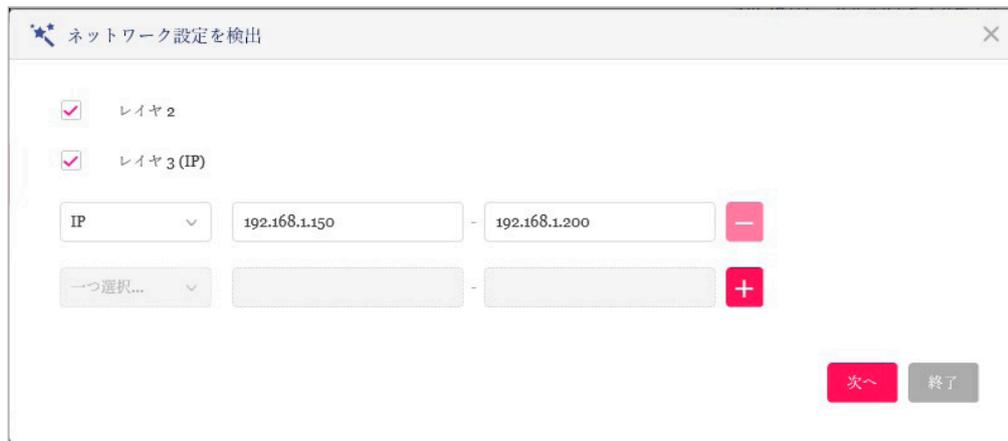


図 4-9 ネットワーク設定を検出

- 「APを検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを検出・表示します。
- デバイスが検出された場合は、そのデバイスを選択して「インポート」をクリックし、ネットワークプロファイルをインポートします。インポート操作により、定義したネットワークも作成されます。「管理」タブをクリックして、定義済みのデバイスを選択し、このネットワークに追加することもできます。

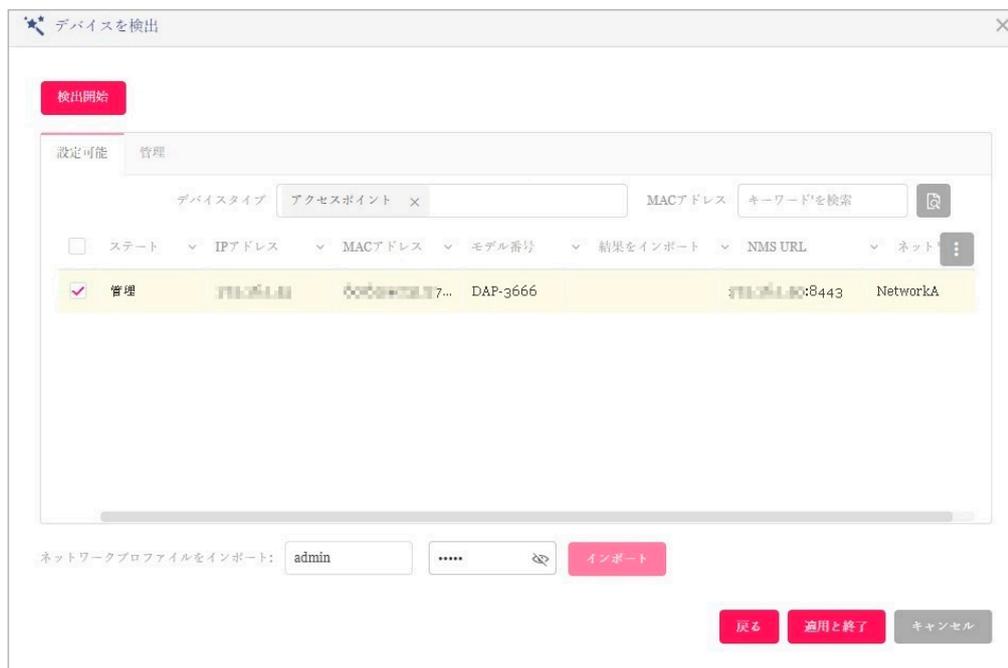


図 4-10 APを検出

参照 管理 / 非管理 AP のネットワークの移動や削除については、「[デバイス管理](#)」を参照してください。

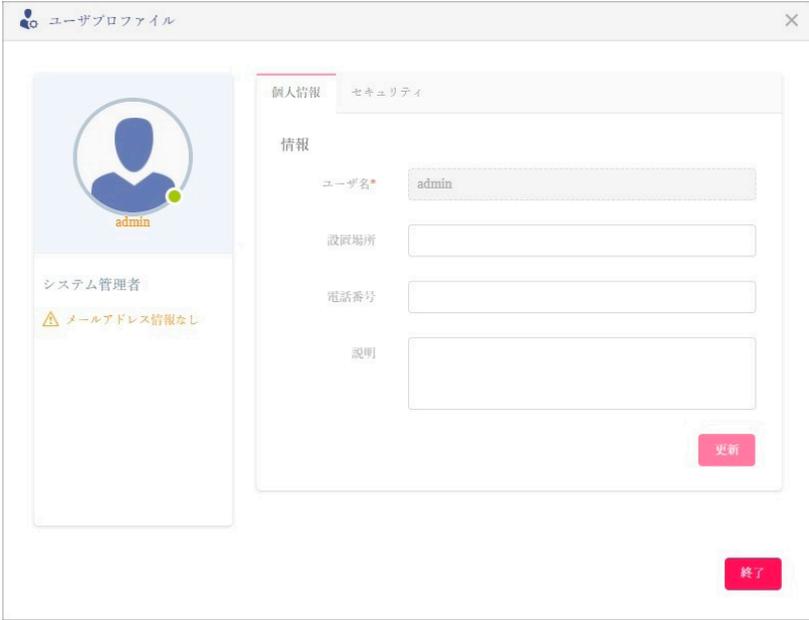
- 右上の「×」ボタンをクリックして画面を閉じます。

ユーザプロフィール

管理者のアカウント情報を設定します。

個人情報

画面右上のユーザアイコン（）をクリック、「ユーザプロフィール」を選択して、以下の画面を表示します。



The screenshot shows a window titled 'ユーザプロフィール' (User Profile). On the left, there is a user profile card for 'admin' with a blue silhouette icon and the text 'システム管理者' (System Administrator) and a warning 'メールアドレス情報なし' (No email address information). The main area has two tabs: '個人情報' (Personal Information) and 'セキュリティ' (Security). Under '個人情報', there are input fields for 'ユーザ名*' (User Name) containing 'admin', '設置場所' (Setting Location), '電話番号' (Phone Number), and '説明' (Description). A red '更新' (Update) button is at the bottom right of the form, and a red '終了' (End) button is at the bottom right of the window.

図 4-11 ユーザプロフィール-個人情報

「設置場所」「電話番号」「説明」を設定し、「更新」をクリックします。

セキュリティ

「セキュリティ」タブを選択すると、以下の画面が表示されます。



The screenshot shows the same window as Figure 4-11, but with the 'セキュリティ' (Security) tab selected. The '個人情報' (Personal Information) tab is now greyed out. Under 'セキュリティ', there are two sections: 'パスワードを変更' (Change Password) with fields for 'パスワード*' (Current Password), '新しいパスワード*' (New Password), and 'パスワード確認*' (Password Confirmation); and 'メールアドレスを変更' (Change Email Address) with a field for '新しいメールアドレス' (New Email Address). Red '保存' (Save) buttons are located below each section, and a red '終了' (End) button is at the bottom right of the window.

図 4-12 ユーザプロフィール-セキュリティ

パスワードおよびメールアドレスを設定・変更することができます。

パスワードを変更する場合は、「パスワード」に現在のパスワードを入力し、「新しいパスワード」「パスワード確認」に新しいパスワードを入力します。

管理インターフェースからのログアウト

画面右上のユーザアイコン（）をクリック、「ログアウト」を選択して、管理インターフェースからログアウトします。

第5章 ダッシュボード

サーバに正常にログインすると、「ダッシュボード」画面が表示されます。このページには、作成されたサイト/ネットワーク、利用可能なアクセスポイントとワイヤレスクライアント、利用可能なスイッチとクライアントの概要が表示されます。

補足 スイッチ製品は未サポートです。

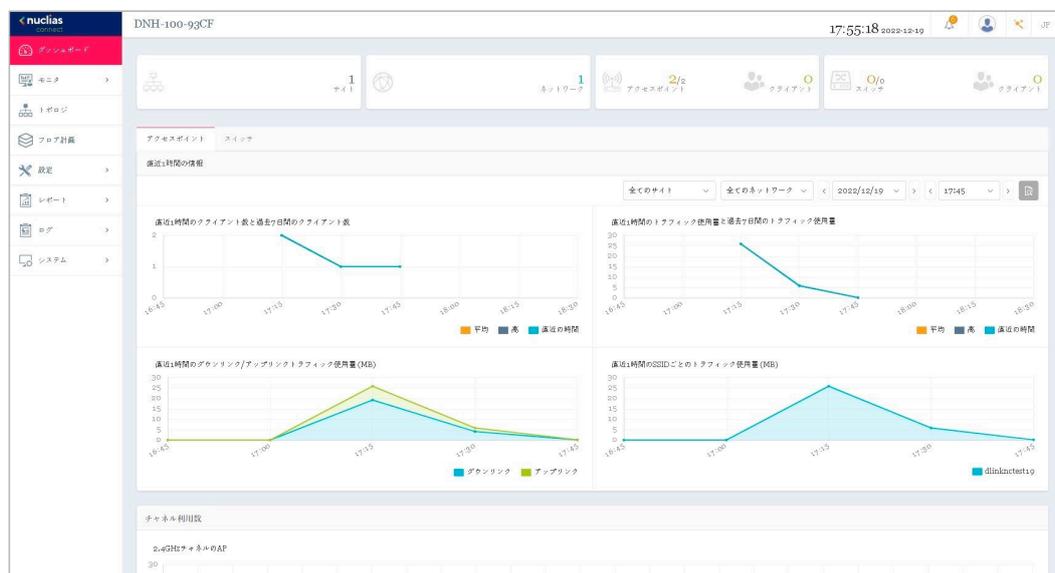


図 5-1 ダッシュボード

画面上部の統計情報には以下の項目が表示されます。

項目	説明
サイト	作成されたプロファイル（サイト）の数を表示します。
ネットワーク	作成されたネットワークの数を表示します。
アクセスポイント	利用可能なアクセスポイントのオンライン数 / 合計数を表示します。
スイッチ	利用可能なスイッチのオンライン数 / 合計数を表示します。

「アクセスポイント」タブには以下の項目が表示されます。

項目	説明
直近1時間の情報	以下の履歴情報を表示します。表示するサイト/ネットワークおよび期間を指定することができます。 <ul style="list-style-type: none"> 直近1時間のクライアント数と過去7日間のクライアント数 直近1時間のトラフィック使用量 (MB) 直近1時間のダウンリンク/アップリンクトラフィック使用量 (MB) 直近1時間のSSIDごとのトラフィック使用量 (MB)
チャンネル利用率	2.4GHz帯域/5GHz帯域のチャンネルごとのアクセスポイントの台数を表示します。
直近のイベント	最新イベントの簡易的なログを表示します。 表示するサイト/ネットワークを指定することができます。

「スイッチ」タブには以下の項目が表示されます。

項目	説明
直近1時間の情報	以下の履歴情報を表示します。表示するサイト/ネットワークおよび期間を指定することができます。 <ul style="list-style-type: none"> 直近1時間のTx/Rxトラフィック使用量 (MB) 直近1時間のPoE使用量 (W)
PoE利用率	PoE利用率ごとのスイッチの台数を表示します。 表示するサイト/ネットワークを指定することができます。
直近のイベント	最新イベントの簡易的なログを表示します。 表示するサイト/ネットワークを指定することができます。

第6章 モニタ

- 「アクセスポイント」
- 「アクセスポイント - デバイス詳細」
- 「アクセスポイント - ワイヤレスクライアント」
- 「アクセスポイント - 隣接 AP」
- 「スイッチ」
- 「スイッチ - デバイス詳細」
- 「スイッチ - スイッチクライアント」
- 「スイッチ - スイッチポート」

補足

スイッチ製品は未サポートです。

アクセスポイント

左側のパネルから **モニタ** > **アクセスポイント** > **アクセスポイント** をクリックし、トラフィック使用量の時間毎の推移と各アクセスポイントのステータスを表示します。

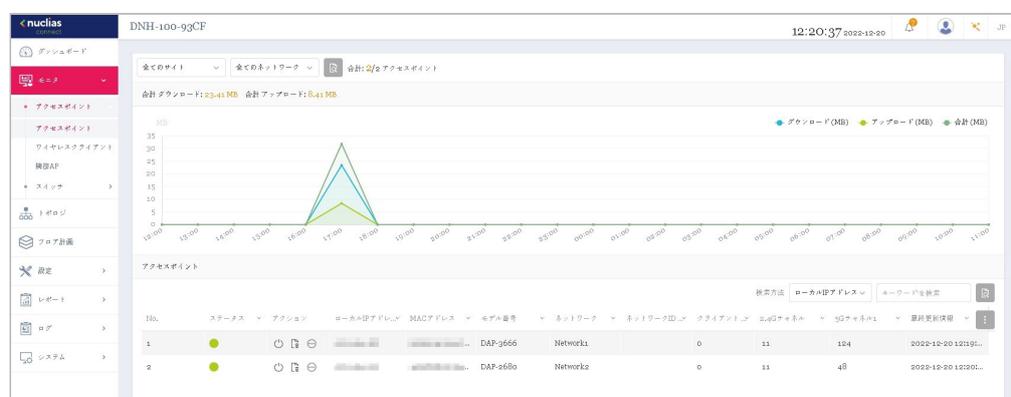


図6-1 モニタ - アクセスポイント - アクセスポイント

■ 対象範囲の指定 / デバイスの検索

- ・ 左上のドロップダウンメニューから「サイト」「ネットワーク」を指定して、🔍 をクリックします。
- ・ 「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、「検索」フィールドにキーワードを入力し、🔍 をクリックして検索を開始します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

- ・ 🔌 をクリックしてデバイスを再起動します。
- ・ 📶 をクリックして、デバイスを非管理へ移動します。
- ・ 📄 をクリックして、デバイス詳細画面に移動します。

■ レポート項目

各アクセスポイントについて、以下の項目を表示することができます。表示項目を変更するには、⋮ をクリックします。

- ・ ステータス
- ・ ローカル IP アドレス
- ・ ローカル IPv6 アドレス
- ・ MAC アドレス
- ・ モデル番号
- ・ ファームウェアバージョン
- ・ 名前
- ・ 設置場所
- ・ サイト
- ・ ネットワーク
- ・ ネットワーク ID
- ・ クライアント
- ・ 2.4G チャネル
- ・ 5G チャネル 1
- ・ 5G チャネル 2 (トライバンド)
- ・ 2.4G 出力
- ・ 5G 出力 1
- ・ 5G 出力 2 (トライバンド)
- ・ ダウンロード
- ・ アップロード
- ・ トラフィック使用量
- ・ トラフィック使用率 (%)
- ・ CPU 使用率 (%)
- ・ メモリ使用率 (%)
- ・ 最終更新情報
- ・ 稼働時間

アクセスポイント - デバイス詳細

左側のパネルから **モニタ** > **アクセスポイント** > **アクセスポイント** をクリックし、アクセスポイントの一覧を表示します。
 アクション欄の  (デバイス詳細ページへのリンク) をクリックすると、デバイスの詳細画面が表示されます。

デバイス詳細画面には、スイッチの包括的な情報が表示され、無線チャンネルや出力などを設定できます。

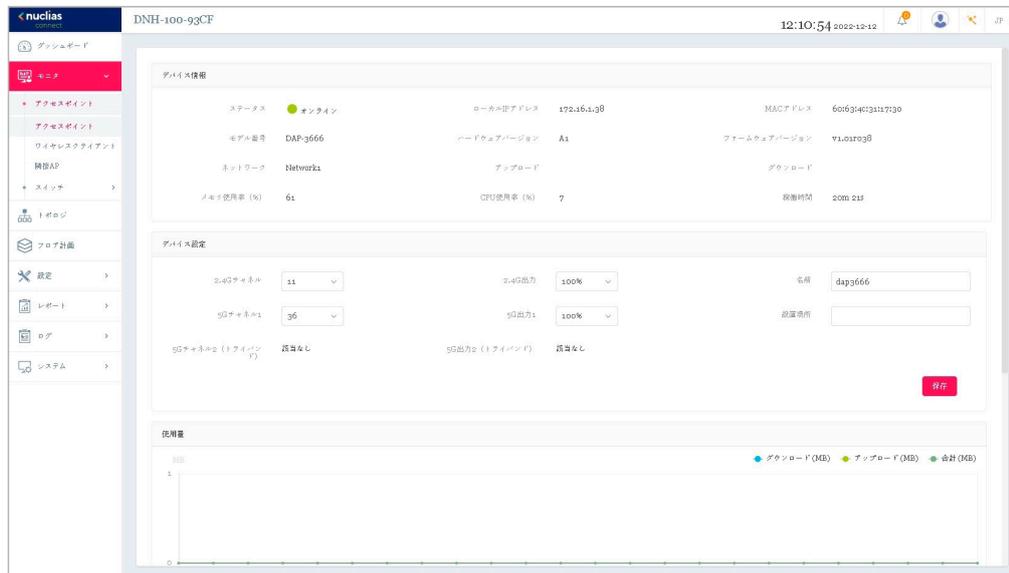


図 6-2 モニタ - アクセスポイント - アクセスポイント - デバイス詳細

注意 自動チャンネル有効時にチャンネル固定をした場合は、自動チャンネルが優先されます。

注意 チャンネル固定を設定していても、AP 側の「Restore to Factory Default Settings」を実行、または筐体を変更した場合、チャンネルは AP 側に設定が保存されるため、ランダムチャンネルに戻ります。

アクセスポイント - ワイヤレスクライアント

接続しているクライアント

左側のパネルから**モニタ** > **アクセスポイント** > **ワイヤレスクライアント**をクリックし、アプリケーションによって管理されているすべての接続されたクライアントのレポートを表示します。

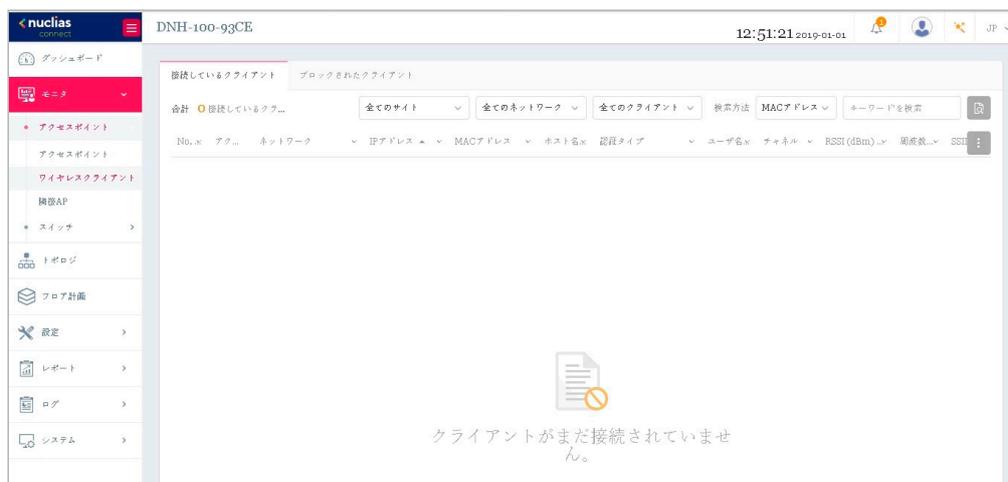


図 6-3 モニタ - アクセスポイント - ワイヤレスクライアント (接続されたクライアント)

■ 対象範囲の指定 / デバイスの検索

- 左上のドロップダウンメニューから「サイト」「ネットワーク」「クライアント」を指定して、をクリックします。
- 「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、「検索」フィールドにキーワードを入力、または項目を指定し、をクリックして検索を開始します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

■ レポート項目

各無線クライアントについて、以下の項目を表示することができます。表示項目を変更するには、をクリックします。

- サイト
- ネットワーク
- IP アドレス
- IPv6 アドレス
- MAC アドレス
- ホスト名
- 認証タイプ
- ユーザ名
- OS
- アップロード
- ダウンロード
- チャンネル
- RSSI (dBm)
- SNR (dB)
- 周波数帯
- SSID
- AP MAC アドレス
- トラフィック使用量
- トラフィック使用率 (%)
- 最終更新情報
- 稼働時間

ブロックされたクライアント

左側のパネルから**モニタ** > **ワイヤレスクライアント**をクリックし、「ブロックされたクライアント」タブを開きます。この画面では、アプリケーションによって検出されたすべてのブロックされたクライアントのレポートを表示できます。

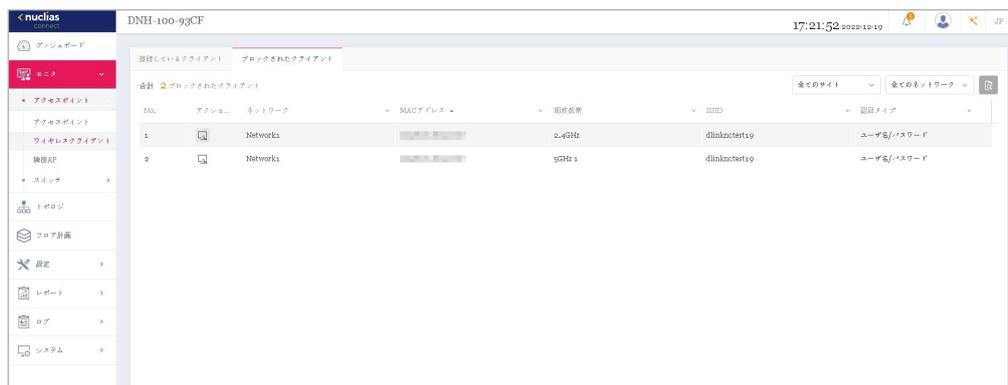


図 6-4 モニタ-アクセスポイント-ワイヤレスクライアント (ブロックされたクライアント)

■ 対象範囲の指定

- 左上のドロップダウンメニューから「サイト」「ネットワーク」を指定して、をクリックします。

■ レポート項目

ブロックされた各無線クライアントについて、以下の項目が表示されます。

- ・ アクション
- ・ ネットワーク
- ・ MAC アドレス
- ・ 周波数帯
- ・ SSID
- ・ 認証タイプ

アクセスポイント - 隣接 AP

左側のパネルからモニタ > アクセスポイント > 隣接 AP をクリックし、隣接 AP の一覧を表示します。

この機能を有効にするには、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソース > 隣接 AP 検知の順に選択し、「有効化」をクリックします。

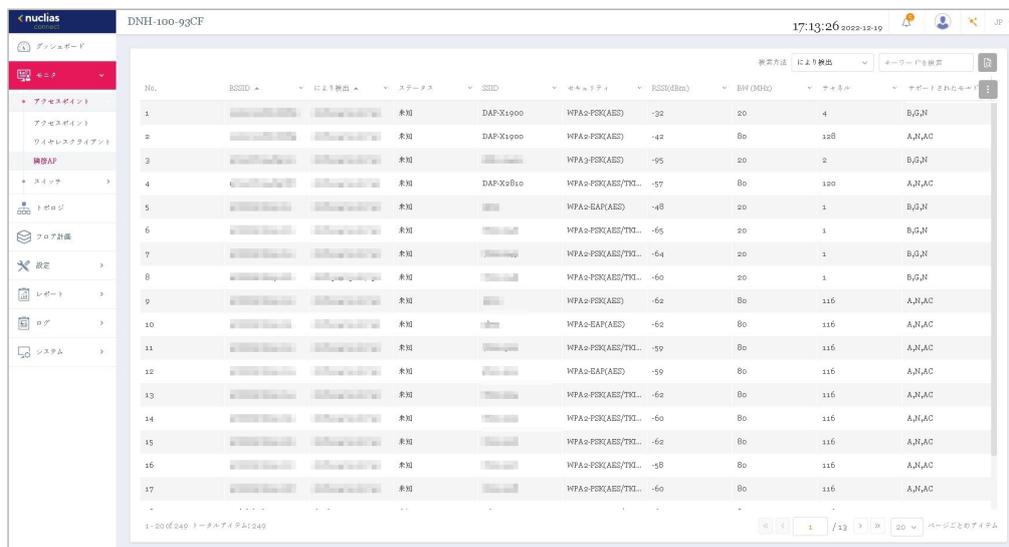


図 6-5 モニタ - アクセスポイント - 隣接 AP

■ デバイスの検索

- 「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、「検索」フィールドにキーワードを入力し、 をクリックして検索を開始します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

以下の項目が表示されます。表示項目を変更するには、 をクリックします。

項目	説明
BSSID	AP の無線インタフェースの MAC アドレスを表示します。
により検出	スキャンした AP の MAC アドレスを表示します。
ステータス	AP のステータス (未知 / 既知 / 管理) を表示します。
SSID	無線ネットワークの名前を表示します。
セキュリティ	使用している暗号化方式を表示します。
RSSI (dBm)	AP が検出した RSSI を表示します。
BW (MHz)	AP が使用していたチャンネル幅が表示されます。
チャンネル	AP が検出されたチャンネル設定が表示されます。
サポートされたモデル	AP が使用している接続モードを表示します。

補足

「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「【付録 A】機能別サポート製品 / バージョンについて (p.125)」をご確認ください。

スイッチ

左側のパネルから**モニタ** > **スイッチ** > **スイッチ**をクリックし、スイッチの一覧を表示します。

補足 スイッチ製品は未サポートです。

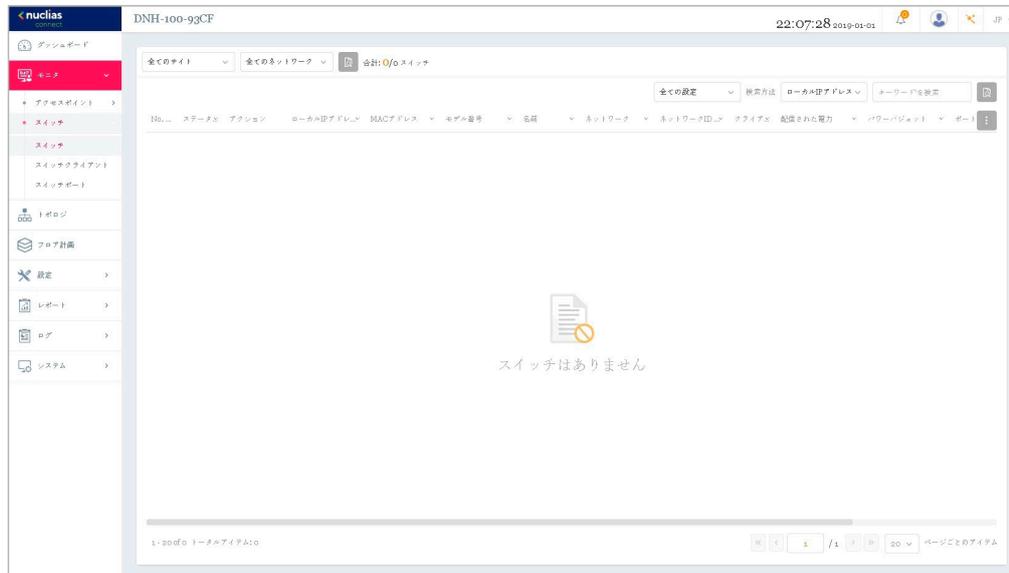


図 6-6 モニタ - スイッチ - スイッチ

■ 対象範囲の指定 / デバイスの検索

- ・ 左上のドロップダウンメニューから設定の種類（プロファイル / スタンドアロン）を指定して、をクリックします。
- ・ 「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、「検索」フィールドにキーワードを入力し、をクリックして検索を開始します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

- ・ をクリックしてデバイスを再起動します。
- ・ をクリックして、デバイスを非管理へ移動します。
- ・ をクリックして、デバイス詳細画面に移動します。

■ レポート項目

各スイッチについて、以下の項目を表示することができます。表示項目を変更するには、をクリックします。

- ・ ステータス
- ・ ローカル IP アドレス
- ・ MAC アドレス
- ・ モデル番号
- ・ ファームウェアバージョン
- ・ ハードウェアバージョン
- ・ シリアル番号
- ・ 名前
- ・ 設置場所
- ・ サイト
- ・ ネットワーク
- ・ ネットワーク ID
- ・ クライアント
- ・ 配信された電力
- ・ パワーバジェット
- ・ CPU 使用率 (%)
- ・ メモリ使用率 (%)
- ・ ポート
- ・ 設定を使用
- ・ 最終更新情報
- ・ 稼働時間

主要な項目の説明は以下の通りです。

項目	説明
名前	ユーザ定義のスイッチの名前を表示します。名前が指定されていない場合は何も表示されません。列をクリックして、名前を設定または変更します。最大 63 文字で入力します。
設置場所	スイッチの位置を表示します。列をクリックして、場所の名前を設定または変更します。最大 32 文字で入力します。
クライアント	スイッチに接続しているクライアントの総数を表示します。クライアントの数をクリックすると、「スイッチクライアント」画面に遷移します。

第6章 モニタ

項目	説明
ポート	スイッチのポートの総数を表示します。 ポートをクリックすると、「スイッチポート」画面に遷移します。
設定を使用	設定モード（プロファイル/スタンドアロン）を表示します。 <ul style="list-style-type: none">プロファイル：プロファイルモードのデバイスは、プロファイル内の同じ設定を共有します。スタンドアロン：デバイス個別の設定があり、プロファイルの影響を受けることはありません。
最終更新情報	スイッチが最後に接続された時刻を表示します。
稼働時間	スイッチが再起動してから経過した起動時間を表示します。

スイッチ - デバイス詳細

左側のパネルから**モニタ**>**スイッチ**>**スイッチ**をクリックし、スイッチの一覧を表示します。

アクション欄の （デバイス詳細ページへのリンク）をクリックすると、デバイスの詳細画面が表示されます。

デバイスの詳細ページには、スイッチの包括的な情報が表示され、ポート、IP インタフェース、ルート設定などを設定できます。

基本タブ

「基本」タブでは、デバイスの基本的な設定を行ったり、デバイス情報の概要を表示したりすることができます。

補足 スイッチ製品は未サポートです。

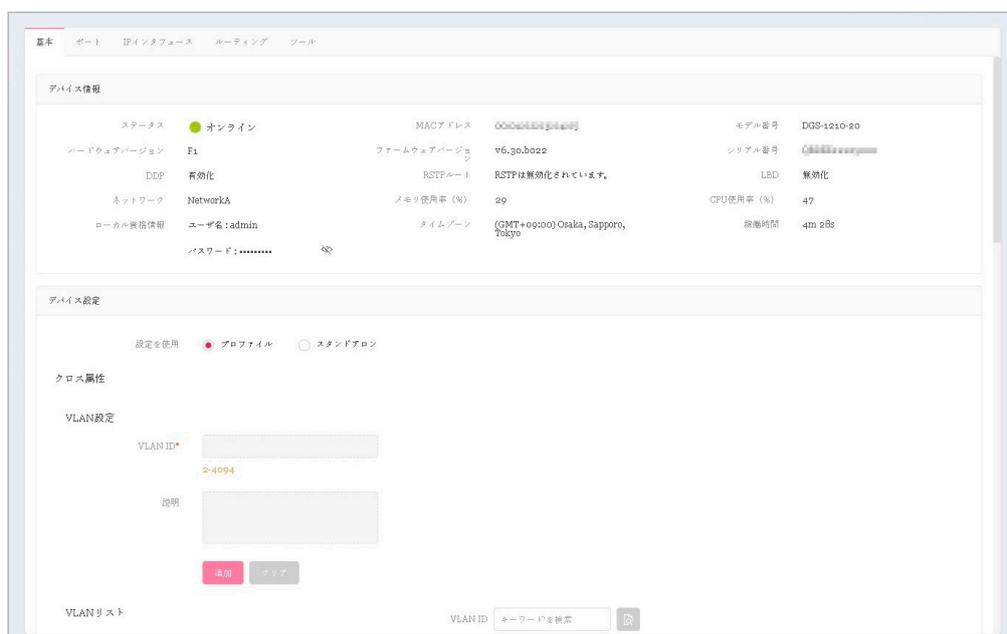


図 6-7 モニタ - スイッチ - スイッチ - デバイス詳細 - 基本タブ

デバイス情報

「デバイス情報」セクションには、以下の項目が表示されます。

- 「ステータス」「MAC アドレス」「モデル番号」「ハードウェアバージョン」「ファームウェアバージョン」「シリアル番号」「DDP」「RSTP ルート」「LBD」「ネットワーク」「メモリ使用率 (%)」「CPU 使用率 (%)」「ローカル資格情報」「タイムゾーン」「稼働時間」

スイッチの機能に関する項目は、以下の通りです。

項目	説明
DDP	スイッチの DDP（D-Link Discovery Protocol）設定を表示します。
ローカル資格情報	ローカル GUI/ コンソールのユーザ名とパスワードを表示します。
LBD	スイッチの LBD（Loopback Detection）設定を表示します。
RSTP ルート	スパンニングツリーのルートブリッジとそのプライオリティを表示します。

デバイス設定

- 「デバイス設定」セクションで、「プロファイル」または「スタンドアロン」を選択します。
 - 「プロファイル」を選択すると、VLAN や IGMP スヌーピングなどの「デバイス」セクションの設定が固定されます。
 - 「スタンドアロン」を選択すると、上記の設定を編集できるようになります。

■ VLAN 設定

- 「設定を使用」が「スタンドアロン」に設定されている場合、VLAN を作成、編集できます。

図 6-8 VLAN 設定

VLAN を作成する場合、以下の手順を実行します。

- 「VLAN ID」に VLAN ID を 2-4094 の範囲で入力します。
- 「説明」に識別しやすくするための説明を入力します。
- 「追加」をクリックして VLAN を作成します。
設定内容をリセットするには、「クリア」をクリックします。

作成された VLAN ID は「VLAN リスト」に表示されます。検索フィールドにキーワードを入力し、 をクリックして VLAN ID を検索します。

VLAN を編集する場合は、対象 VLAN の をクリックします。設定完了後、「保存」をクリックして変更を保存します。

VLAN を削除する場合は、対象 VLAN の をクリックします。

■ IGMP スヌーピング

- IGMP スヌーピングはデフォルトで無効になっています。「設定を使用」が「スタンドアロン」に設定されている場合、IGMP スヌーピングを有効化できます。

図 6-9 IGMP スヌーピング設定

- 「IGMP スヌーピング」を「有効」に設定します。
- 「VLAN」に VLAN ID を 1-4094 の範囲で入力します。(例:「1-4,7」または「all」)

■ アンクロス属性

4. 「アンクロス」セクションでは、プロフィール経由で設定できない機能が表示されます。

アンクロス属性

名前

設置場所

STPブリッジプライオリティ

図 6-10 アンクロス属性

- (1) 「名前」「設置場所」を入力します。
- (2) ドロップダウンメニューから「STP ブリッジプライオリティ」を選択します。

■ 設定の適用

5. 「デバイス設定」セクションの設定を変更した後、「適用」をクリックして設定をスイッチに適用します。

IP 接続

「IP 接続」セクションでは、プライマリ接続を設定できます。

IP 接続

タイプ DHCP 静的IP

ローカルIPアドレス*

VLAN* 20 現在このVLANに属しているメンバポート

ネットマスク*

ゲートウェイ*

DNS

図 6-11 IP 接続

1. IP の種類 (DHCP または固定 IP) を選択します。
2. 以下の項目を設定します。
 - 「ローカル IP アドレス」 (固定 IP のみ)
 - 「VLAN」
 - 「ネットマスク」 (固定 IP のみ)
 - 「ゲートウェイ」 (固定 IP のみ)
 - 「プライマリ / セカンダリ / サード DNS」 (固定 IP のみ)
3. 「適用」をクリックして、設定をスイッチに適用します。

CPU 使用率

「CPU 使用率」セクションには、CPU 使用率のグラフが表示されます。

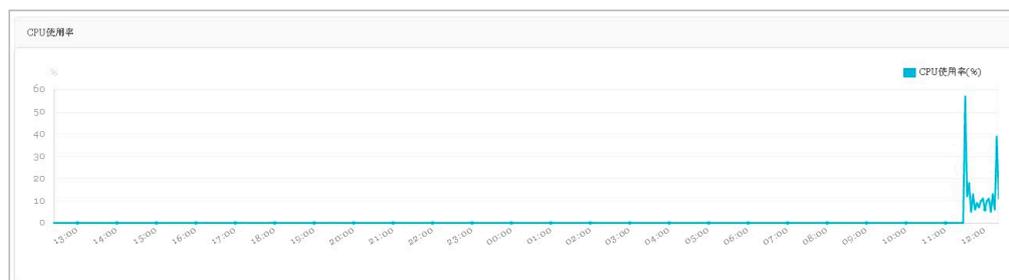


図 6-12 CPU 使用率

Y 軸には CPU 使用率のパーセンテージ、X 軸には時間（1 時間毎）が表示されます。

ポートタブ

「ポート」タブには、ポートステータスの概要が表示されます。ポートの色とアイコン表示により、各ポートのステータスを確認することができます。ポートアイコンをクリックすると、該当ポートのポート詳細画面が表示されます。

補足

スイッチ製品は未サポートです。

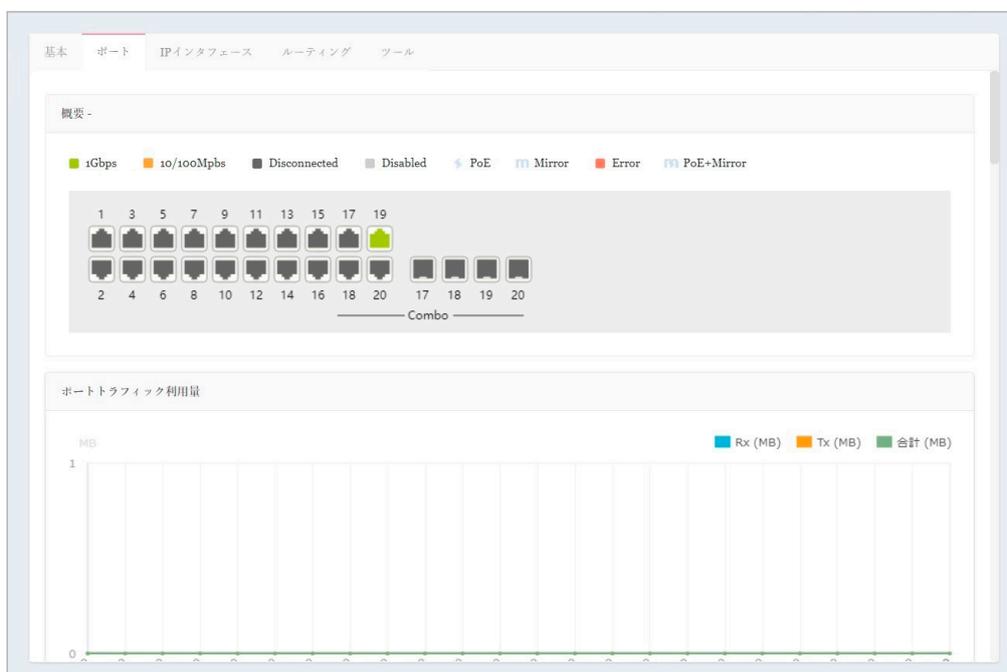


図 6-13 デバイス詳細 - ポートタブ

概要

ポートの色とアイコンが示すステータスは以下の通りです。

項目	説明
緑	1Gbps イーサネットに接続しています。
オレンジ	10/100Mbps イーサネットに接続しています。
ダークグレー	ポートが切断されています。
ライトグレー	ポートが無効です。
	PoE による電源供給が行われています。
	ポートはミラーリングされています。
赤	エラーが検出されました。
	PoE による電源供給が行われています。また、ポートはミラーリングされています。

ポートトラフィック利用量

「ポートトラフィック利用量」セクションでは、時間ごとの Rx と Tx の使用状況を示すグラフが表示されます。

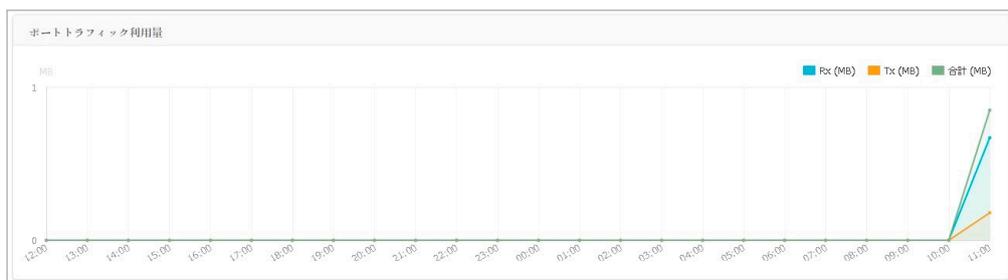


図 6-14 ポートトラフィック利用量

ポート情報

「ポート情報」セクションでは、すべてのアクティブポートと非アクティブポートの概要を表示できます。

ポート	アグリゲート	リンク	Txバイト数	Rxバイト数	合計バイト数	使用済電力	ポートタイプ	VLAN	許可されたVLAN	ポートステータス	RSTP
1	-	自動 / 1Gbps全二重	776.27 (KB)	2.50 (MB)	3.26 (MB)	-	アクセス	1		有効化	有効化
2	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
3	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
4	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
5	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
6	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
7	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
8	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
9	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
10	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化
11	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化	有効化

図 6-15 ポート情報

テーブルには以下の項目が表示されます。

- 「ポート (番号)」「アグリゲート」「リンク」「Tx/Rx/合計バイト数」「使用済電力」「ポートタイプ」「VLAN」「許可された VLAN」「ポートステータス」「RSTP」「LBD」「DDP」「ポートシャットダウンスケジュール」「ミラー」「アクセスポリシー」「LLDP」「ポート名」
 - 「アグリゲート」では、ポートチャンネル ID と集約タイプ (スタティック / LACP) を表示します。
 - 「VLAN」では、トランクモードのネイティブ VLAN ID またはアクセスモードの VLAN ID を表示します。また、音声 VLAN ID に所属する場合、音声 VLAN ID を表示します。
 - 「許可された VLAN」は、ポートタイプが「トランク」の場合、許可された VLAN ID を表示します。

■ ポートの検索

- 「検索方法」のドロップダウンメニューで検索項目の属性 (「VLAN」または「Port」) を選択し、「ポートタイプ」(「アクセス」「トランク」「全てのタイプ」) を選択した後、 をクリックして検索を開始します。「検索」フィールドにキーワードを入力して検索することも可能です。

■ ポートの変更

スイッチのポートまたはポートグループの設定を変更するには、「基本」タブの「デバイス設定」セクションで「設定を使用」が「スタンドアロン」に設定されていることを確認してください。

- 変更するポートの横にあるチェックボックスにチェックを入れます。
- をクリックして編集を行います。下にスクロールして、当該ポートのポート設定を編集してください。

図 6-16 ポート設定

項目	説明
ポートシャットダウンスケジュール	ポートのシャットダウン機能に時間プロファイルを適用します。時間プロファイル画面で定義されたプロファイルを選択することができます。
PoE 供給のスケジュール	PoE 供給機能に時間プロファイルを適用します。

項目	説明
ポートタイプ	<p>スイッチポートは、次の2つのタイプのいずれに設定できます。</p> <ul style="list-style-type: none"> 「トランク」: トランクポートでは、選択したポートが 802.1Q のタグ付きトラフィックを受け入れ/パスすることができます。 <ul style="list-style-type: none"> 「ネイティブ VLAN」: すべてのアンタグトラフィックがこの VLAN に配置されます。1-4094 の範囲で指定します。 「許可された VLAN」: 選択された VLAN のみがこのリンクを通過できます。all (すべて) または 1-4094 の範囲で指定します。 「アクセス」: アクセスポートは、すべてのトラフィックを定義された VLAN に配置します。 <ul style="list-style-type: none"> 「VLAN」: すべてのトラフィックがこの VLAN に配置されます。1-4094 の範囲で指定します。 「アクセスポリシー」: このポートに制限ポリシーを適用します。 <ul style="list-style-type: none"> 「無効」: すべてのデバイスがこのポートにアクセスできます。 「スタティック MAC ホワイトリスト」: このリストで指定された MAC アドレスを持つデバイスのみがこのポートにアクセスできます。 「ポートセキュリティ delete-on-time モード」: エントリがエージアウトした場合、またはユーザがこれらのエントリを手動で削除した場合に、学習されたすべての MAC アドレスが消去されます。「ダイナミックホワイトリストサイズ制限」の設定により、動的に学習されたエントリの数を制限できます。「ダイナミックホワイトリスト MAC」の総数が「ダイナミックホワイトリストサイズ制限」の値を超えると、後続のすべての MAC アドレスがこのポートへのアクセスを拒否されます。 「ユーザ定義のアクセスポリシー」: 「アクセスポリシー」画面で定義したポリシー名を適用します。

3. 設定を変更後、「適用」をクリックしてスイッチに設定を適用します。

アグリゲート管理

「アグリゲート管理」セクションでは、2~8 個のポートを1つのリンクアグリゲーショングループにまとめることができます。

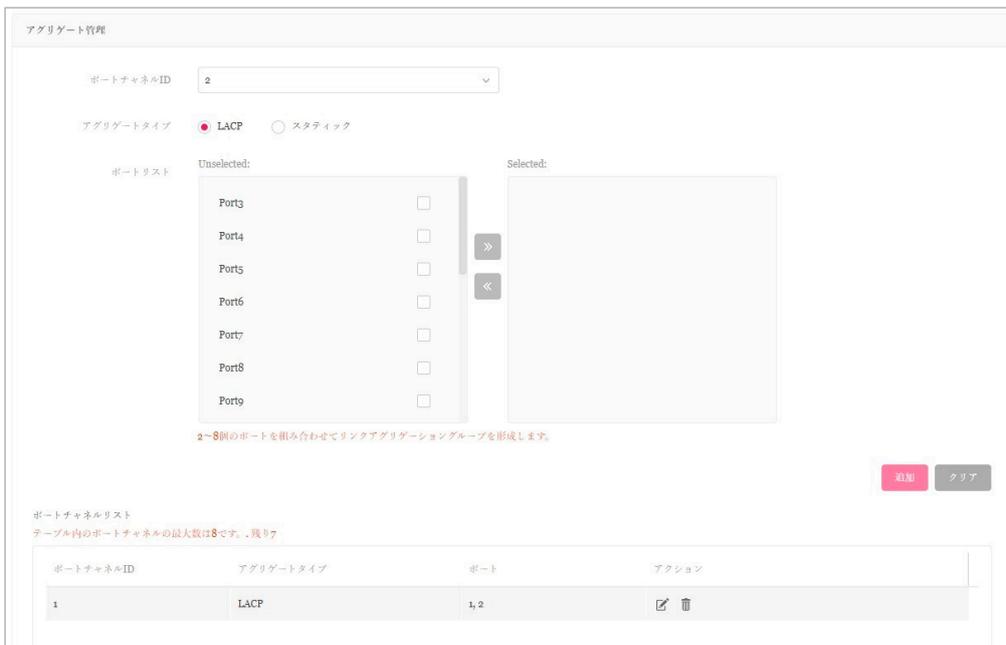


図 6-17 アグリゲート管理

■ アグリゲーショングループの作成

- 「ポートチャネル ID」ドロップダウンメニューから、1~8 を選択します。
- 「アグリゲートタイプ」として「LACP」または「スタティック」を選択します。
- 「ポート」リストから、2~8 個のポートを選択します。
- 「追加」をクリックして、リンクアグリゲーショングループを形成します。
設定をキャンセルするには、「クリア」をクリックします。
- 「適用」をクリックして設定をスイッチに適用します。

■ ポートチャネルリスト

「ポートチャネルリスト」に、作成したリンクアグリゲーションの概要が表示されます。
「ポートチャネル ID」「アグリゲートタイプ」「ポート (番号)」が表示されます。

■ アグリゲーショングループの編集・削除

「アクション」フィールドで、 をクリックしてアグリゲーショングループを編集します。設定完了後、「保存」をクリックして設定を保存します。グループを削除する場合は、対象グループの  をクリックします。

「適用」をクリックして設定をスイッチに適用します。

ミラー管理

「ミラー管理」セクションでは、スイッチポートのネットワークパケットを別のポートにミラーリングできます。

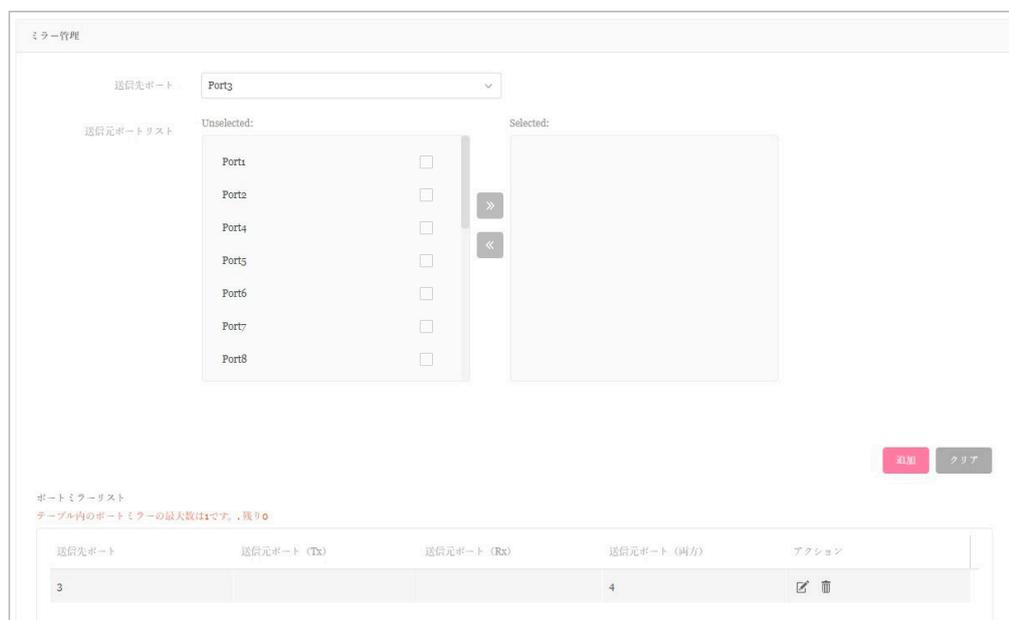


図 6-18 ミラー管理

■ ミラーリングの作成

1. ドロップダウンメニューから「送信先ポート」を選択します。
2. 「送信元ポートリスト」ミラーリングするポートを選択します。
3. 選択したポートについて、ミラーリングするトラフィックのタイプ（「Both（両方）」「Rx」「Tx」）を選択します。
4. 「追加」をクリックして、エントリを保存します。
設定をキャンセルするには、「クリア」をクリックします。
5. 「適用」をクリックして設定をスイッチに適用します。

■ ポートミラーリスト

「ポートミラーリスト」には、ミラーリングしたポートの概要が表示されます。「送信先ポート」「送信元ポート (Tx/Rx/Both)」が表示されます。

■ ミラーリングの編集・削除

「アクション」フィールドで、 をクリックしてエントリを編集します。設定完了後、「保存」をクリックして設定を保存します。エントリを削除する場合は、対象エントリの  をクリックします。

「適用」をクリックして設定をスイッチに適用します。

クライアント情報

「クライアント情報」セクションに、クライアント情報の概要が表示されます。

No.	クライアントMACアドレス	クライアントIPv4アドレス	ポート	VLAN	LLDP	製造	最終更新情報
1	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59
2	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59
3	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 14:42:46
4	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59
5	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59
6	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59
7	xxxxxx:xxxx:xxxx	-	1	1	-	-	2022/11/17 11:27:59

図 6-19 クライアント情報

■ クライアント情報の表示・検索

- 「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、キーワードを入力し、 をクリックして検索を開始します。

以下の項目が表示可能です。表示項目を変更するには、 をクリックします。

- 「サイト」「ネットワーク」「クライアント MAC アドレス」「クライアント IPv4 アドレス」「ポート」「VLAN」「LLDP」「製造」「最終更新情報」
 - 「ポート」では、クライアントが接続されているスイッチのポート番号を表示します。ポート番号をクリックすると、ポート詳細画面が開きます。
 - 「LLDP」では、隣接機器の LLDP 情報を表示します。
 - 「製造」では、LLDP 経由のリモートデバイスの製造名を表示します。
 - 「最終更新情報」では、ネットワーク上でクライアントが最後に検出された時刻を表示します。

IP インタフェースタブ

「IP インタフェース」タブでは、IPv4 インタフェースを設定したり、概要を表示することができます。

補足 スイッチ製品は未サポートです。

Default 15:00:18 2022-11-17

基本 ポート IP インタフェース ルーティング ツール

IPv4 インタフェース

VLAN ID: 1

ステート: 有効化

IP アドレス*

ネットマスク*

適用 クリア IP 接続が DHCP モードであり、IP インタフェースを追加できません。

IPv4 インタフェーステーブルのエントリの最大数は4です。残り3

VLAN ID	ステート	IP アドレス	リンクステータス...	アクション
1	有効化	172.16.1.59 / 255.255.255.0	Up	

適用

図 6-20 デバイス詳細 - IP インタフェースタブ

■ IPv4 インタフェースの作成

1. 「VLAN ID」を選択して、インタフェース管理の「ステート（状態）」を有効または無効に設定します。
2. IPv4 IP アドレスとネットマスクを入力します。
3. 「追加」をクリックして、IP インタフェースを VLAN に適用します。
設定をキャンセルするには、「クリア」をクリックします。
4. 「適用」をクリックして、設定をスイッチに適用します。

■ IPv4 インタフェーステーブル

「IPv4 インタフェーステーブル」には、「VLAN ID」「ステート」「IP アドレス」「リンクステータス」が表示されます。

■ インタフェースの編集・削除

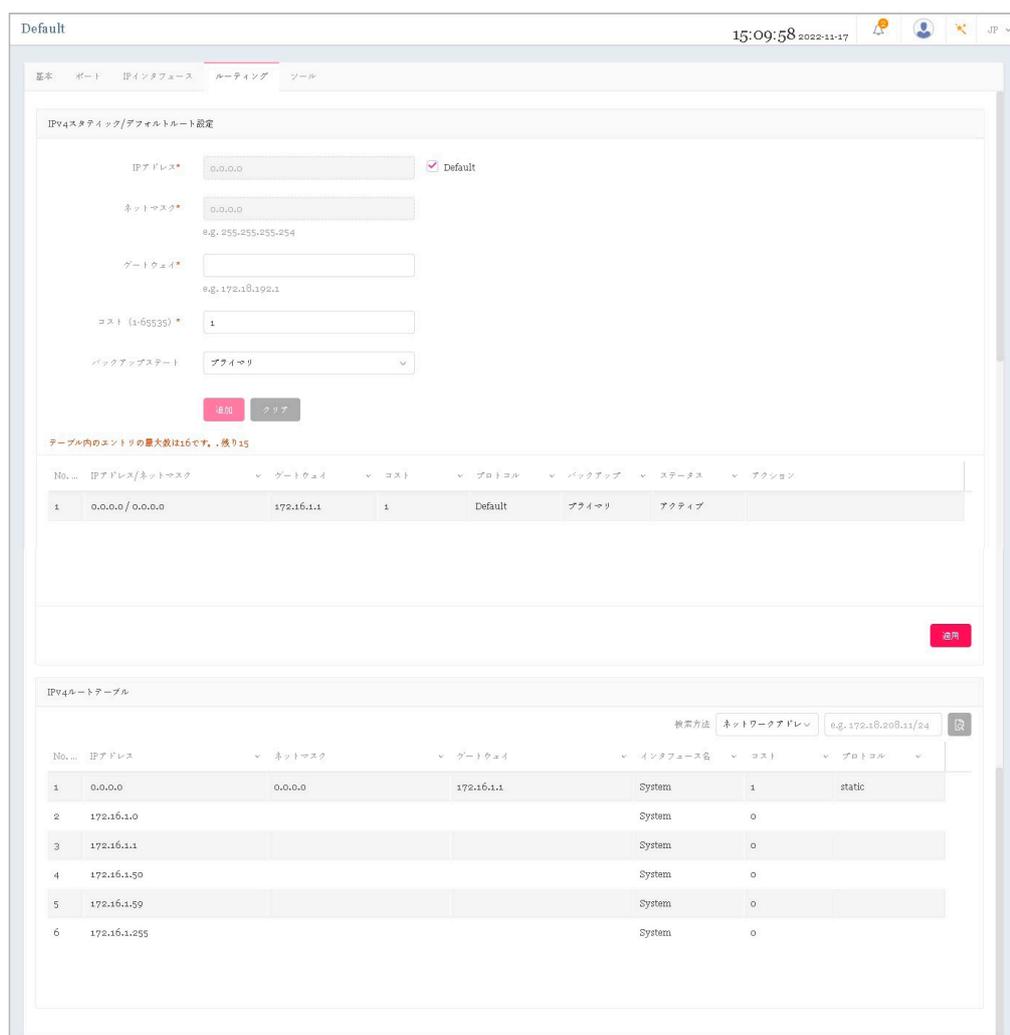
「アクション」フィールドで、 をクリックしてインタフェースを編集します。設定完了後、「保存」をクリックして設定を保存します。インタフェースを削除する場合は、対象インタフェースの  をクリックします。

「適用」をクリックして、設定をスイッチに適用します。

ルーティングタブ

「ルーティング」タブでは、IPv4 アドレスのスタティックルーティングを設定できます。

補足 スイッチ製品は未サポートです。



The screenshot displays the 'IPv4スタティック/デフォルトルート設定' (IPv4 Static/Default Route Configuration) page. It includes a configuration form with the following fields:

- IPアドレス*: 0.0.0.0 (checked as Default)
- ネットマスク*: 0.0.0.0 (example: 255.255.255.254)
- ゲートウェイ*: (example: 172.16.1.1)
- コスト (1-65535)*: 1
- バックアップステート: プライマリ

Buttons for '適用' (Apply) and 'クリア' (Clear) are present. Below the form is a table of configured routes:

No.	IP アドレス/ネットマスク	ゲートウェイ	コスト	プロトコル	バックアップ	ステータス	アクション
1	0.0.0.0 / 0.0.0.0	172.16.1.1	1	Default	プライマリ	アクティブ	

At the bottom, the 'IPv4ルートテーブル' (IPv4 Routing Table) is shown with a search method of 'ネットワークアドレス' and a search value of 'e.g. 172.16.208.11/24':

No.	IP アドレス	ネットマスク	ゲートウェイ	インタフェース名	コスト	プロトコル
1	0.0.0.0	0.0.0.0	172.16.1.1	System	1	static
2	172.16.1.0			System	0	
3	172.16.1.1			System	0	
4	172.16.1.50			System	0	
5	172.16.1.59			System	0	
6	172.16.1.255			System	0	

図 6-21 デバイス詳細 - ルーティングタブ

■ IPv4 スタティック / デフォルトルート設定

1. 「IP アドレス」「ネットマスク」を入力、または「Default」にチェックを入れます。
2. 「ゲートウェイ」「コスト」を入力し、「バックアップステート（プライマリ/バックアップ）」を選択します。

第6章 モニタ

- 「追加」をクリックして、ルート設定を保存します。
設定をキャンセルするには、「クリア」をクリックします。
- 「適用」をクリックして、設定をスイッチに適用します。

■ スタティックルートテーブルの表示

「IPv4 スタティック/デフォルトルート設定」の下部には、スタティックルートの一覧が表示されます。

- 「IP アドレス/ネットマスク」「ゲートウェイ」「コスト」「プロトコル」「バックアップ」「ステータス」が表示されます。

■ スタティックルートの編集・削除

「アクション」フィールドで、 をクリックしてルートを編集します。設定完了後、「保存」をクリックして設定を保存します。

ルートを削除する場合は、対象エントリの  をクリックします。

「適用」をクリックして、設定をスイッチに適用します。

■ IPv4 ルートテーブル

IPv4 ルートテーブルには、スイッチのルート情報が格納されます。以下の項目が表示されます。

- 「IP アドレス」「ネットマスク」「ゲートウェイ」「インタフェース名」「コスト」「プロトコル」

「検索方法」ドロップダウンメニューから検索条件（ネットワークアドレス / IP アドレス）を選択し、アドレスを入力、 をクリックしてエントリを検索することができます。

電源タブ

「電源」タブには、「システム消費電力」のグラフと「PoE ポートステート」の一覧が表示されます。「電力」タブは、PoE 対応スイッチのみ表示されます。

補足 スイッチ製品は未サポートです。

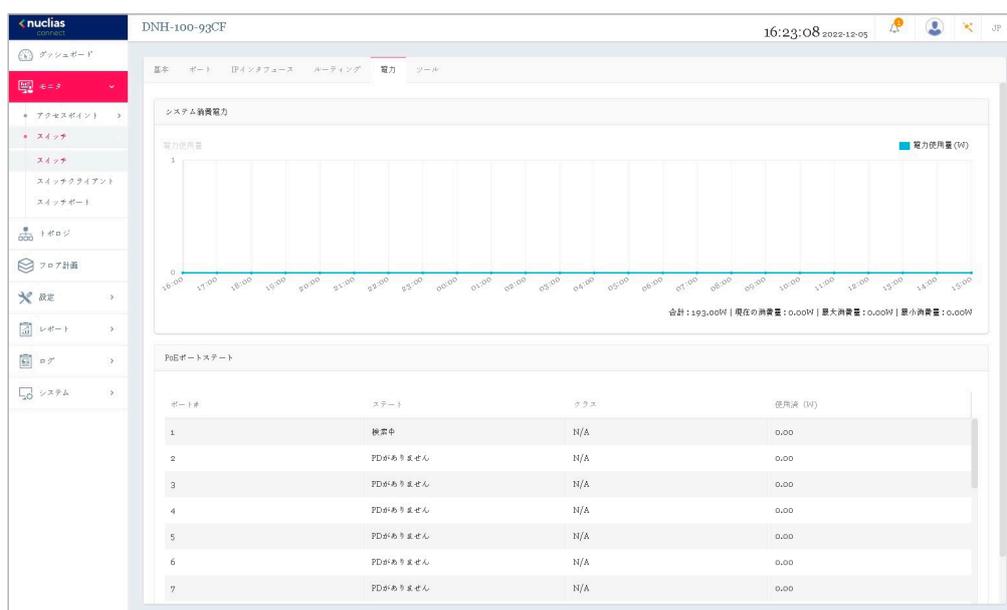


図 6-22 デバイス詳細 - 電源タブ

■ システム消費電力

「システム消費電力」のグラフには、スイッチの電力使用量 (W) が時間単位で表示されます。

また、合計 / 現在の消費量 / 最大消費量 / 最小消費量 も確認することができます。

■ PoE ポートステート

「PoE ポートステート」の一覧には、以下の項目が表示されます。

項目	説明
ポート #	ポート番号が表示されます。
ステータス	PoE ポートのステータスが表示されます。
クラス	IEEE 分類（「N/A」または IEEE クラス 0~4 の値）が表示されます。
使用済 (W)	現在 PoE ポートで使用されている電力量 (W) が表示されます。

ツールタブ

「ツール」タブには、トラブルシューティングに役立つ以下のツールが用意されています。

- ・「Ping」「MAC 転送テーブル」「ケーブルテスト」「サイクル PoE」「デバイスの検索」「他のデバイスに設定をコピー」

デバイスがオフラインの場合、ツールは無効になります。

補足 スイッチ製品は未サポートです。

Ping

Ping ツールを使用すると、デバイスへの接続可否を判断できます。

図 6-23 Ping

1. ホスト名または IP アドレスを入力し、「Ping」をクリックして ping テストを実行します。
2. サーバが ping 信号を受信すると、Ping 統計の概要（Packets: Sent/Received/Lost）が表示されます。信号を受信されない場合、デバイスに到達不能であることを示すメッセージが表示されます。

MAC 転送テーブル

MAC フォワーディングテーブルには、「MAC アドレス」「VLAN」「ポート」「(IP アドレス) タイプ」が表示されます。

図 6-24 MAC 転送テーブル

「実行」をクリックして処理を開始します。

「MAC」フィールドで、MAC アドレスの検索に役立つ関連キーワードを入力し、をクリックして検索を開始します。

ケーブルテスト

ケーブルテストでは、1つまたは複数のポートの接続をテストできます。

ケーブルテスト

このポートでケーブルテストを実行

ポート テスト

e.g. 1-5,7,11,20-23

警告: このテストは、デバイスへの通信を中断します。

ケーブルテスト結果

ポート	タイプ	リンクステータス...	テスト結果	ケーブル長(M)
データが見つかりませんでした				

図 6-25 ケーブルテスト

1. ポート番号を入力し、「テスト」をクリックしてケーブルテストを開始します。
2. 「ポート (番号)」「タイプ」「リンクステータス」「テスト結果」「ケーブル長」の情報が表示されます。「テスト結果」の欄には、「OK」「Open」「Short」「Test failed」「-」のいずれかのステータスが表示されます。

注意 ケーブルテストにより、デバイスへのトラフィックが中断されます。

サイクル PoE

サイクル PoE 機能を使用すると、特定のポートで PoE を無効化してから再度有効化することができます。

このツールは、PoE が有効な場合にのみ実行できます。スイッチが PoE をサポートしていない場合、このセクションは無効になります。

サイクルPoE

PoEを無効化して、再度有効化

ポート テスト

e.g. 1-5,7,11,20-23

PoEはスイッチでサポートされていません。

警告: PoE受電デバイスは一時的にパワーダウンします。

サイクルPoEテスト結果

図 6-26 サイクル PoE

デバイスの検索

「デバイスの検索」機能は、スイッチのLEDを点灯させることで、ラベルの付いていないスイッチを特定する場合に役立ちます。



図 6-27 デバイスの検索

1. 「開始」をクリックすると、スイッチが点灯します。すべてのLEDが5分間緑色に点灯します。
2. デバイスが見つかったら、「デバイスの検索結果」に「Locating device」というメッセージが表示されます。デバイスが見つからない場合は、「The device is unreachable」というメッセージが表示されます。スイッチから障害メッセージを受信すると、「Locate device failed」というメッセージが表示されます。
3. 手動で点灯を停止するには、「停止」ボタンをクリックします。

他のデバイスに設定をコピー

本機能を使用すると、以下の設定をネットワーク内の他のデバイスにコピーできます。

- ユーザ設定モード、VLAN設定、IGMPスヌーピング設定、ポート設定、アグリゲート管理、ミラー管理

注意 コピー元とコピー先の2つのデバイスは同じモデルである必要があります。



図 6-28 他のデバイスに設定をコピー

1. コピー先となるネットワーク内のスイッチを選択します。
2. 「コピー」をクリックして、お使いのデバイスから選択したデバイスに設定をコピーします。

第6章 モニタ

3. 確認画面が表示されるので、「コピー」をクリックして続行します。
処理をキャンセルする場合には、「キャンセル」をクリックします。

スイッチ-スイッチクライアント

左側のパネルからモニタ>スイッチ>スイッチクライアントをクリックします。

本画面には、スイッチネットワークに接続されているすべてのアクティブなクライアントデバイスの履歴一覧が表示されます。

補足 スイッチ製品は未サポートです。

No.	クライアントMACアドレス	クライアントIPv4アドレス	スイッチMACアドレス	スイッチ名	ポート	VLAN	LLDP	製造	最終更新情報
1	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
2	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
3	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
4	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 16:28...
5	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
6	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
7	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
8	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
9	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 16:30...
10	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 16:33...
11	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 16:26...
12	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	70-89-C2-CF...	-	2022/11/17 11:29...
13	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...
14	08:00:27:00:00:00	-	08:00:27:00:00:00	-	1	1	-	-	2022/11/17 11:27...

図 6-29 モニタ-スイッチ-スイッチクライアント

■ 対象範囲の指定 / クライアントの検索

- ・ 左上のドロップダウンメニューから「サイト」「ネットワーク」を指定して、 をクリックします。
- ・ スイッチ (MAC アドレス) を指定し、「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、検索フィールドにキーワードを入力し、 をクリックして検索を開始します。

■ レポート項目

各スイッチクライアントについて、以下の項目を表示することができます。表示項目を変更するには、 をクリックします。

- ・ サイト
- ・ ネットワーク
- ・ クライアント MAC アドレス
- ・ クライアント IPv4 アドレス
- ・ スイッチ MAC アドレス
- ・ スイッチ名
- ・ ポート
- ・ VLAN
- ・ LLDP
- ・ 製造
- ・ 最終更新情報

- 「スイッチ MAC アドレス」では、クライアントが接続されているスイッチの MAC アドレスを表示します。MAC アドレスをクリックすると、スイッチの詳細画面が開きます。
- 「ポート」では、クライアントが接続している D-Link スイッチのポート番号を表示します。ポート番号をクリックすると、該当ポートの詳細画面が開きます。

スイッチ - スイッチポート

左側のパネルからモニタ > スイッチ > スイッチポートをクリックします。

補足 スイッチ製品は未サポートです。

本画面では、すべてのサイトおよびネットワークのすべてのスイッチポートのステータスを表示できます。

No.	SWITCH/PORT	アクション	アグリゲート名	リンク	ポートタイプ	VLAN	許可されたVLAN	ポートステータス	PoE	ポート	RSTP	LBD
7	/7	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
8	/8	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
9	/9	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
10	/10	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
11	/11	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
12	/12	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
13	/13	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
14	/14	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
15	/15	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
16	/16	⊕	-	自動/トランク	アクセス	1	-	有効化	無効化	20	有効化	無効化
17	/17	⊕	-	RJ45:自動/-	アクセス	1	-	有効化	無効化	20	有効化	無効化
18	/18	⊕	-	RJ45:自動/-	アクセス	1	-	有効化	無効化	20	有効化	無効化
19	/19	⊕	-	RJ45:自動/-	アクセス	1	-	有効化	無効化	20	有効化	無効化
20	/20	⊕	-	RJ45:自動/-	アクセス	1	-	有効化	無効化	20	有効化	無効化

図 6-30 モニタ - スイッチ - スイッチポート

■ 対象範囲の指定 / ポートの検索

- ・ 左上のドロップダウンメニューから「サイト」「ネットワーク」を指定して、 をクリックします。
- ・ 以下のフィルタリング項目を指定し、関連するキーワードを入力して をクリックして検索を開始します。
 - 「ポートグループ」(ポート数)
 - 「スイッチ」(スイッチ MAC アドレス)
 - 「検索方法」: 「VLAN」または「ポート」
 - (VLAN を指定した場合) 「ポートタイプ」: 「全てのタイプ」「アクセス」「トランク」

■ レポート項目

各スイッチポートについて、以下の項目を表示することができます。表示項目を変更するには、 をクリックします。

- ・ SWITCH/PORT
 - ・ アグリゲート
 - ・ リンク
 - ・ ポートタイプ
 - ・ VLAN
 - ・ 許可された VLAN
 - ・ ポートステータス
 - ・ PoE
 - ・ ポート
 - ・ RSTP
 - ・ LBD
 - ・ DDP
 - ・ ポートシャットダウンスケジュール
 - ・ PoE 供給スケジュール
 - ・ アクセスポリシー
 - ・ ミラー
 - ・ LLDP
 - ・ ポート名
 - ・ Rx ブロードキャストパケット
 - ・ Tx ブロードキャストパケット
 - ・ Rx マルチキャストパケット
 - ・ Tx マルチキャストパケット
 - ・ Rx バイト数
 - ・ Tx バイト数
 - ・ Rx パケット数
 - ・ Tx パケット数
 - ・ 合計バイト数
- 「SWITCH/PORT」では、スイッチ名とポート番号を表示します。
 - 「アグリゲート」では、ポートチャネルグループのリンクアグリゲーションタイプ (Static/LACP/-) を表示します。
 - 「リンク」では、ポートのリンク設定とリンク状態を表示します。

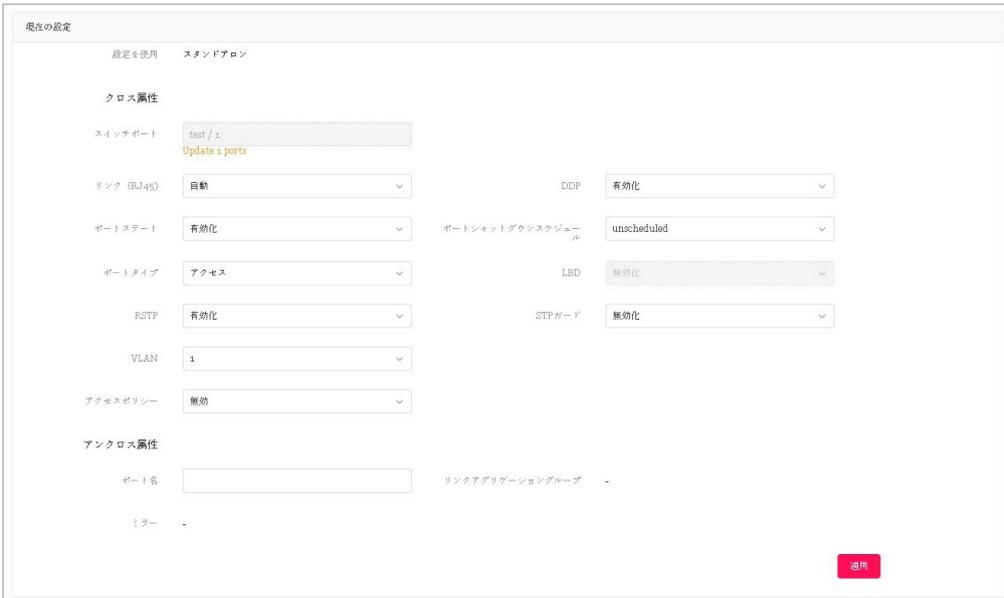
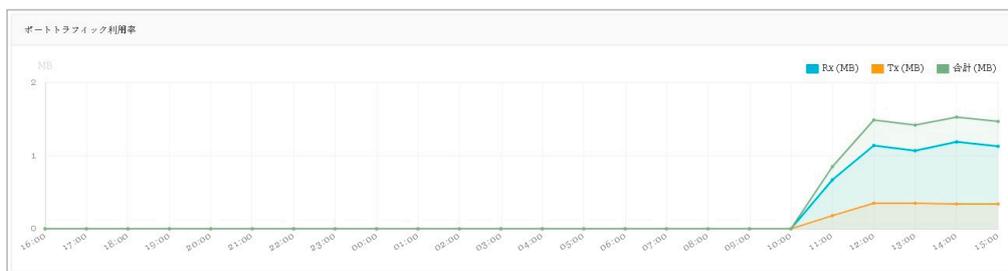
第6章 モニタ

■ 特定ポートの詳細

「アクション」欄で、 をクリックしてポート詳細画面に移動します。選択したスイッチの特定のポートの詳細画面が表示されます。

ポートの詳細画面では、以下の情報が表示されます。

- ・「Overview (ポート接続ステータス)」 「ポートトラフィック利用率」 「現在の設定」 「ステータス」 「トラブルシューティング (ケーブルテスト、サイクル PoE)」 「パケット概要」 「クライアント情報」



現在の設定

設定を使用 スタンドアロン

クロス属性

スイッチポート: test / 1
 Update 1 ports

リンク (RJ45): 自動 DDP: 有効化

ポートステート: 有効化 ポートシャットダウンスケジュール: unscheduled

ポートタイプ: アクセス LBD: 無効化

RSTP: 有効化 STPガード: 無効化

VLAN: 1

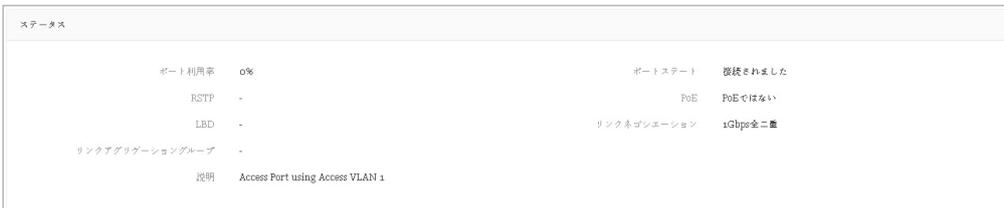
アクセスポリシー: 無効

アックロス属性

ポート名: リンクアグリゲーショングループ: -

ミラー: -

適用



ステータス

ポート利用率	0%	ポートステート	接続されました
RSTP	-	PoE	PoEではない
LBD	-	リンクネゴシエーション	1Gbps全二重
リンクアグリゲーショングループ	-		
説明	Access Port using Access VLAN 1		

トラブルシューティング

ケーブルテスト

このポートでケーブルテストを実行

テスト

警告: このテストは、デバイスへの通信を中断します。

ケーブルテスト結果

ポート	タイプ	リンクステ...	テスト結果	ケーブル長(M)
データが見つかりませんでした				

サイクルPoE

PoEを無効化して、再度有効化

テスト PoEがスリッパでポートされていません。

警告: PoE変更デバイスは一時的にパワーダウンします。

サイクルPoEテスト結果

パケット概要

タイムフレーム **Last 15 Minut**

	合計	Rx	Tx	レート (Rx, Tx)
Total Traffic	2904	2683	221	-
Broadcast	1954	1954	0	-
Multicast	581	581	0	-
CRC Error	0	0	-	-
Discard	1347	1347	0	-
Fragment	0	0	-	-
Collision	0	-	0	-
Error	0	0	0	-

クライアント情報

検索方法 **Client MAC Address** e.g. 3c11e1-0416-53120

No.	クライアントMACアドレス	クライアントIPv4アドレス	VLAN	LLDP	製造	最終更新情報
1	000c291251443b	-	1	-	-	2022/11/17 11:27:59
2	001cf01faebf	-	1	-	-	2022/11/17 11:27:59
3	0080c4c6810bc4e	-	1	-	-	2022/11/17 11:27:59
4	6c119b8f1b8778b	-	1	-	-	2022/11/17 11:27:59
5	6c119b8f1b87789	-	1	-	-	2022/11/17 11:27:59
6	9cd643104134101	-	1	-	-	2022/11/17 11:27:59
7	9cd643104135113	-	1	-	-	2022/11/17 11:27:59

第7章 トポロジ

トポロジ画面では、ネットワーク内のデバイス間のトポロジ関係を表示します。

トポロジ画面を開くと、メイン画面にネットワークトポロジ図が表示され、右側にネットワークとデバイスの概要が表示されます。ネットワークとデバイスの概要には、ネットワーク名、所属サイト、範囲、合計デバイス数、オンラインデバイス数といった情報が含まれます。

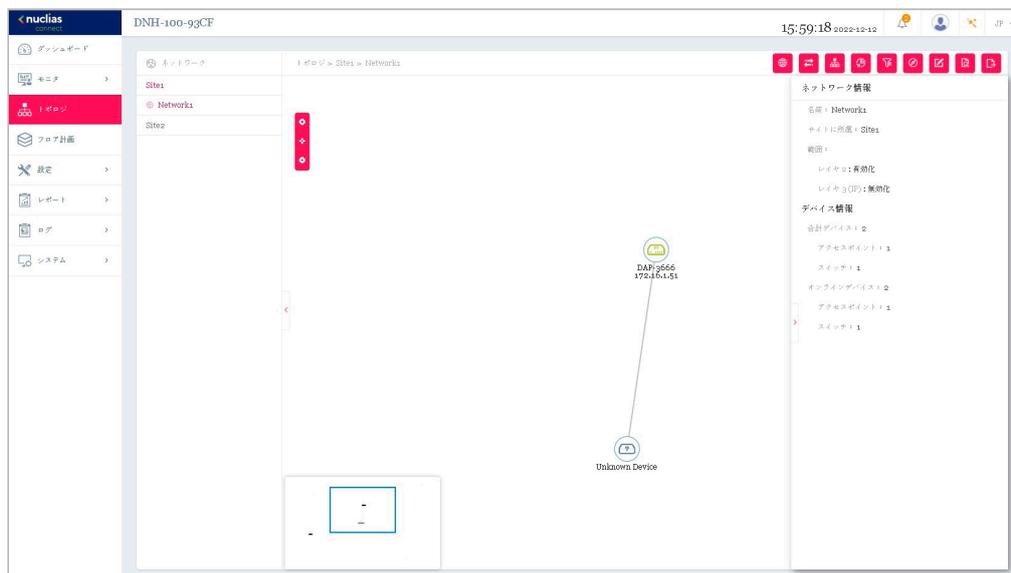


図 7-1 トポロジ

■ 詳細情報の確認

デバイスのアイコンをダブルクリックすると、右側にデバイスの情報が表示されます。

デバイス情報の ⓘ をクリックすると、デバイスの詳細画面が開きます。

リンクをダブルクリックすると、リンク情報が表示されます。

■ トポロジの表示の調整

🔍 (拡大)、🔍 (縮小)、🔄 (リセット) をクリックして、トポロジの拡大縮小などを行います。

デバイス情報

デバイス情報には以下の項目が表示されます。

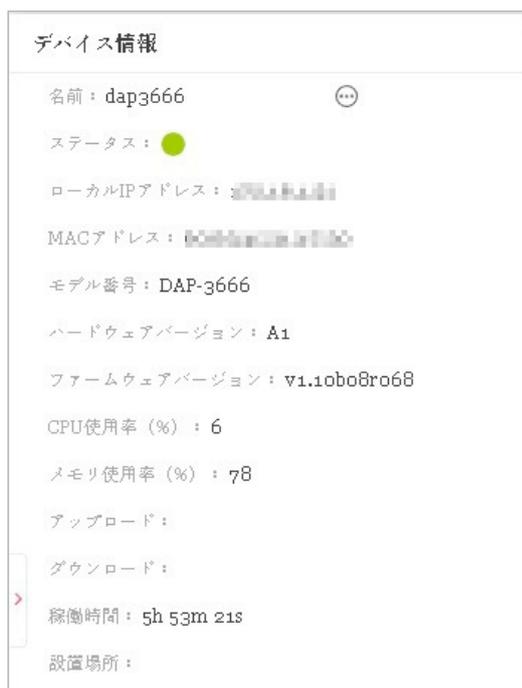


図 7-2 デバイス情報

項目	説明
アクセスポイント	
名前	サーバ上でアクセスポイントを識別するための名前を表示します。☺をクリックすると、デバイス詳細画面に遷移します。AP名はサイトに対して一意である必要があります。
ステータス	APの接続ステータス（オンライン、オフライン）が表示されます。緑色はオンライン、赤色はオフラインを示します。
ローカルIPアドレス	IPアドレスを表示します。
MACアドレス	アクセスポイントのシステムMACアドレスを表示します。
モデル番号	アクセスポイントの型番を表示します。
ハードウェアバージョン	アクセスポイントのハードウェアバージョンを表示します。
ファームウェアバージョン	ファームウェアバージョンを表示します。
CPU使用率 (%)	アクセスポイントのCPU使用率を表示します。
メモリ使用率 (%)	アクセスポイントのメモリ使用率を表示します。
アップロード	アクセスポイントのアップロードトラフィックを表示します。
ダウンロード	アクセスポイントのダウンロードトラフィックを表示します。
稼働時間	前回の起動または再起動後からのAPの稼働時間を表示します。
設置場所	デバイスの設置場所を表示します。
スイッチ	
名前	サーバ上でスイッチを識別するための名前を表示します。☺をクリックすると、デバイス詳細画面に遷移します。スイッチ名はサイトに対して一意である必要があります。
ステータス	スイッチの接続状態（オンラインまたはオフライン）を表示します。緑色はオンラインを示し、赤色はオフラインを示します。
ローカルIPアドレス	IPアドレスを表示します。
MACアドレス	スイッチのシステムMACアドレスを表示します。
モデル番号	スイッチの型番を表示します。
シリアル番号	スイッチのシリアル番号を表示します。
IGMPスヌーピング	IGMPスヌーピングのステータス（有効化/無効化）を表示します。
ハードウェアバージョン	スイッチのハードウェアバージョンを表示します。
ファームウェアバージョン	スイッチのファームウェアバージョンを表示します。
CPU使用率 (%)	スイッチのCPU使用率を表示します。
タイムゾーン	デバイスが属するタイムゾーンを表示します。
RSTPルート	ルートブリッジとそのスパンニングツリープライオリティを表示します。表示形式は以下の通りです。 <ul style="list-style-type: none"> 「ルートは [X]/ ルートブリッジプライオリティ:Y」- [X] はルートスイッチのデバイス名(システム名)を表します。[Y] はルートスイッチのブリッジプライオリティを表します。 「RSTPは無効化されています。」- スイッチでRSTPが有効になっていません。RSTPは、ポートではなくスイッチでのみ有効になります。 「-」- スイッチがオフライン、または情報を中継しないことを意味します。
LBD	スイッチのLBD設定のステータス（有効化/無効化）を表示します。
DDP	スイッチのDDP設定のステータス（有効化/無効化）を表示します。
稼働時間	前回の起動または再起動後からのスイッチの稼働時間を表示します。
設置場所	スイッチの設置場所を表示します。

リンクの作成

デバイス間のリンクを手動で定義することができます。

1.  をクリックして、編集を開始します。
2. ターゲットデバイスアイコンのいずれかをクリックすると、リンクの線を引っ張ることができます。別のデバイスアイコンをクリックしてリンクを作成します。

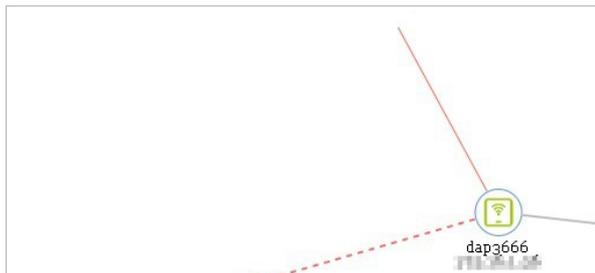


図 7-3 リンクの作成

3. リンクが作成されると、リンク設定画面が表示されます。



図 7-4 リンク設定

4. リンクタイプとリンクポートを設定し、「OK」をクリックします。
5.  (保存して終了) をクリックして変更を保存します。

トポロジ情報の設定と表示

右上には、スイッチとアクセスポイントの基本情報を変更および確認するためのオプションがあります。

各アイコンの説明は以下の通りです。

項目	説明
ネットワーク情報を表示 	ネットワークとデバイスの情報を表示します。
背景画像を変更 	トポロジの背景イメージを変更します。
自動アレンジ 	トポロジのリンクタイプ (Star/Tree) と中央デバイスを設定します。
トポロジーの凡例 	トポロジーの凡例 (トポロジで使用されるシンボルと色の意味) を表示します。
ディスプレイに接続 	ノード情報 (IP アドレスや名前) の表示内容を設定します。
再検出 	トポロジを再検出します。
検索 	ネットワーク内の管理デバイスを検索します。
エクスポート 	トポロジを PDF ファイルとしてエクスポートします。

第8章 フロア計画

フロア計画は、スケーリングを行うための描画であり、部屋、空間、交通パターンなど、物理的性質の関係を全体図で表示します。

1. "ここ"をクリックします。

1つ以上のフロアプランが定義されている場合、左側にフロア計画の一覧が表示されます。**+** をクリックして新規にフロアプランを作成します。



図 8-1 フロア計画

2. フロアプランの名前を入力して、サイトとネットワークを選択します。
3. 「画像を選択」をクリック、またはドラッグ&ドロップにより画像をアップロードします。

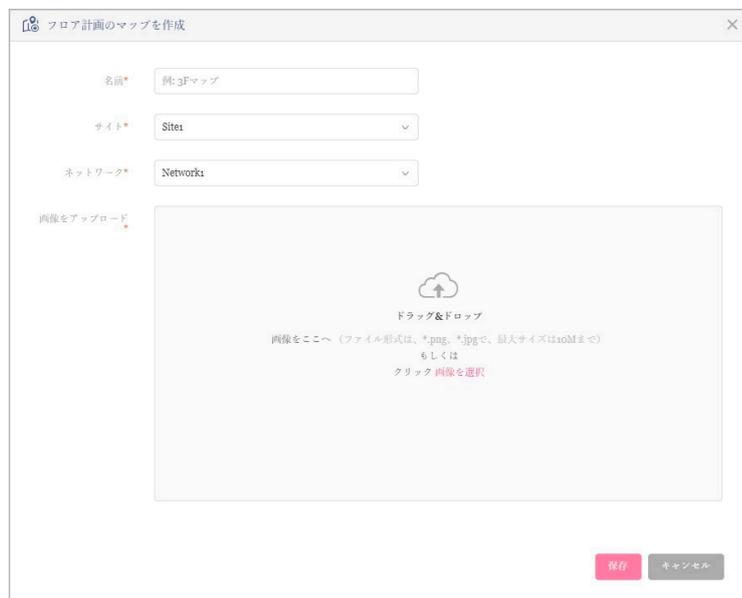


図 8-2 フロア計画のマップを作成

第8章 フロア計画

4. 「デバイスを選択」をクリックしてデバイスを選択し、画像内に配置します。
デバイスアイコンをクリックしたまま、デバイスを適切な位置に移動します。

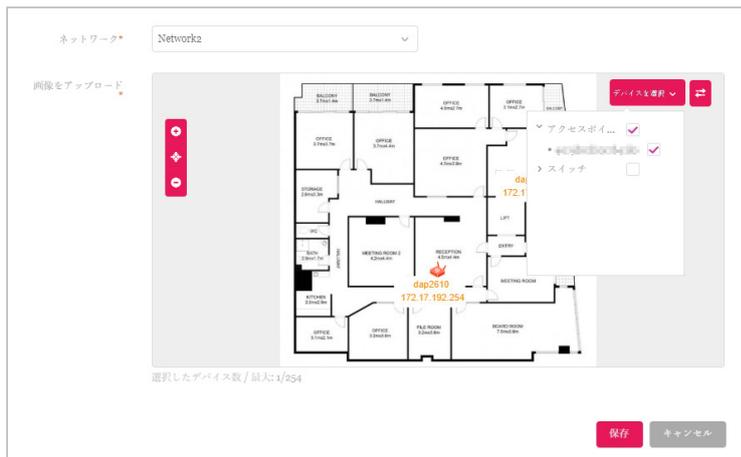


図 8-3 デバイスの配置

5. 「保存」をクリックします。

デバイスアイコンは、接続ステータスの色（オンライン：緑、オフライン：赤）で表示されます。

デバイスアイコンの上にマウスオーバーすると、デバイス情報（名前、モデル番号、IP アドレスなど）を確認することができます。

第9章 設定

- 「プロファイルの作成」
- 「プロファイル設定」
- 「ファームウェアの更新」
- 「SSL 証明書」
- 「決済代行システム ※本項目は日本ではサポート対象外となります。」

プロファイルの作成

設定 > プロファイルを作成に移動し、「ネットワークを追加」をクリックして、新しいサイトやネットワークを作成することができます。

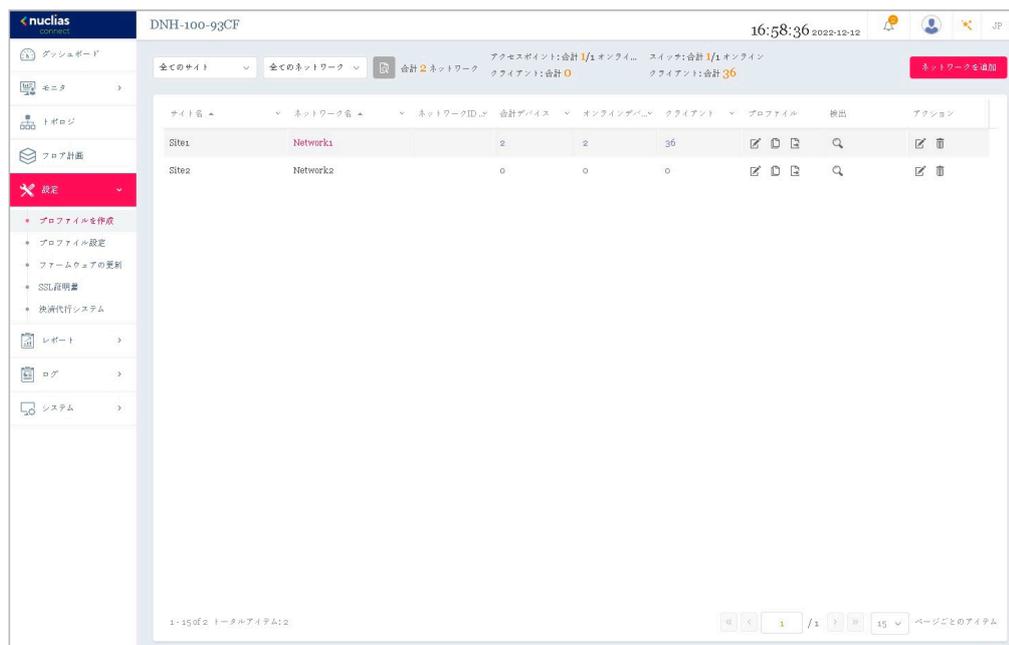


図 9-1 プロファイルを作成

既存のネットワークに対しては、以下の操作を実行することができます。

項目	説明
プロファイルを編集	選択したサイトのプロファイル設定画面を開きます。セキュリティ、アクセスコントロール、ユーザ認証などの設定を編集できます。
このネットワークにプロファイルをコピー	既存のプロファイルを指定したサイトとネットワークにコピーします。
ネットワークプロファイルをエクスポート	選択したプロファイル (*.dat) をローカルディレクトリにエクスポートします。
検出	「ネットワーク設定を検出」画面を開きます。この画面から、L2 プロトコル層に配置されているデバイス、または特定の IP アドレス / プレフィックスサブネット IP を検索できます。 (1) 条件を定義し、「次へ」をクリックします。 (2) 「検出開始」をクリックして、デバイスを検出します（「設定可能」「管理」タブ）。
ネットワークを編集	「ネットワークを編集」画面を開きます。この画面から、ネットワーク設定を編集したり、新しいサイトまたは既存のサイトに移行したりすることができます。
ネットワークを削除	選択したネットワーク設定を削除します。

ネットワークの追加

1. 新しいネットワークを作成するには、「プロファイルを作成」画面で「ネットワークを追加」ボタンをクリックします。



図 9-2 プロファイルを作成

2. 「ネットワークを追加」画面で、以下の項目を設定します。
「次へ」をクリックして次に進みます。前のページに戻るには「戻る」をクリックします。

- (1) 「サイト」ドロップダウンメニューから既存のサイトを選択するか、新しいサイト（newSite）を選択し、空のフィールドにサイトの名前を入力します。
- (2) 「ネットワーク名」フィールドに、新しいネットワークの名前を入力します。
- (3) 「ネットワークID」フィールドはオプションで、REST API機能に使用されます。REST APIを使用しない場合は、入力する必要はありません。



図 9-3 ネットワークを追加

注意 サイト名やネットワーク名にバックスラッシュが含まれる場合、CLIで処理することができませんのでご注意ください。

3. 「ネットワーク設定」画面が表示されます。「アクセスポイント」にチェックを入れ、ネットワーク設定を定義します。
「次へ」をクリックして次に進みます。前のページに戻るには「戻る」をクリック、設定プロセスを中止するには「キャンセル」をクリックします。

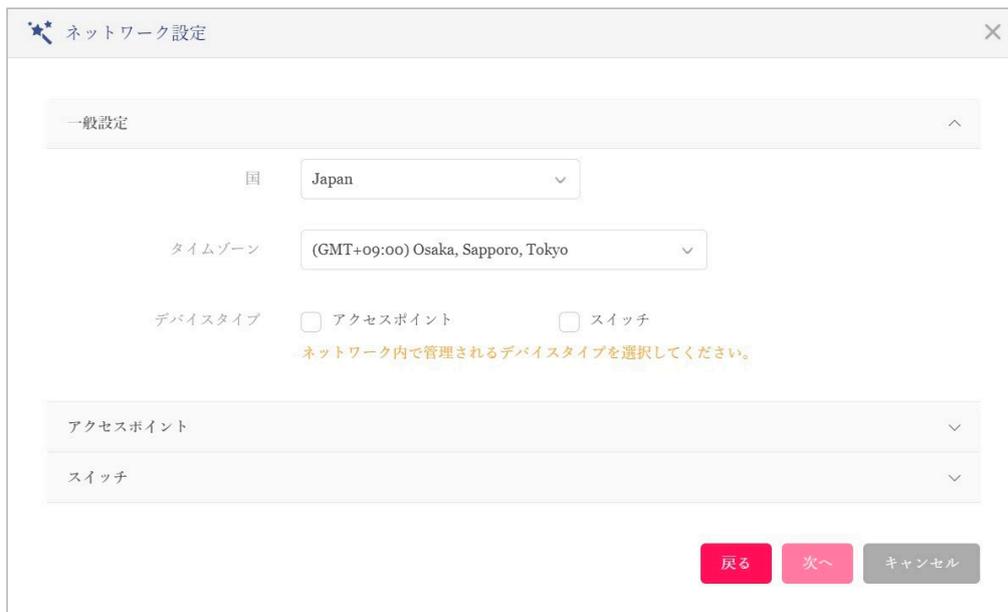


図 9-4 ネットワークの設定

補足 スイッチ製品は未サポートです。

4. 「ネットワーク設定を検出」画面が表示されます。データリンクレイヤ（「レイヤ2」または「レイヤ3（IP）」）を選択して、ネットワーク検出を実行するネットワークのタイプを定義します。「次へ」をクリックして続行します。設定プロセスを中止するには「キャンセル」をクリックします。

レイヤ3が選択されている場合は、ドロップダウンメニューをクリックして、IPまたはプレフィックスセグメンテーションのいずれかを定義します。**+**をクリックして追加のIP/プレフィックスセグメントを追加します。

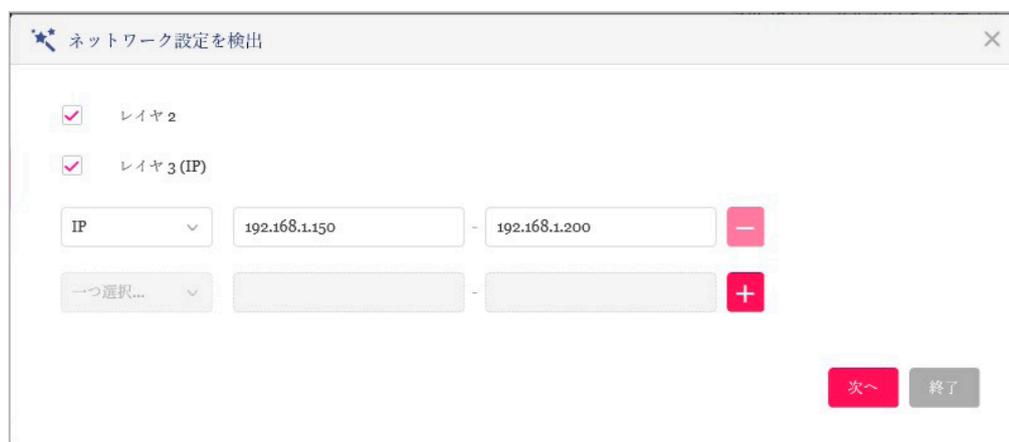


図 9-5 ネットワーク設定を検出

5. 「APを検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを検出・表示します。
6. デバイスが検出された場合は、そのデバイスを選択して「インポート」をクリックし、ネットワークプロファイルをインポートします。インポート操作により、定義したネットワークも作成されます。「管理」タブをクリックして、定義済みのデバイスを選択し、このネットワークに追加することもできます。

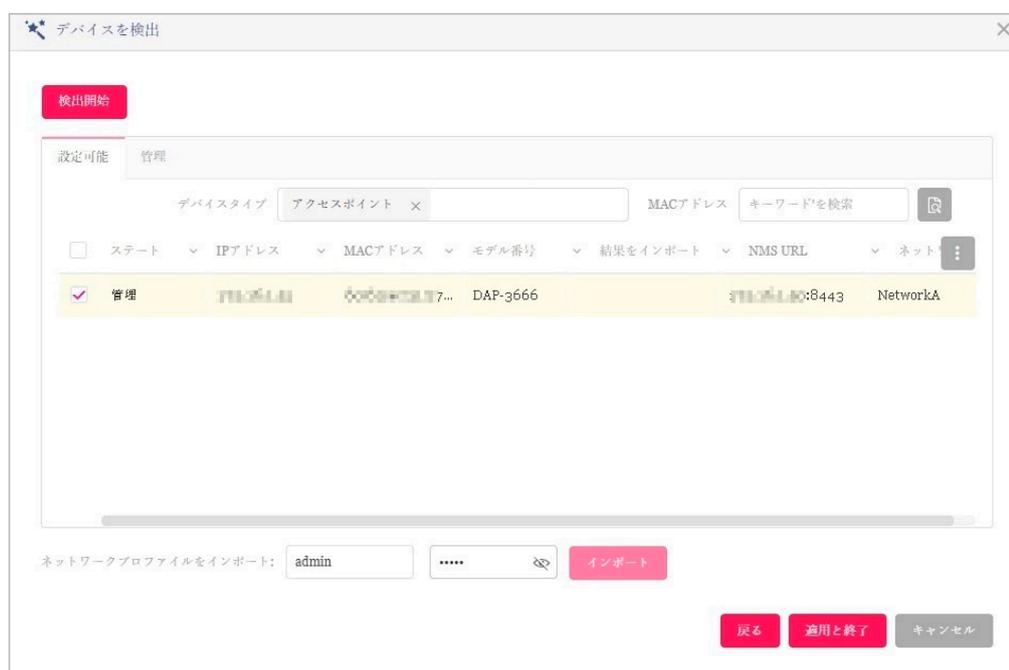


図 9-6 APを検出

参照 管理 / 非管理 AP のネットワークの移動や削除については、「[デバイス管理](#)」を参照してください。

7. 右上の「×」ボタンをクリックして画面を閉じます。

プロファイル設定

プロファイル設定機能では、既存のネットワークを管理することができます。

1. 設定 > プロファイル設定に移動して、既存のサイトを表示します。
2. サイトを選択し、次いで利用可能なネットワークを選択すると、編集可能なすべての設定が表示されます。

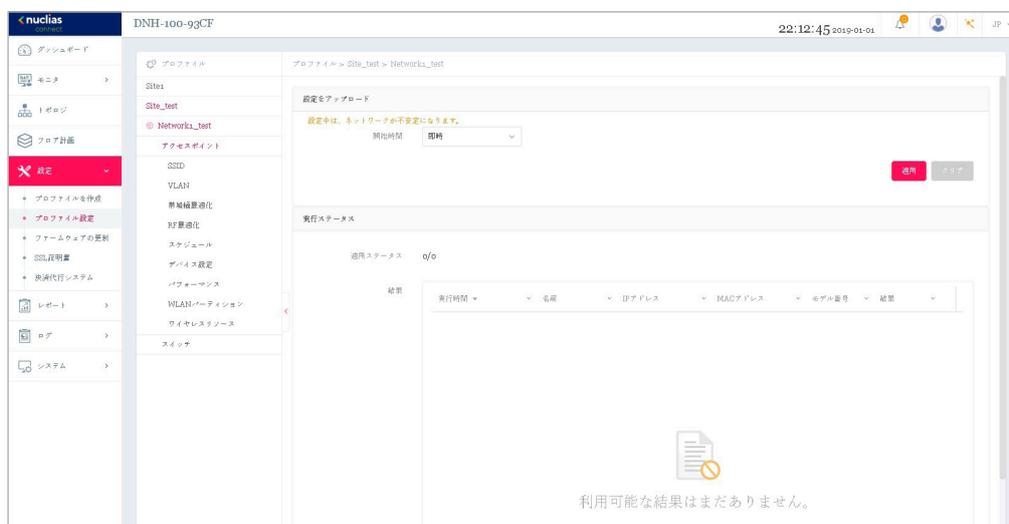


図 9-7 プロファイル設定

■ 設定のアップロード

ネットワークを選択した後、本画面から設定のアップロード機能を利用できます。

サイトまたはネットワーク設定の更新を有効にするには、設定をアクセスポイントにアップロードする必要があります。

1. 「設定をアップロード」セクションで、「開始時間」ドロップダウンメニューをクリックし、アクセスポイントに設定を更新する時間（「即時」または「時間を選択」）を選択します。
2. 「時間を選択」を選択した場合は、設定をアップロードする日時を設定します。「開始時間」を定義した後、「適用」をクリックしてアップロードを開始します。

「クリア」をクリックして、定義済みの設定を削除します。

「実行ステータス」のセクションで、アップロード設定機能のステータスが報告されます。更新完了後に結果が表示されます。

注意 SSIDに変更のあるプロファイルの適用は、全SSIDの停波を伴います。

■ ネットワークの各種設定

ネットワークを選択した後、表示されるメニューから各種デバイス設定を行うことができます。詳細は次ページ以降で説明します。

● アクセスポイント

- 「アクセスポイント - SSID」
- 「アクセスポイント - VLAN」
- 「アクセスポイント - 帯域幅の最適化」
- 「アクセスポイント - RF 最適化」
- 「アクセスポイント - スケジュール」
- 「アクセスポイント - デバイス設定」
- 「アクセスポイント - パフォーマンス設定」
- 「アクセスポイント - WLAN パーティション」
- 「アクセスポイント - ワイヤレスリソース」

● スイッチ ※スイッチ製品は未サポートです。

- 「スイッチ - 一般 - RADIUS サーバ」
- 「スイッチ - 一般 - 時間プロファイル」
- 「スイッチ - 基本」
- 「スイッチ - IPv4 ACL」
- 「スイッチ - アクセスポリシー」
- 「スイッチ - ポート設定」
- 「スイッチ - SNTP 設定」

アクセスポイント - SSID

「SSID」画面には、ネットワークのワイヤレス設定に関する構成可能なパラメータが表示されます。

注意 DNH-100 がサポートしている機能でも管理する AP 側でサポートされていない機能は使用できませんのでご注意ください。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > SSID の順に移動して、現在の設定を表示します。

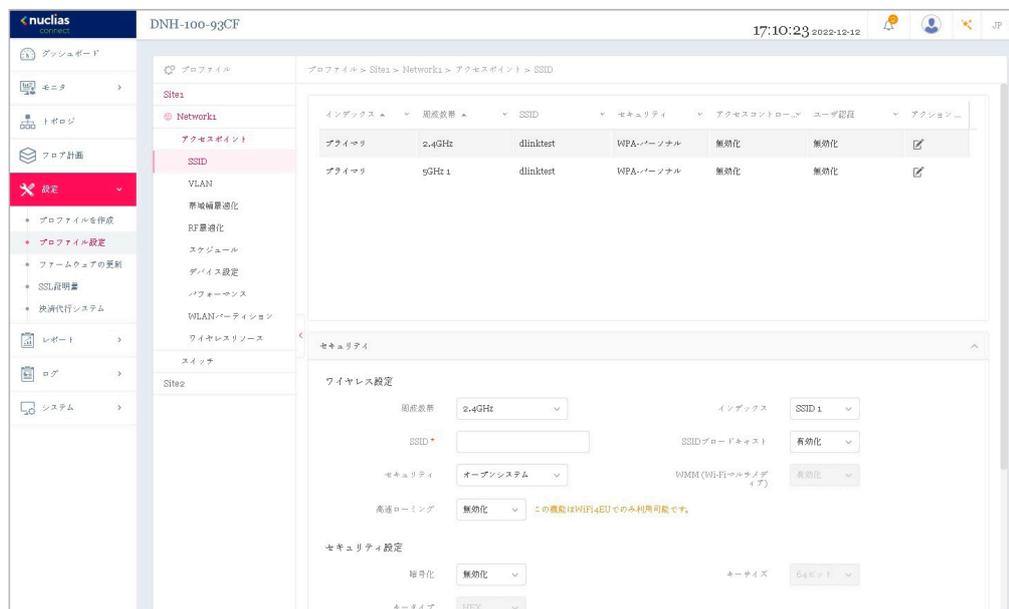


図 9-8 プロファイル設定 - アクセスポイント - SSID

セキュリティ



図 9-9 SSID - セキュリティ

「セキュリティ」セクションでは、以下の設定項目が表示されます。

項目	説明
周波数帯	ドロップダウンメニューをクリックして、無線周波数帯域を選択します。 ・ 選択肢：「2.4GHz」「5GHz 1」「5GHz 2（トライバンド）」
インデックス	ドロップダウンメニューをクリックして SSID インデックスを選択します。新しい SSID を作成するには、最初に本項目を選択します。 ・ 選択肢：プライマリ、SSID1-SSID7
SSID	ワイヤレスネットワーク名を入力します。SSID はすべての周波数で同じである必要があります。また、対象の接続先アクセスポイントのネットワーク名（SSID）が、Nuclias Connect で定義されているネットワーク名（SSID）と同じであることを確認してください。詳細については、アクセスポイント側のインタフェースで Basic Settings > Wireless Settings と Advanced Settings > DHCP Server > Dynamic Pool Settings を参照してください。「Domain Name」に Nuclias Connect で定義されたネットワーク名（SSID）が反映されるようになります。
SSID ブロードキャスト	ドロップダウンメニューをクリックして、ワイヤレス SSID の可視性を有効または無効にします。

第9章 設定

項目	説明
セキュリティ	ドロップダウンメニューをクリックして、ワイヤレスセキュリティプロトコルを選択します。 <ul style="list-style-type: none"> • 選択肢：「オープンシステム」（事前共有キー不要） 「Enhanced Open」 「Enhanced Open + Open」 「WPA- パーソナル」 「WPA- エンタープライズ」（RADIUS サーバが必要） 「802.1X」
WMM (Wi-Fi マルチメディア)	ドロップダウンメニューをクリックして、Wi-Fi マルチメディアを有効または無効にします。 「ワイヤレスモード」が「802.11g/b 混在」または「802.11aのみ」に設定されている場合に指定可能です。
高速ローミング	高速ローミング機能を有効または無効にします。 注意 802.11k/rのみサポートしています。802.11vはサポートしていません 注意 日本語のメッセージ（「この機能はWiFi4EUでのみ利用可能です。」）は誤りですので、無視してください。

「セキュリティ設定」のパラメータは、選択したセキュリティの種類によって変わります。以下のセクション以降の説明を参照してください。

■ 新規 SSID の追加

新しい SSID を追加する場合は、各セクションのパラメータを定義後に画面下部の「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の  をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

補足 「高速ローミング」、「Enhanced Open」機能は、製品によりサポート可否が異なります。詳細は「【付録 A】機能別サポート製品/バージョンについて (p.125)」をご確認ください。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

■ 「セキュリティ」項目を「オープンシステム」に設定した場合



セキュリティ設定

暗号化: 有効化 キーサイズ: 64ビット

キータイプ: HEX

キー値:

図 9-10 SSID - セキュリティ (オープンシステム)

項目	説明
セキュリティ設定	
暗号化	ドロップダウンメニューをクリックして、WEP オープンシステムの暗号化を有効または無効にします。
キーサイズ	ドロップダウンメニューをクリックして、WEP キーのサイズを選択します。 <ul style="list-style-type: none"> • 選択肢：「64 ビット」「128 ビット」
キータイプ	ドロップダウンメニューをクリックして、WEP キーのタイプを選択します。 <ul style="list-style-type: none"> • 選択肢：「ASCII」「HEX」
キー値	オープンシステムの WEP 暗号化キーを入力します。

■ 「セキュリティ」項目を「WPA- パーソナル」に設定した場合

図 9-11 SSID - セキュリティ (WPA- パーソナル)

項目	説明
セキュリティ設定	
WPA モード	ドロップダウンメニューをクリックして、WPA- モードを選択します。 ・ 選択肢：「自動 (WPA もしくは WPA2)」「WPA2 もしくは WPA3」「WPA2 のみ」「WPA3 のみ」
暗号化タイプ	ドロップダウンメニューをクリックして、暗号化タイプを選択します。 ・ 選択肢：「自動」(「自動 (WPA もしくは WPA2)」を指定した場合) ・ 選択肢：「AES」(「WPA2 もしくは WPA3」「WPA2 のみ」「WPA3 のみ」を指定した場合)
パスワード	使用するシークレットパスワードを入力します。
グループキー更新間隔	WPA グループキーの更新間隔の値を入力します。

補足 「WPA3」機能は、製品によりサポート可否が異なります。詳細は「【付録 A】機能別サポート製品/バージョンについて (p.125)」をご確認ください。

■ 「セキュリティ」項目を「WPA- エンタープライズ」に設定した場合

図 9-12 SSID - セキュリティ (WPA- エンタープライズ)

項目	説明
セキュリティ設定	
WPA モード	ドロップダウンメニューをクリックして、WPA モードを選択します。 ・ 選択肢：「自動 (WPA もしくは WPA2)」「WPA2 のみ」「WPA3 のみ」 注意 DAP-3666 は WPA3- エンタープライズは未サポートです。
暗号化タイプ	ドロップダウンメニューをクリックして、暗号化タイプを選択します。 ・ 選択肢：「自動」(「自動 (WPA もしくは WPA2)」を指定した場合) ・ 選択肢：「AES」(「WPA2 のみ」「WPA3 のみ」を指定した場合)
グループキー更新間隔	WPA グループキーの更新間隔の値を入力します。

第9章 設定

項目	説明
ネットワークアクセス保護	ネットワークアクセス保護機能を有効または無効にします。
プライマリ RADIUS サーバ設定 / バックアップ RADIUS サーバ設定 (オプション)	
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットを入力します。
プライマリアカウントサーバ設定 / バックアップアカウントサーバ設定 (オプション)	
アカウントモード	ドロップダウンメニューをクリックして、アカウントモードを有効または無効にします。
アカウントサーバ	アカウントサーバの IP アドレスを入力します。
アカウントポート	アカウントサーバのポート番号を入力します。
アカウントシークレット	アカウントサーバのシークレットを入力します。

補足

Radius Request は AP から送信されます。

補足

「ネットワークアクセス保護」、「WPA3」機能は、製品によりサポート可否が異なります。詳細は「【付録 A】機能別サポート製品 / バージョンについて (p.125)」をご確認ください。

■ 「セキュリティ」項目を「802.1X」に設定した場合

図 9-13 SSID - セキュリティ (802.1X)

項目	説明
セキュリティ設定	
キー更新間隔	キーの更新間隔の値を入力します。
プライマリ RADIUS サーバ設定 / バックアップ RADIUS サーバ設定 (オプション)	
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットパスフレーズを入力します。
プライマリアカウントサーバ設定 / バックアップアカウントサーバ設定 (オプション)	
アカウントモード	ドロップダウンメニューをクリックして、アカウントモードを有効または無効にします。
アカウントサーバ	アカウントサーバの IP アドレスを入力します。
アカウントポート	アカウントサーバのポート番号を入力します。
アカウントシークレット	アカウントサーバのシークレットパスフレーズを入力します。

アクセスコントロール

図 9-14 SSID - アクセスコントロール

「アクセスコントロール」セクションでは、以下の設定項目が表示されます。

項目	説明
ACL	
アクション	ドロップダウンメニューをクリックして、クライアントに適用するアクションを選択します。 ・ 選択肢: 「許可」「拒否」「無効化」
MAC アドレス	アクセスを許可または拒否するクライアントの MAC アドレスを入力します。 MAC アドレスと説明 (オプション) を入力した後、「追加」をクリックします。
説明	MAC アドレスの説明を入力します。
MAC アドレスリストをアップロード	「ブラウザ...」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードするには、「ダウンロード」をクリックします。
IP フィルタ設定	
アクション	ドロップダウンメニューをクリックして、IP フィルタ機能を有効または無効にします。
IP アドレス	IP アドレスを入力します。
サブネットマスク	サブネットマスクを入力します。 IP アドレスとサブネットマスクを入力した後、「追加」をクリックします。

■ 新規 SSID の追加

新しい SSID を追加する場合は、各セクションのパラメータを定義後に画面下部の「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の  をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

ユーザ認証



図 9-15 SSID - ユーザ認証

「ユーザ認証」セクションでは、以下の設定項目が表示されます。

項目	説明
認証タイプ	ドロップダウンメニューをクリックして、ワイヤレスクライアントに適用する認証タイプを選択します。 <ul style="list-style-type: none"> 選択肢: 「無効化」「Web リダイレクトのみ」「ユーザ名/パスワード」「リモート RADIUS」「LDAP」「POP3」「パスコード」「外部キャプティブポータル」「MAC アドレス」「クリックスルー」「ソーシャルログイン」
アイドルタイムアウト (2~1440)	クライアントがアクセスポイントから切断され、指定した時間が経過すると再認証が必要となります。本値は、経過後に STA を切断する時間ではなく、再接続に際して再認証が必要となる時間を設定します。 注意 Nuclias Connect の「アイドルタイムアウト」(本項目) が、DAP-2680/DAP-3666 の WebUI における「Session Timeout」に該当します。
同時ログインを有効化	同時ログインを有効または無効に設定します。 「ユーザ名/パスワード」「リモート RADIUS」「LDAP」「POP3」を選択した場合に設定します。
セッションタイムアウト (2~1440)	ログイン後、指定時間が経過すると再認証が必要になります。 「ユーザ名/パスワード」「リモート RADIUS」「LDAP」「POP3」「クリックスルー」を選択した場合に設定します。
許可 (1~720)	ワイヤレスクライアントが 1 日に再ログインできる回数を定義します。開始時刻は 0:00 です。 「セッションタイムアウト」を有効化した場合に設定します。
間隔 (0~720)	セッションタイムアウトの制限回数を超えた後、無線クライアントがログインできるようになるまでの期間を定義します。 「セッションタイムアウト」を有効化した場合に設定します。
ホワイトリストを有効化 (認証タイプが「Web リダイレクトのみ」以外の場合)	
ホワイトリストを有効化	チェックを入れると、ホワイトリスト機能が有効になります。
MAC アドレス	ホワイトリストに登録するネットワークデバイスの MAC アドレスを入力し、「追加」をクリックしてアドレスをホワイトリストテーブルに追加します。
ホワイトリストファイルをアップロード	「ブラウザ ...」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードするには、「ダウンロード」をクリックします。
IP インタフェース設定	
IRIF ステータス	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。
VLAN ID (VID)	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。
IP アドレスの取得	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。
IP アドレス	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。
サブネットマスク	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。
ゲートウェイ	IP インタフェース設定は、 設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト 内で設定される必要があります。

項目	説明
DNS	IP インタフェース設定は、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト内で設定される必要があります。
ユーザ名/パスワード (認証タイプが「ユーザ名/パスワード」の場合)	
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力します。 ユーザ名とパスワードを入力した後、「追加」をクリックします。入力値をリセットする場合は「Clear」をクリックします。
ユーザ名/パスワードファイルをアップロード	「ブラウザ...」をクリックして、ローカルコンピュータに保存されたユーザ名/パスワードリストのファイルを選択します。「アップロード」をクリックしてユーザリストを更新します。現在のユーザリストをダウンロードするには、「ダウンロード」をクリックします。
リモート RADIUS (認証タイプが「リモート RADIUS」「MAC アドレス」の場合)	
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットを入力します。
リモート RADIUS タイプ	RADIUS サーバのタイプを選択します。 ・ 選択肢: 「SPAP」「MS-CHAPv2」
NAS ID	NAS ID を有効または無効にします。有効にした場合、NAS ID を入力します。 NAS ID 設定は「リモート RADIUS」選択時のみ設定可能です。3 台の RADIUS サーバで共通の設定となります。
アカウントモード	アカウントモードを有効または無効にします。「リモート RADIUS」選択時のみ設定可能です。
アカウントサーバ	アカウントサーバの IP アドレスを入力します。「リモート RADIUS」選択時のみ設定可能です。
アカウントポート	アカウントサーバのポート番号を入力します。「リモート RADIUS」選択時のみ設定可能です。
アカウントシークレット	アカウントサーバのシークレットを入力します。「リモート RADIUS」選択時のみ設定可能です。
LDAP (「認証タイプが「LDAP」の場合)	
サーバ	LDAP サーバの IP アドレスを入力します。
ポート	LDAP サーバのポート番号を入力します。
認証モード	ドロップダウンメニューをクリックして、認証モードを選択します。 ・ 選択肢: 「シンプル」「TLS」
ユーザ名	LDAP データベースにアクセスして検索できる管理者のユーザ名を入力します。
パスワード	LDAP データベースにアクセスして検索できる管理者のパスワードを入力します。
ベース DN	LDAP データベースのベースドメイン名を入力します。
アカウント属性	アカウントの属性を入力します。
識別子	管理者の名前を入力します。「自動コピー」にチェックを入れると、入力済みの他のパラメータの値が反映されます。
POP3 (認証タイプが「POP3」の場合)	
サーバ	POP3 サーバの IP アドレスを入力します。
ポート	POP3 サーバのポート番号を入力します。
接続タイプ	ドロップダウンメニューをクリックして、接続タイプを選択します。 ・ 選択肢: 「なし」「SSL/TLS」
パスコードリスト (認証タイプが「パスコード」の場合)	
パスコードリスト	このネットワークに割り当てられたフロントデスクユーザによって生成されたパスコードを表示します。 外部キャプティブポータル (認証タイプが「外部キャプティブポータル」の場合)
サーバアドレス	ドロップダウンメニューから「http://」または「https://」を選択し、キャプティブポータルの URL を入力します。
Web リダイレクション (認証タイプが「MAC アドレス」以外の場合)	
Web リダイレクション	チェックを入れると、Web サイトのリダイレクト機能が有効になります。
Web サイト	ドロップダウンメニューから「http://」または「https://」を選択し、リダイレクト先 URL を入力します。
ウォールガーデンを有効化 (認証タイプが「Web リダイレクトのみ」以外の場合)	
ウォールガーデンを有効化	チェックを入れると、ウォールガーデン機能が有効になります。
ウォールガーデン範囲	ウォールガーデンの範囲を IP アドレス、IP アドレス/サブネットもしくはドメイン名を入力します。
ウォールガーデンファイルをアップロード	「ブラウザ...」をクリックして、ローカルコンピュータに保存されたウォールガーデン範囲リストのファイルを選択します。「アップロード」をクリックしてリストを更新します。現在のリストをダウンロードするには、「ダウンロード」をクリックします。
ソーシャルログイン (認証タイプが「ソーシャルログイン」の場合)	
Facebook	ソーシャルログインの資格情報として Facebook を使用します。
Google	ソーシャルログインの資格情報として Google を使用します。
スプラッシュページカスタマイズ (「認証タイプが「Web リダイレクトのみ」「外部キャプティブポータル」「MAC アドレス」以外の場合)	
認証タイプ	認証タイプを選択します。

第9章 設定

項目	説明
テンプレートを選択	ド롭ダウンメニューをクリックして、使用するログインスタイルを選択します。 <ul style="list-style-type: none">・「プレビュー」をクリックして、選択したスタイルをプレビューします。・「エディタ」をクリックして、スプラッシュページを編集します。・「ログインファイルをアップロード」をクリックして、新しいスタイルをアップロードします。・をクリックして、選択したスタイルを削除します。・をクリックして、スタイルテンプレートをダウンロードします。

■ 新規 SSID の追加

新しい SSID を追加する場合は、各セクションのパラメータを定義後に画面下部の「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の  をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 パスコード認証をご利用の場合、一部のブラウザでキャプティブポータル画面が表示されない、または HSTS エラーメッセージが表示されます。本問題を回避するには、DNH-100 に対し、有効な SSL 証明書を適用します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 認証設定の一部機能は、製品によりサポート可否が異なります。詳細は「[【付録 A】機能別サポート製品/バージョンについて \(p.125\)](#)」をご確認ください。

ホットスポット

図 9-16 SSID - ホットスポット 2.0

「ホットスポット 2.0」セクションでは、以下の設定項目が表示されます。

項目	説明
ホットスポット	
ホットスポット 2.0	ドロップダウンメニューをクリックして、ホットスポット 2.0 機能を有効または無効にします。
OSEN	ドロップダウンメニューをクリックして、OSEN (OSU Server-Only Authenticated L2 Encryption Network) のセキュリティ認証を有効または無効にします。
クロス接続を許可	ドロップダウンメニューをクリックして、クライアントのクロス接続を有効または無効にします。
P2P を管理	ドロップダウンメニューをクリックして、P2P 管理を有効または無効にします。
DGAF	ドロップダウンメニューをクリックして、DGAF (Downstream Group-Addressed Forwarding) を有効または無効にします。有効にすると、AP はダウンストリームのグループアドレスフレームを転送することができます。
プロキシ ARP	ドロップダウンメニューをクリックして、プロキシ ARP を有効または無効にします。
L2TIF	ドロップダウンメニューをクリックして、L2TIF (Layer 2 Traffic Inspection and Filtering) を有効または無効にします。
インターネットワーキング	
インターネットワーキング	ドロップダウンメニューをクリックして、インターネットワーキングを有効または無効にします。
アクセスネットワークタイプ	アクセスネットワークのタイプを選択します。 <ul style="list-style-type: none"> 選択肢:「プライベートネットワーク」「ゲストアクセス付きプライベートネットワーク」「有料公衆ネットワーク」「無料公衆ネットワーク」「パーソナルデバイスネットワーク」「緊急サービスのみのネットワーク」「テストもしくは実験」「ワイルドカード」
インターネット	この接続を介したインターネットの利用を有効または無効にします。
ASRA	ドロップダウンメニューをクリックして、ASRA (Additional Steps required for Access) を有効または無効にします。
ESR	ドロップダウンメニューをクリックして、ESR (Emergency services reachable) を有効または無効にします。
UESA	ドロップダウンメニューをクリックして、UESA (Unauthenticated Emergency Service Accessible) を有効または無効にします。
Venue グループ	Venue グループの値を入力します。 <ul style="list-style-type: none"> 設定可能範囲: 0-255
Venue タイプ	Venue タイプの値を入力します。 <ul style="list-style-type: none"> 設定可能範囲: 0-255
Venue 名	言語を選択し、Venue 名を入力します。
HESSID	Homogenous Extended Service Set (ESS) ID を入力します。サービスプロバイダネットワークを識別するために使用されます。
WAN メトリック	
WAN リンクステータス	アクセスポイントの WAN リンクステータスを選択します。 <ul style="list-style-type: none"> 選択肢:「リンクアップ」「リンクダウン」「テストステートでのリンク」

第9章 設定

項目	説明
WAN 対称リンク	WAN 対称リンクのステータスを「はい」「いいえ」から選択します。「はい」の場合、アップロード/ダウンロードは同じ速度になります。
WAN 帯域	WAN 帯域のステータスを「はい」「いいえ」から選択します。アクセスポイントやネットワークがキャパシティの上限に達している場合、「はい」を選択します。
WAN メトリックダウンロードスピード (kbps)	WAN 接続のダウンロードスピードを kbps 単位で入力します。ダウンロードスピードが不明な場合は 0 を指定します。
WAN メトリックアップリンクスピード (kbps)	WAN 接続のアップロードスピードを kbps 単位で入力します。アップロードスピードが不明な場合は 0 を指定します。
リスト	
ネットワーク認証タイプ	接続タイプを選択します。 <ul style="list-style-type: none"> 選択肢:「利用規約への同意」「オンライン登録をサポート」「http/https リダイレクション」「DNS リダイレクション」「http/https リダイレクション」「DNS リダイレクション」の場合は、URL を入力する必要があります。
利用可能な IP アドレスタイプ	利用可能な IP アドレスタイプを選択します。ネットワークへの認証後、ホットスポットのオペレータやモバイルデバイスによってこのアドレスタイプが使用されます。 <ul style="list-style-type: none"> 選択肢:「アドレスタイプは利用できません。」「利用可能なグローバル IP アドレス」「利用可能なポート制限された IPv4 アドレス」「利用可能なシングル NAT されたプライベート IPv4 アドレス」「利用可能なダブル NAT されたプライベート IPv4 アドレス」「利用可能なポート制限された IPv4 アドレスとシングル NAT された IPv4 アドレス」「利用可能なポート制限された IPv4 アドレスとダブル NAT された IPv4 アドレス」「アドレスタイプの IPv4 可用性は不明です。」「利用可能な IPv6 アドレスタイプ」「アドレスタイプの IPv6 可用性は不明です。」
ドメイン名リスト	
ドメイン名	アクセスポイントの実行エンティティのドメイン名を入力し、「追加」をクリックします。
ローミングコンソーシアム	
ローミングコンソーシアム	サービスプロバイダや、ローミングパートナーのグループを入力し、「追加」をクリックします。ネットワークに接続する際に、それらのセキュリティ認証が使用されます。 <ul style="list-style-type: none"> 入力可能な値: 6 桁または 10 桁の 16 進数
NAI レルムリスト	
NAI レルム	 をクリックして NAI レルムを入力します。BSS で利用可能な全ての NAI レルムを設定します。入力した NAI レルムを削除する場合は、  をクリックします。
EAP 方式	以下の手順で EAP 方式を設定します。 <ol style="list-style-type: none"> EAP 方式を選択します。  をクリックして、認証 ID とパラメータタイプを指定します。認証 ID/パラメータタイプを削除する場合は、 をクリックします。 「追加」をクリックして、EAP 方式のエントリを追加します。
RFC 4282	RFC 4282 への準拠を「はい」「いいえ」から選択します。「追加」をクリックして、上記 NAI レルムの入力情報とともにエントリとして追加します。
3GPP セルラーネットワーク	
MCC/MNC	アクセスポイントで利用可能な 3GPP セルラーネットワークを指定します。MCC と MNC の値を入力し、「追加」をクリックします。 <ul style="list-style-type: none"> 設定可能範囲: 000-999 (「MCC」)、00-999 (「MNC」)
接続機能	
IP プロトコル	IP プロトコルを選択します。 <ul style="list-style-type: none"> 選択肢:「ICMP」「TCP」「UDP」
ポート番号	ポート番号を入力します。
ステータス	IP プロトコルのステータスを選択します。 <ul style="list-style-type: none"> 選択肢:「閉じる」「オープン」「不明」
オペレータフレンドリー名	言語を選択し、オペレータフレンドリー名を入力します。Hotspot Venue オペレータの識別名です。
OSU (Online Sign-Up)	
OSU SSID	OSU SSID を入力します。本機能を使用すると、モバイルクライアントで利用可能なオンラインサービスを選択してオンラインサービスにサインインすることができます。
OSU サーバ URI	OSU サーバ URI を入力します。
OSU 方式リスト	
OSU 方式	言語を選択し、OSU 方式を入力します。「追加」をクリックして、OSU 方式を追加します。
OSU コンフィグ	OSU コンフィグを選択します。 <ul style="list-style-type: none"> 選択肢:「コンフィグ 1」「コンフィグ 2」
OSU 言語コード	OSU 言語コードを選択します。
OSU フレンドリー名	言語を選択し、OSU フレンドリー名を入力します。
OSU Nai	OSU NAI (Network Access Identifier) を入力します。

項目	説明
OSU サービス説明	OSU サービスの説明を入力します。
OSU アイコン言語コード	OSU アイコン言語コードを選択します。
OSU アイコンファイルパス	OSU アイコンのファイルパスを入力します。
OSU アイコンファイル名	OSU アイコンのファイル名を入力します。
OSU アイコン幅	OSU アイコンの幅の値を入力します。 ・ 指定可能範囲：0-256 (px)
OSU アイコン高さ	OSU アイコンの高さの値を入力します。 ・ 指定可能範囲：0-256 (px)
OSU アイコンタイプ	アイコンファイルの種類を選択します。 ・ 選択肢：「PNG」「JPEG」「GIF」「TIFF」「SVG」

■ 新規 SSID の追加

新しい SSID を追加する場合は、各セクションのパラメータを定義後に画面下部の「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の  をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「Hotspot2.0」機能は、製品によりサポート可否が異なります。詳細は「[【付録 A】機能別サポート製品 / バージョンについて \(p.125\)](#)」をご確認ください。

注意 Nuclias Connect 管理下において、プロファイルのホットスポット設定を行う場合、以下の既知の問題があります。

- ・ 「WAN リンクステータス」項目の「テストステートでのリンク」オプションの設定は AP に適切に適用されません。本項目では「リンクアップ」または「リンクダウン」を指定してください。
- ・ 「OSU サービス説明」項目の設定値は AP に適用されません。

アクセスポイント - VLAN

「VLAN」画面には、ネットワークの仮想 LAN サブネットワーク設定に関する構成可能なパラメータが表示されます。

プロフィール設定 > サイト > ネットワーク > アクセスポイント > VLAN の順に移動します。

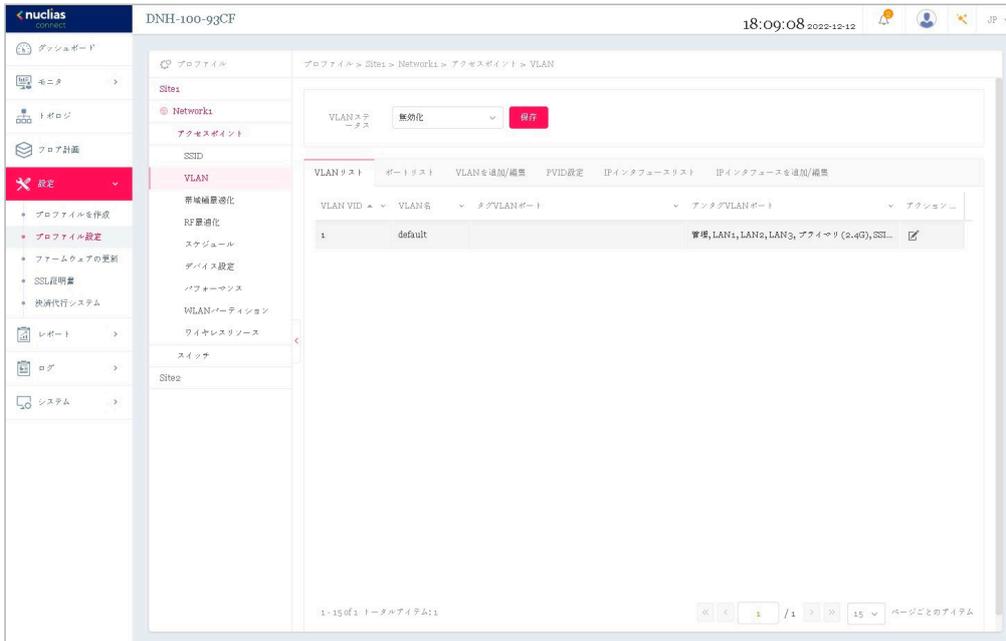


図 9-17 プロファイル設定 - アクセスポイント - VLAN

「VLAN」画面には、以下の項目が表示されます。

項目	説明
VLAN ステータス	ドロップダウンメニューをクリックして、VLAN を有効または無効にします。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

VLAN リスト

「VLAN リスト」タブには、定義済みの VLAN リストが表示されます。

をクリックして、既存の VLAN を変更します。

をクリックして、既存の VLAN を削除します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

ポートリスト

「ポートリスト」タブには、ポート割り当てのリストが表示されます。リストには、ネットワーク内のアクセスポイントで使用可能なタグ付きおよびタグなしポートが表示されます。

項目	説明
タグ VID	ポートが VLAN のタグ付メンバであることを示します。
アンタグ VID	ポートが VLAN のタグなしメンバであることを示します。
PVID (ポート VLAN ID)	接続された仮想 LAN セグメントが表示されます。

VLAN を追加 / 編集

「VLAN を追加 / 編集」タブでは、新しい VLAN を作成し、その VLAN にタグなしポートを割り当てることができます。「VLAN リスト」タブの「編集」アイコンをクリックすると、このタブに移動して既存の VLAN を変更することができます。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

PVID 設定

「PVID 設定」タブでは、このネットワーク内のアクセスポイントおよびワイヤレスクライアントのポート VLAN 識別子（PVID）設定を表示および設定することができます。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

IP インタフェースリスト

「IP インタフェースリスト」タブでは、IP インタフェース概要を表示できます。以下の情報が表示されます。

- ・「VLAN VID」「VLAN 名」「IP アドレスの取得」「IP アドレス」

設定を編集するには、アクション欄から  をクリックして「IP インタフェースを追加 / 編集」画面を表示します。

設定を削除するには  をクリックします。

IP インタフェースを追加 / 編集

「IP インタフェースを追加 / 編集」タブでは、IP インタフェースを追加または編集できます。以下の設定項目が表示されます。

- ・「VLAN VID」「IP アドレスの取得」「IP アドレス」「サブネットマスク」「ゲートウェイ」「DNS」

「保存」をクリックして、変更を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

アクセスポイント - 帯域幅の最適化

「帯域幅最適化」画面には、使用可能な帯域幅を最適化するための構成可能なパラメータが表示されます。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > 帯域幅最適化の順に移動して、現在の設定を表示します。

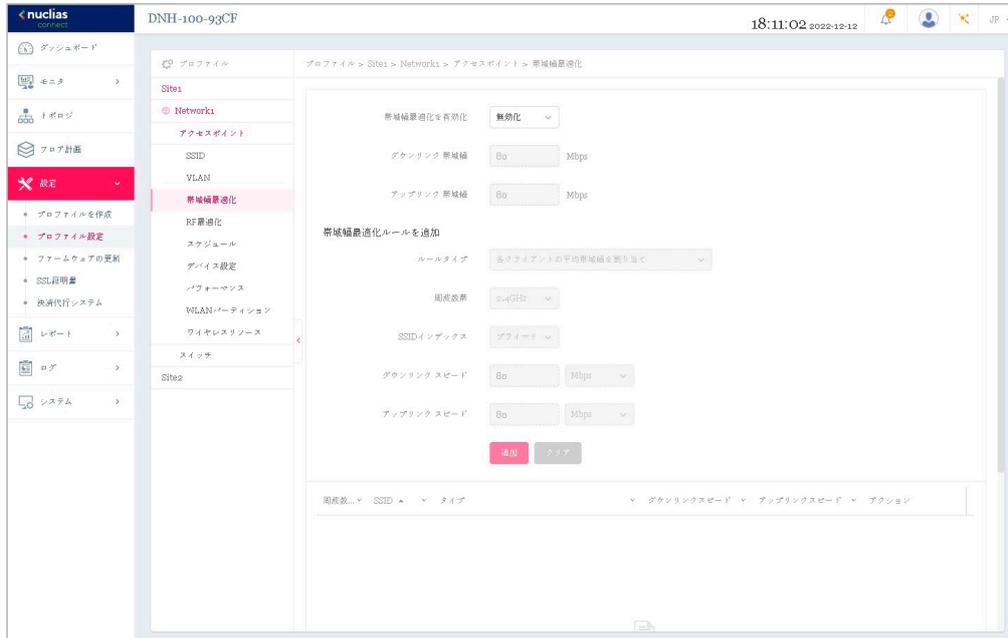


図 9-18 プロファイル設定 - アクセスポイント - 帯域幅設定

以下の設定項目が表示されます。

項目	説明
帯域幅最適化を有効化	ドロップダウンメニューをクリックして、帯域幅最適化機能を有効または無効にします。
ダウンリンク帯域幅	ネットワーク内のアクセスポイントのダウンリンク帯域幅の合計速度を入力します。
アップリンク帯域幅	ネットワーク内のアクセスポイントのアップリンク帯域幅の合計速度を入力します。
帯域幅最適化ルールを追加	
ルールタイプ	ドロップダウンメニューをクリックして、ルールタイプを選択します。 <ul style="list-style-type: none"> 「各クライアントの平均帯域幅を割り当て」：ダウンリンク/アップリンクスピードの設定値を、各クライアントで平等にシェアします。 「この SSID に特定の帯域幅を割り当て」：すべてのクライアントで割り当てられた帯域幅を共有します。 「各クライアントの最大帯域幅を割り当て」：ダウンリンク/アップリンクスピードの設定値が、各クライアントの最大値となります。 「11a/b/g/n クライアントに異なる帯域幅を割り当て」：a/b/g/n のクライアントに異なる帯域幅を割り当てます。 <ul style="list-style-type: none"> - 11b/g/n クライアント：10% / 20% / 70% - 11a/n クライアント：20% / 80%
周波数帯	ドロップダウンメニューをクリックして、ルールを適用する無線周波数帯域を選択します。 <ul style="list-style-type: none"> ・ 選択肢：「2.4GHz」「5GHz 1」「5GHz 2 (トライバンド)」
SSID インデックス	ドロップダウンメニューをクリックして、ルールを適用する SSID を選択します。
ダウンリンク スピード	各ステーションまたは指定された SSID に割り当てるダウンリンク スピードを入力します。
アップリンク スピード	各ステーションまたは指定された SSID に割り当てるアップリンク スピードを入力します。

■ 新規ルールの追加

新しくルールを追加する場合は、ルールの定義後に「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象ルールの をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

アクセスポイント - RF 最適化

「RF 最適化」画面には、ワイヤレスネットワークのアクセスポイントで使用される設定可能な無線周波数（RF）のパラメータが表示されます。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > RF 最適化に移動して、現在の設定を表示します。

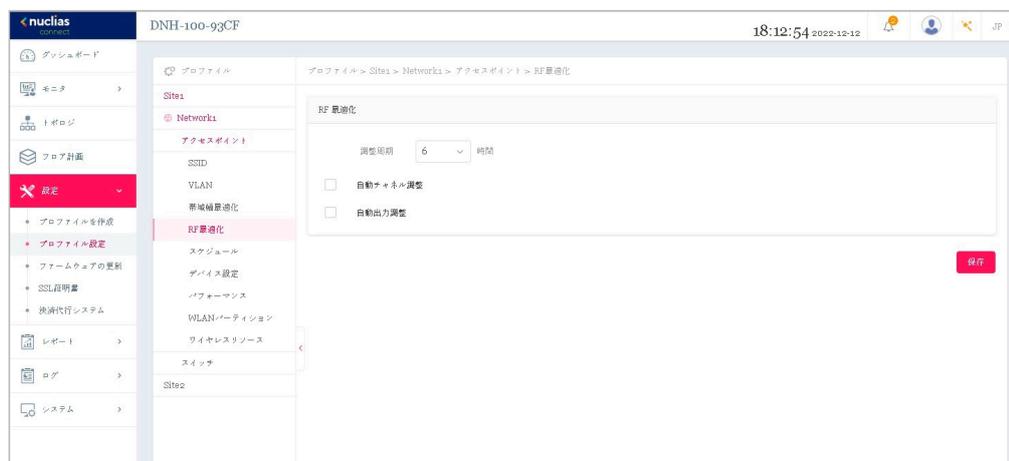


図 9-19 プロファイル設定 - アクセスポイント - RF 設定

以下の設定項目が表示されます。

項目	説明
調整周期	ドロップダウンメニューをクリックして、RF 周波数を調整する周期を 1 時間単位で設定します。
自動チャンネル調整	チェックボックスにチェックを入れて、RF 干渉を回避するためにクライアントのチャンネルを自動的に調整する機能を有効にします。
自動出力調整	「自動チャンネル調整」が有効な場合に使用できます。チェックボックスにチェックを入れて、干渉が存在する場合にカバーレージを最適化するために AP 無線電力を自動的に調整する機能を有効にします。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

アクセスポイント - スケジュール

「スケジュール」画面には、指定した曜日や時間帯に SSID をアクティブにするためのワイヤレススケジュール設定が表示されます。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > スケジュールに移動して、現在の設定を表示します。

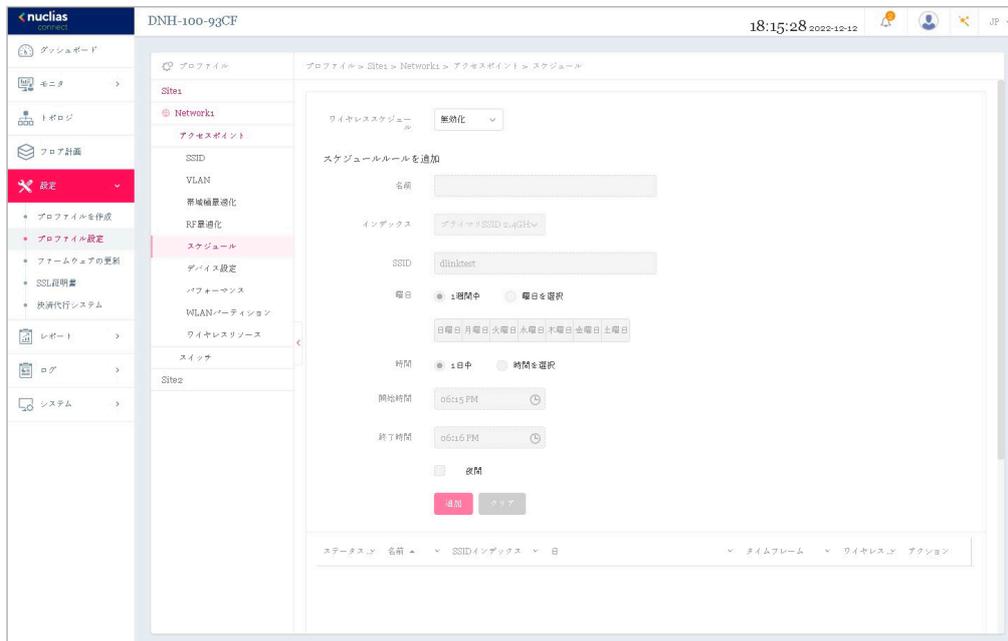


図 9-20 プロファイル設定 - アクセスポイント - スケジュール

以下の設定項目が表示されます。

項目	説明
ワイヤレススケジュール	ドロップダウンメニューをクリックして、ワイヤレススケジュール機能を有効または無効にします。
スケジュールルールを追加	
名前	スケジュールルールの名前を入力します。
インデックス	ドロップダウンメニューをクリックして、スケジュール設定が適用される SSID を選択します。
SSID	SSID 名が表示されます。
曜日	ラジオボタンをクリックして、スケジュールで無線をアクティブとする曜日を設定します。 <ul style="list-style-type: none"> 「1 週間中」：1 週間の全ての曜日でルールを有効にします。 「曜日を選択」：ルールを有効にする曜日を指定します。
時間	ラジオボタンをクリックして、スケジュールで無線をアクティブとする時間を選択します。 <ul style="list-style-type: none"> 「1 日中」：終日ルールを有効にします。 「時間を選択」：ルールの開始時刻と終了時刻を指定します。
開始時間	開始時間を設定します。この機能は、「時間」が「時間を選択」の場合にのみ使用できます。
終了時間	終了時間を設定します。この機能は、「時間」が「時間を選択」の場合にのみ使用できます。
夜間	チェックボックスをオンにすると、夜間のアクティビティが有効になります。「12:00 AM」をまったく場合は、本オプションにチェックを入れる必要があります。

■ 新規ルールの追加

新しくルールを追加する場合は、ルールの定義後に「追加」をクリックします。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

■ 既存ルールの変更

ルールを変更する場合は、対象ルールの  をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの  をクリックします。

定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

アクセスポイント - デバイス設定

「デバイス設定」画面では、このネットワーク内のアクセスポイントのログインおよびアクセシビリティ設定を表示および変更することができます。

注意 DNH-100 がサポートしている機能でも管理する AP 側でサポートされていない機能は使用できませんのでご注意ください。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > デバイス設定に移動して、現在の設定を表示します。

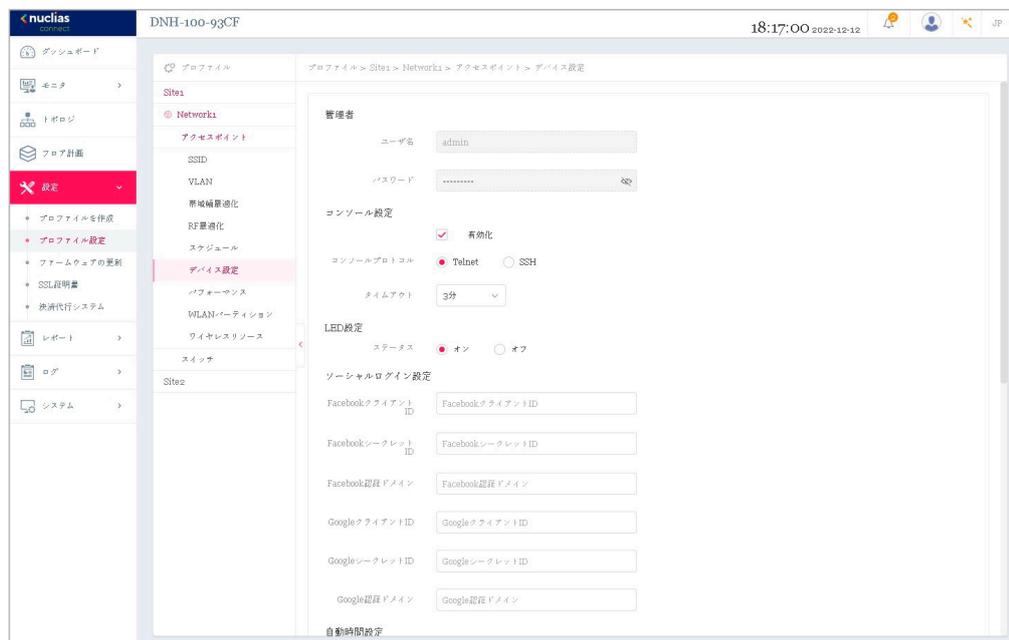


図 9-21 プロファイル設定 - アクセスポイント - デバイス設定

以下の設定項目が表示されます。

項目	説明
管理者	
ユーザ名	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理ユーザ名が表示されます。
パスワード	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理者パスワードが表示されます。
コンソール設定	
有効化	チェックを入れると、コンソール機能が有効になります。
コンソールプロトコル	ラジオボタンをクリックして、ネットワーク内のすべてのアクセスポイントに適用されるコンソールプロトコルを選択します。 • 選択肢：「Telnet」「SSH」
タイムアウト	ドロップダウンメニューをクリックして、アクティブなコンソールセッションのタイムアウト値を選択します。
LED 設定	
ステータス	デバイスの LED をオンまたはオフに設定します。
ソーシャルログイン設定	
Facebook クライアント ID	Facebook クライアント ID を入力します。
Facebook シークレット ID	Facebook シークレット ID を入力します。
Facebook 認証ドメイン	Facebook 認証ドメインを入力します。
Google クライアント ID	Google クライアント ID を入力します。
Google シークレット ID	Google シークレット ID を入力します。
Google 認証ドメイン	Google 認証ドメインを入力します。
自動時間設定	
NTP サーバを有効化	このチェックボックスをオンにすると、Network Time Protocol (NTP) サーバ機能が有効になります。
NTP サーバ	NTP サーバの IP アドレスまたはドメイン名を入力します。
国設定	
国を選択	ドロップダウンメニューをクリックして、ネットワーク内の AP の国を選択します。 「Japan」の設定から変更しないでください。
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
サマータイムを有効化	チェックボックスをオンにすると、サマータイム機能が有効になります。
DST 開始 (24 時間)	ドロップダウンメニューをクリックして、サマータイム (DST) の開始日時を指定します。
DST 終了 (24 時間)	ドロップダウンメニューをクリックして、サマータイム (DST) の終了日時を指定します。
DST オフセット (分)	ドロップダウンメニューをクリックして、DST オフセット (分) を選択します。

第9章 設定

項目	説明
外部シスログサーバ設定	
外部シスログサーバ (キャプティブポータルログ)	外部シスログサーバの IP アドレスまたはドメイン名を入力します。本機能は、キャプティブポータルログのみ対応しています。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

注意 管理デバイスを Nuclias Connect 管理モードからスタンドアロンモードに変更した場合、「外部シスログサーバ(キャプティブポータルログ)」設定は削除されます。

アクセスポイント - パフォーマンス設定

「パフォーマンス」画面では、ネットワーク上のアクセスポイントのワイヤレスパフォーマンスを設定できます。本画面では、2.4GHz と 5GHz の両方の周波数帯域について、詳細なワイヤレス設定を行うことができます。

注意 DNH-100 がサポートしている機能でも管理する AP 側でサポートされていない機能は使用できませんのでご注意ください。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > パフォーマンスに移動して、現在の設定を表示します。

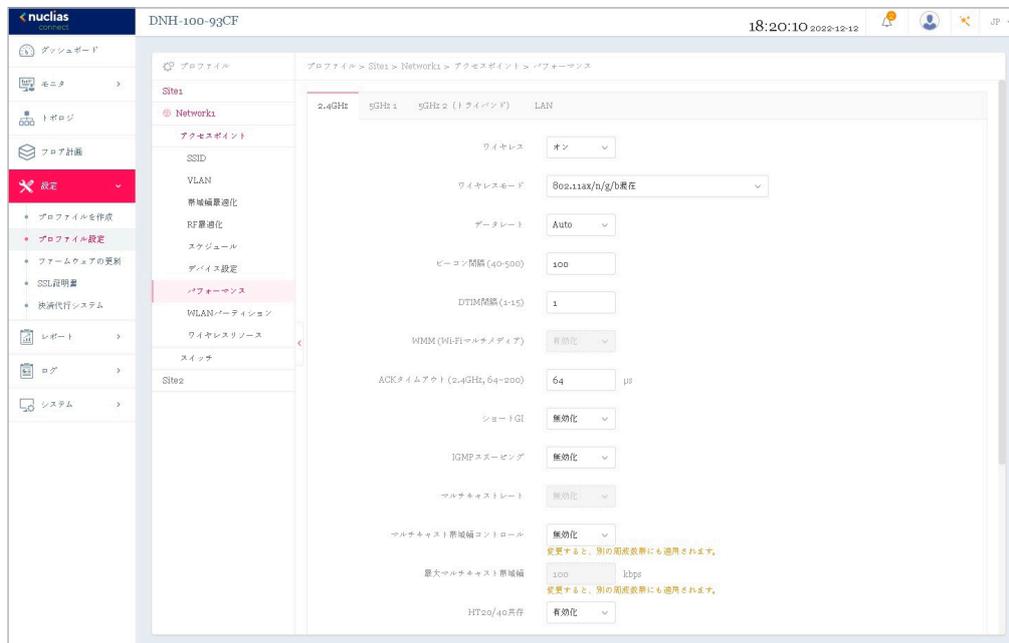


図 9-22 プロファイル設定 - アクセスポイント - パフォーマンス設定 (「2.4GHz」「5GHz 1」「5GHz 2 (トライバンド)」タブ)

2.4GHz/5GHz 1/5GHz 2 (トライバンド)

「2.4GHz」「5GHz 1」「5GHz 2 (トライバンド)」タブを選択した場合、以下の設定項目が表示されます。

項目	説明
ワイヤレス	ドロップダウンメニューをクリックして、ネットワークの無線帯域をオンまたはオフにします。
ワイヤレスモード	ドロップダウンメニューをクリックして、ネットワークで使用されるワイヤレスモードを選択します。 <ul style="list-style-type: none"> 選択肢：(2.4GHz の場合) 「802.11ax/n/g/b 混在」「802.11g/b 混在」「802.11n のみ」 (5GHz 1/5GHz 2 の場合) 「Mixed 802.11n/a」「802.11a のみ」「802.11n のみ」「Mixed 802.11ax/ac/n/a」
データレート	ドロップダウンメニューをクリックして、無線のデータレートを選択します。 ワイヤレスモードが「802.11g/b 混在」(2.4GHz) または「802.11a のみ」(5GHz 1/5GHz 2) の場合にのみ設定できます。
ビーコン間隔	ビーコン間隔の値を入力します。 <ul style="list-style-type: none"> 初期値：100
DTIM 間隔	DTIM 間隔の値を入力します。 <ul style="list-style-type: none"> 初期値：1
WMM (Wi-Fi マルチメディア)	ドロップダウンメニューをクリックして、Wi-Fi マルチメディア (WMM) 機能を有効または無効にします。 ワイヤレスモードが「802.11g/b 混在」(2.4GHz) または「802.11a のみ」(5GHz 1/5GHz 2) の場合にのみ設定できます。
ACK タイムアウト	ACK タイムアウト値を入力します。 <ul style="list-style-type: none"> 初期値：64
ショート GI	ドロップダウンメニューをクリックして、ショート GI 機能を有効または無効にします。

項目	説明
IGMP スヌーピング	ドロップダウンメニューをクリックして、IGMP スヌーピング機能を有効または無効にします。
マルチキャストレート	ドロップダウンメニューをクリックして、マルチキャストレート値を選択します。 ワイヤレスモードが「802.11g/b 混在」(2.4GHz) または「Mixed 802.11n/a」「802.11a のみ」(5GHz 1/5GHz 2) の場合にのみ設定できます。
マルチキャスト帯域幅コントロール	ドロップダウンメニューをクリックして、マルチキャスト帯域コントロール機能を有効または無効にします。
最大マルチキャスト帯域幅	マルチキャスト帯域幅の最大値を入力します。「マルチキャスト帯域幅コントロール」が有効の場合に設定します。 ・初期値：100
HT20/40 共存	ドロップダウンメニューをクリックして、HT20/40 共存機能を有効または無効にします。 2.4GHz 帯の「チャンネル幅」で「自動 20/40MHz」を選択した場合に指定可能です。
DHCPOFFER をマルチキャストからユニキャストに変更	ドロップダウンメニューをクリックして、ユニキャストへの DHCP オファー転送を許可または拒否します。
RTS 長	RTS の長さの値を入力します。 ・初期値：2346
フラグメント長	フラグメント長の値を入力します。 ・初期値：2346
チャンネル幅	ドロップダウンメニューをクリックして、ネットワークで使用されるチャンネル幅を選択します。 ・選択肢：(「802.11g/b 混在」「802.11a のみ」の場合)「20MHz」 (「802.11ax/n/g/b 混在」「802.11n のみ」「Mixed 802.11n/a」の場合)「20MHz」「自動 20/40MHz」 (「Mixed 802.11ax/ac/n/a」の場合)「20MHz」「自動 20/40MHz」「自動 20/40/80/160MHz」

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「ワイヤレスモード」で設定可能なモードは DAP 製品により異なります。

補足 「チャンネル幅」で設定可能なチャンネル範囲は DAP 製品により異なります。

LAN



図 9-23 パフォーマンス設定（「LAN」タブ）

「LAN」タブをクリックした場合、以下の設定項目が表示されます。

項目	説明
STP (スパニングツリー)	ドロップダウンメニューをクリックして、スパニングツリー機能を有効または無効にします。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「STP (スパニングツリー)」の設定は、製品によりサポート可否が異なります。詳細は「[【付録 A】機能別サポート製品/バージョンについて \(p.125\)](#)」をご確認ください。

アクセスポイント - WLAN パーティション

WLAN パーティション」画面には、ワイヤレスパーティション設定が表示されます。これにより、関連付けられたワイヤレスクライアント間の通信を有効/無効にできます。

注意 DNH-100 がサポートしている機能でも管理する AP 側でサポートされていない機能は使用できませんのでご注意ください。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > WLAN パーティションに移動し、「2.4GHz」または「5GHz 1」、「5GHz 2（トライバンド）」タブをクリックして、現在の設定を表示します。

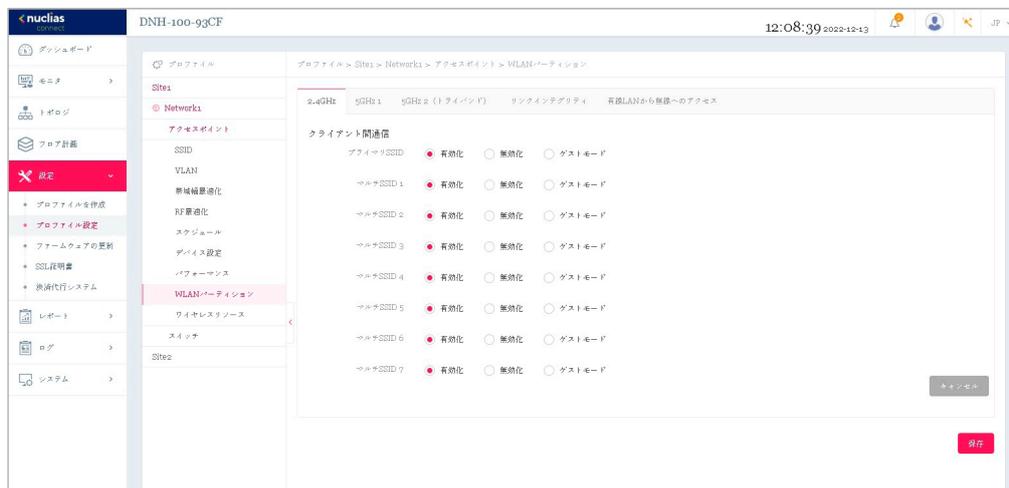


図 9-24 プロファイル設定 - アクセスポイント - WLAN パーティション（「2.4GHz」「5GHz 1」「5GHz 2（トライバンド）」タブ）

以下の設定項目が表示されます。

項目	説明
	クライアント間通信
プライマリ SSID/ マルチ SSID 1-7	ラジオボタンをクリックして、WLAN パーティションへの SSID のメンバーシップを有効または無効にします。この SSID がゲストとしてこの WLAN パーティションにアクセスできるようにするには、「ゲストモード」を選択します。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

リンクインテグリティ

リンクインテグリティ機能は、LAN と AP が切断された際に無線セグメントの AP との関連付けを解除します。



図 9-25 WLAN パーティション（「リンクインテグリティ」タブ）

「リンクインテグリティ」タブをクリックした場合、以下の設定項目が表示されます。

項目	説明
リンクインテグリティ	ドロップダウンメニューをクリックして、無線のリンクインテグリティ機能を有効または無効にします。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「リンクインテグリティ」機能は、製品によりサポート可否が異なります。詳細は「[【付録 A】機能別サポート製品 / バージョンについて \(p.125\)](#)」をご確認ください。

有線 LAN から無線へのアクセス

「有線 LAN から無線へのアクセス」機能を使用すると、イーサネットは関連する無線デバイスからデータを送受信できます。



図 9-26 WLAN パーティション（「有線 LAN から無線へのアクセス」タブ）

「有線 LAN から無線へのアクセス」タブをクリックした場合、以下の設定項目が表示されます。

項目	説明
有線 LAN から無線へのアクセス	ドロップダウンメニューをクリックして、有線 LAN から無線 LAN へのアクセス機能を有効または無効にします。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

アクセスポイント - ワイヤレスリソース

「ワイヤレスリソース」画面には、ワイヤレスネットワークのリアルタイム RF 管理に役立つ設定が表示されます。

注意 DNH-100 がサポートしている機能でも管理する AP 側でサポートされていない機能は使用できませんのでご注意ください。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソースに移動し、「2.4GHz」または「5GHz 1」、「5GHz 2（トライバンド）」タブをクリックして、現在の設定を表示します。

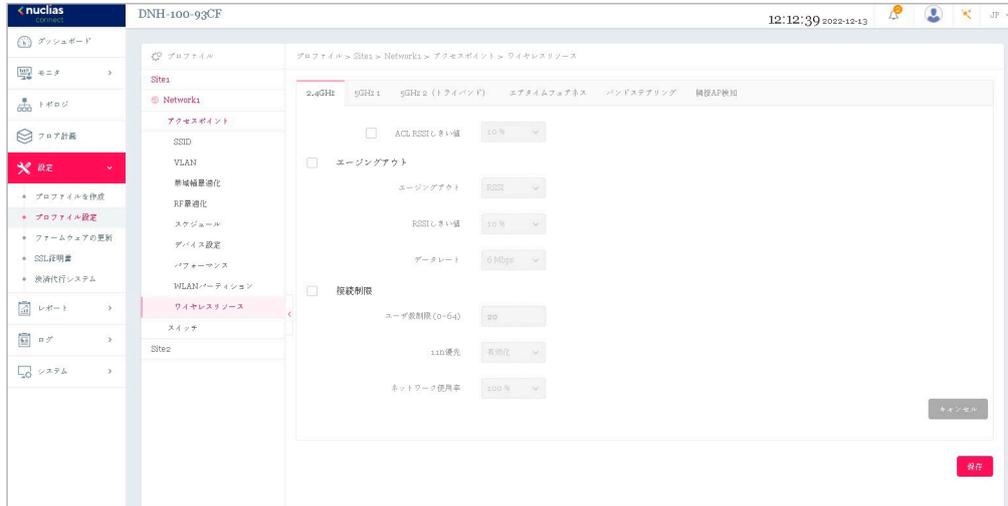


図 9-27 プロファイル設定 - アクセスポイント - ワイヤレスリソース（「2.4GHz」「5GHz 1」「5GHz 2（トライバンド）」タブ）

「2.4GHz」または「5GHz 1」、「5GHz 2（トライバンド）」タブを選択した場合、以下の設定項目が表示されます。

項目	説明
ACL RSSI しきい値	ACL RSSI しきい値機能を有効にするチェックボックスをオンにし、ドロップダウンメニューをクリックして、ACL RSSI しきい値のパーセントを選択します。
エージングアウト	
エージングアウト	チェックボックスをクリックしてエージングアウトを有効/無効にします。
エージングアウト	ドロップダウンメニューをクリックして、エージングアウトモードを選択します。 ・ 選択肢：「RSSI」「データレート」
RSSI しきい値	エージングアウトモードで「RSSI」を選択した場合に設定可能です。 10%~100%の値を選択します。このパラメータは、無線クライアントがプローブに応答するための最小 RSSI を設定します。クライアントの RSSI 値が指定のパーセンテージより小さい場合、ワイヤレスクライアントは切断されます。
データレート	エージングアウトモードで「データレート」を選択した場合に設定可能です。 ドロップダウンメニューをクリックして、データレート接続制限を選択します。
接続制限	
接続制限	チェックボックスをクリックして接続制限を有効/無効にします。 接続制限は、負荷分散を提供するように設計されています。このポリシーにより、ワイヤレスネットワークでのユーザアクセス管理が可能になります。本機能が有効になっていて、ユーザ数またはネットワーク使用率が指定された値を超えた場合、それ以上のクライアントアソシエーションは許可されません。
ユーザ数制限	ユーザ接続数の上限を入力します。 ・ 初期値：20 ・ 設定可能範囲：0-64
11n 優先	ドロップダウンメニューをクリックして、802.11n の優先使用を有効または無効にします。
ネットワーク使用率	ドロップダウンメニューをクリックして、ネットワーク使用率を選択します。

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「11n 優先」機能は、製品 / バージョンにより以下の機能が適用されます。

- ・ DAP-X2850/DAP-X2810：「11n/ac/ax Preferred」（2.4GHz）、「11n/ax Preferred」（5GHz）
- ・ DAP-3666/DAP-2680/DAP-2610：「11n Preferred」（2.4GHz）、「11n/ac Preferred」（5GHz）

エアタイムフェアネス

エアタイムフェアネス機能を使用すると、ネットワーク全体のパフォーマンスを向上させることができます。この機能では、接続デバイスの通信速度によらず、全てのクライアントに対して通信時間を均等に分配します。これにより、低速なデバイスが存在する場合でも他のデバイスの通信を妨げず、ネットワーク全体で快適な通信環境を実現することができます。

注意 無線デバイスのWiFi通信速度が遅い原因として、接続距離が長い/信号強度が弱い/古いレガシーハードウェアを利用しているなどの理由が考えられます。このような場合、エアタイムフェアネス機能を使用することでネットワーク全体のパフォーマンスを向上させることが可能です。設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソースに移動します。「エアタイムフェアネス」タブをクリックして、現在の設定を表示します。

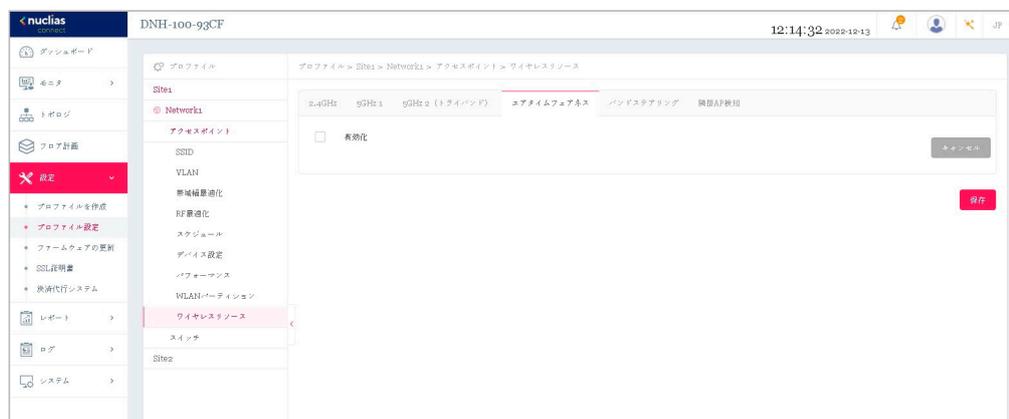


図 9-28 ワイヤレスリソース（「エアタイムフェアネス」タブ）

チェックボックスをオンにすると、エアタイムフェアネス機能が有効になります。「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

補足 「エアタイムフェアネス」機能は、製品によりサポート可否が異なります。詳細は「【付録 A】機能別サポート製品 / バージョンについて (p.125)」をご確認ください。

バンドステアリング (5GHz 優先)

バンドステアリング機能を使用すると、デュアルバンド対応クライアントが混雑の少ない5GHzネットワークに接続し、2.4GHzのみをサポートするクライアントについては2.4GHzネットワークを使用するように設定することができます。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソースに移動します。「バンドステアリング」タブをクリックすると、既存の設定が表示されます。

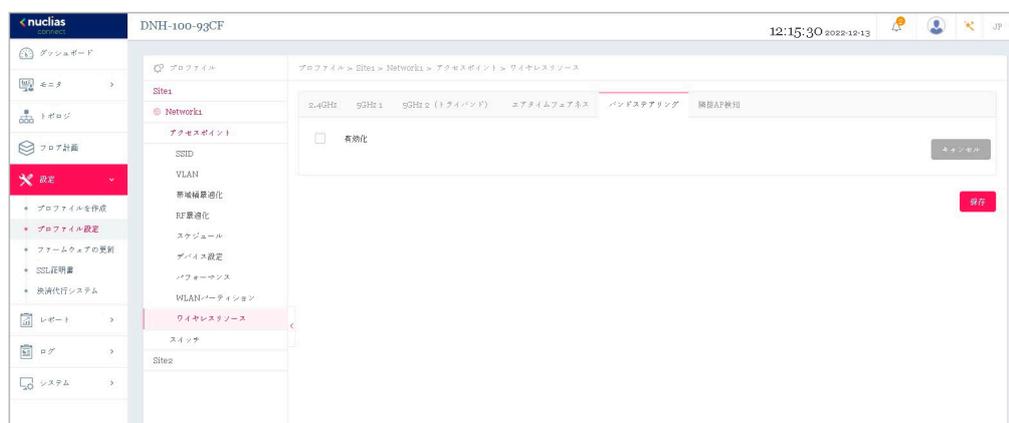


図 9-29 ワイヤレスリソース（「バンドステアリング」タブ）

チェックボックスをオンにすると、ワイヤレスバンドステアリング機能が有効になります。「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

隣接 AP 検知

本機能では、隣接 AP 検知を設定します。隣接 AP 検知では、AP の場所と隣接関係を判断し、不正 AP の特定と WLAN の計画に役立てることができます。

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソースに移動します。「隣接 AP 検知」タブをクリックすると、以下の画面が表示されます。

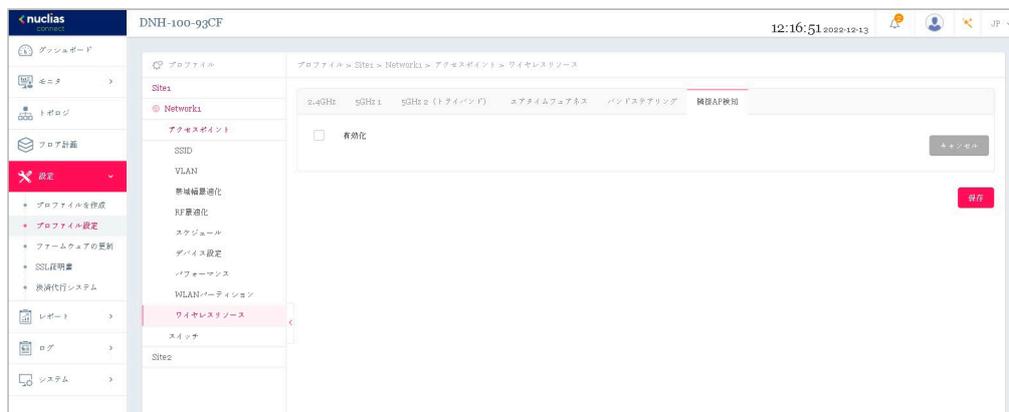


図 9-30 ワイヤレスリソース（「隣接 AP 検知」タブ）

「有効」をオンにして検出を有効にし、「保存」をクリックして設定を保存します。

■ 隣接 AP の確認

検出された AP リストを確認するには、**モニタ > アクセスポイント > 隣接 AP** に移動します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

補足 「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「[【付録 A】機能別サポート製品 / バージョンについて \(p.125\)](#)」をご確認ください。

スイッチ - 一般 - RADIUS サーバ

補足 スイッチ製品は未サポートです。

ネットワーク内のすべてのスイッチに対して適用される、共通のリモート RADIUS サーバを設定します。本機能では、スイッチからのアクセス要求を 1 つ以上の指定されたリモート RADIUS サーバに転送します。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > 一般 > RADIUS サーバの順に移動します。

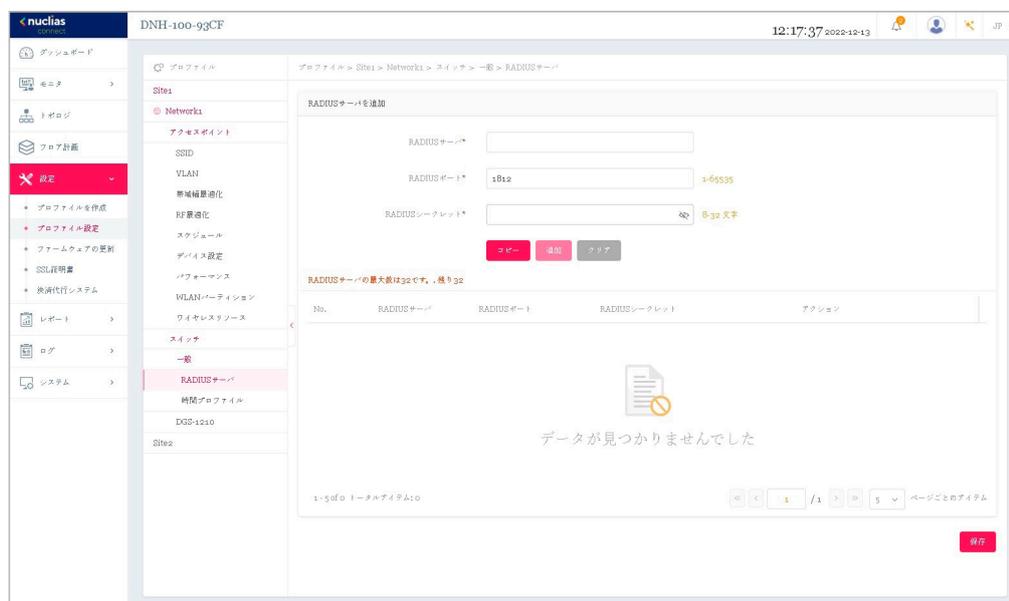


図 9-31 プロファイル設定 - スイッチ - RADIUS サーバ

■ 新規エントリの追加

- 新しく RADIUS サーバを追加する場合は、以下の項目を設定します。
 - 「RADIUS サーバ」：RADIUS 認証サーバの IP アドレスを入力します。
 - 「RADIUS ポート」：RADIUS サーバの UDP ポートを入力します。
 - 「RADIUS シークレット」：サーバとの通信に使用するシークレットを入力します。

「コピー」をクリックして他のネットワークから RADIUS サーバをコピーすることもできます。「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

- 「追加」をクリックします。

■ 既存エントリの変更

既存エントリの設定を変更する場合は、対象サーバの  をクリックします。設定完了後、「保存」をクリックしてサーバ設定を保存します。

エントリを削除する場合は、対象エントリの  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

■ RADIUS サーバテーブルの表示・検索

RADIUS サーバテーブルには、定義した RADIUS サーバの情報（IP アドレス、ポート、シークレット）が表示されます。

No.	RADIUSサーバ	RADIUSポート	RADIUSシークレット	アクション
1	10.90.90.100	1812	  

図 9-32 RADIUS サーバテーブル

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

スイッチ - 一般 - 時間プロフィール

補足 スイッチ製品は未サポートです。

ネットワーク内のすべてのスイッチに対して適用される、共通の時間プロフィールを設定します。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > 一般 > 時間プロフィールの順に移動します。

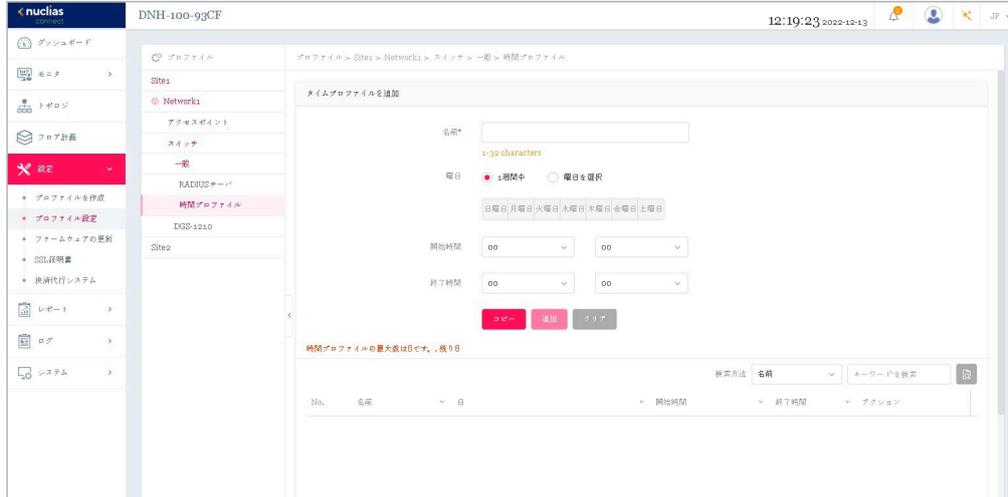


図 9-33 プロファイル設定 - スイッチ - 時間プロフィール

■ 新規エントリの追加

- 新しくタイムプロフィールを追加する場合は、以下の項目を設定します。
 - 「名前」：プロフィールの名前を入力します。
 - 「曜日」：スイッチの稼働日を指定します。
 - 「開始時間 / 終了時間」：開始時刻と終了時刻を指定します。

「コピー」をクリックして他のネットワークからタイムプロフィールをコピーすることもできます。
「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

- 「追加」をクリックします。

■ 既存エントリの変更

既存エントリを設定を変更する場合は、対象プロフィールの  をクリックします。設定完了後、「保存」をクリックして設定を保存します。
エントリを削除する場合は、対象エントリの  をクリックします。
設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロフィール設定を保存します。

■ 時間プロフィールテーブルの表示・検索

時間プロフィールテーブルには、定義した時間プロフィールの情報（時間プロフィールの名前、稼働日、開始 / 終了時刻）が表示されます。

- ドロップダウンメニューを使用して、「名前」「日」のいずれかを指定します。
- 関連するキーワードを入力し、 をクリックして検索を開始します。



図 9-34 時間プロフィールテーブル

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

スイッチ - 基本

補足 スイッチ製品は未サポートです。

「基本」画面では、VLAN、IGMP スヌーピング、QoS などのスイッチ全体の設定を行うことができます。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > 基本の順に移動します。

以下では、各機能について説明します。

VLAN 設定

このセクションでは、VLAN を追加、編集、または削除できます。

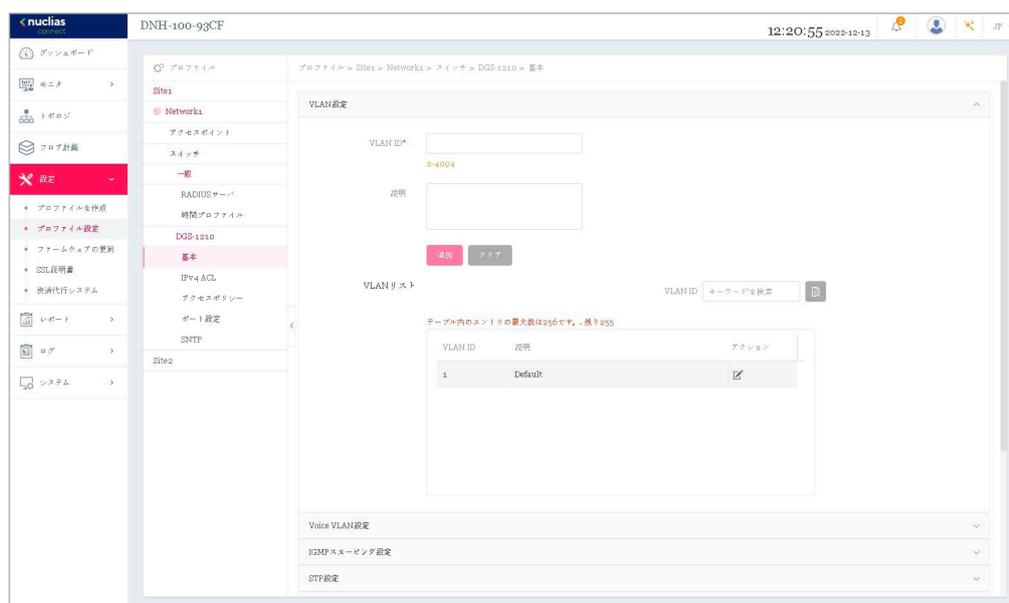


図 9-35 プロファイル設定 - スイッチ - 基本 (VLAN)

■ VLAN の追加

1. 「VLAN ID」フィールドに、2~4094 の範囲で VLAN ID を入力します。
2. VLAN の説明を入力します。
3. 「追加」を選択して VLAN を追加します。
設定値をリセットするには、「クリア」をクリックします。

■ VLAN リストの表示・検索

VLAN リストには、VLAN の概要が表示されます。

1. 「VLAN ID」検索フィールドにキーワードを入力し、 をクリックして検索を開始します。

■ VLAN の編集・削除

「アクション」フィールドで、 をクリックして VLAN を編集します。設定完了後、「保存」をクリックして設定を保存します。

VLAN を削除する場合は、対象 VLAN の  をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

Voice VLAN 設定

このセクションでは、グローバルな音声 VLAN 設定と音声 VLAN OUI（Organizationally Unique Identifier）を表示および設定できます。

図 9-36 基本 (Voice VLAN 設定)

■ 音声 VLAN の設定 / 音声 VLAN OUI の追加

1. 「Voice VLAN」フィールドで、音声 VLAN を有効または無効に設定します。
2. 音声 VLAN を有効化した場合、以下の設定を行います。
 - 「Voice VLAN ID」
 - 「Voice VLAN COS」

「Voice VLAN ID」フィールドの右側で、音声 VLAN に属するメンバーポートの数を確認できます。番号をクリックすると、「ポート設定」画面に移動します。

3. 音声 VLAN のユーザ定義 OUI を追加する場合、「Voice VLAN OUI」セクションで OUI アドレスとその説明を入力します。
4. 「追加」をクリックして、音声 VLAN OUI を追加します。ユーザ定義 OUI は最大 10 件まで作成できます。入力した値をリセットするには「クリア」をクリックします。

■ 音声 VLAN OUI リストの表示・検索

音声 VLAN OUI リストがテーブルに一覧表示されます。デフォルトの定義済みエントリは編集したり削除したりすることはできません。

テーブル内のユーザ定義エントリの最大数は10です。残り10

OUIアドレス ▲	マスク ▲	説明 ▲	アクション
00:01:e3:00:00:00	ff:ff:ff:00:00:00	Siemens	
00:03:6b:00:00:00	ff:ff:ff:00:00:00	Cisco	
00:09:6e:00:00:00	ff:ff:ff:00:00:00	Avaya	
00:0f:e2:00:00:00	ff:ff:ff:00:00:00	Huawei & 3COM	
00:60:b9:00:00:00	ff:ff:ff:00:00:00	NEC & Philips	

図 9-37 基本 (Voice VLAN 設定 - Voice VLAN OUI)

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

IGMP スヌーピング設定

IGMP スヌーピングを使用すると、スイッチはマルチキャストグループを認識し、それに応じてネットワークトラフィックを転送できます。

図 9-38 基本 (IGMP スヌーピング設定)

1. IGMP スヌーピング機能を有効または無効に設定します。
2. 有効化する場合、VLAN の VLAN ID を入力します。VLAN の最大数は 256 です。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

STP 設定

RSTP (Rapid Spanning Tree Protocol) は、ループフリートポロジと高速コンバージェンス時間を保証できます。

図 9-39 基本 (STP 設定)

1. ネットワーク内のすべてのスイッチで RSTP を有効または無効に設定します。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

DHCP サーバスクリーン設定

DHCP (Dynamic Host Configuration Protocol) サーバスクリーニングは、不正な DHCP サーバパケットをフィルタリングすることによって、より高いセキュリティを提供します。

図 9-40 喜保院 (DHCP サーバスクリーン設定)

1. DHCP サーバスクリーニング機能を有効または無効にします。
2. 有効化する場合、「許可された DHCP サーバ IP」に許可する DHCP サーバの IP アドレスを入力します。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

第9章 設定

ジャンボフレームの設定

ジャンボフレームは、大きなペイロードを持つイーサネットフレームです。フレームの過負荷を軽減し、システムスループットを向上させ、CPU使用率を削減するために使用されます。



図 9-41 基本 (ジャンボフレーム設定)

1. ジャンボフレームを有効または無効に設定します。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

QoS

QoS 機能は、DiffServ を使用して特定のタイプのデータに優先順位を付けることができます。トラフィック分類として、Differentiated Services Code Point (DSCP) を使用して、各パケットで優先順位がマークされます。

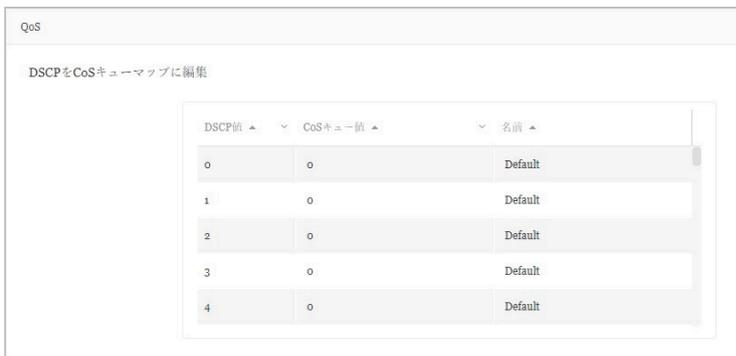


図 9-42 基本 (QoS 設定)

1. DSCP と CoS (Class of Service) キューのマッピングを設定するには、各 DSCP 値に対し、CoS キュー値とその名前を設定します。値のフィールドをクリックして設定できます。各 DSCP 値に対し、1 つの CoS キュー値のみマッピングできます。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

LBD 設定

ループバック検出 (LBD) 機能は、1 つまたは複数のポートで発生するループを検出できます。



図 9-43 LBD 設定

1. LBD 機能を有効または無効に設定します。デフォルトでは無効になっています。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

DDP 設定

D-Link Discovery Protocol (DDP) は、D-Link 製品で使用される通信プロトコルです。本機能を有効にすると、デバイスが検出可能になり、DNC サーバで管理できるようになります。



図 9-44 DDP 設定

1. DDP 機能を有効または無効に設定します。本機能は、デフォルトで有効になっています。

「基本」画面で各セクションの設定が完了したら、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード](#) (p.56)」を参照してください。

ローカル資格情報設定

お使いのデバイスのユーザ名とパスワードが表示されます。

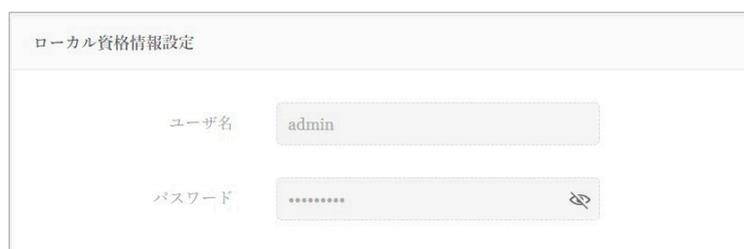


図 9-45 ローカル資格情報設定

スイッチ - IPv4 ACL

補足 スイッチ製品は未サポートです。

スイッチの IPv4ACL (Access Control List) 機能では、指定のトラフィックをブロックすることにより、ネットワークのパフォーマンスとセキュリティを向上させることができます。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > IPv4 ACL の順に移動して設定を行います。



図 9-46 プロファイル設定 - スイッチ - IPv4 ACL

■ ルールの作成

「ユーザー定義 IPv4ACL ルール」セクションでは、次の項目が表示されます。

項目	説明
シーケンス番号	シーケンス番号を設定します。シーケンス番号を自動割り当てするには、「Auto」にチェックを入れます。 ・ 指定可能範囲：1-65535
ポリシー	スイッチを通過するトラフィックを「許可」または「拒否」するように設定します。
プロトコル	プロトコルを選択します。 ・ 選択肢：「すべて」「TCP」「UDP」
送信元	送信元 IP アドレスを指定します。 ・ 「すべて」：すべてのトラフィック送信元が検証されます。 ・ 「IPv4 アドレス」：送信元 IPv4 アドレスを入力します。
送信元ポート	送信元ポートの番号を指定します。 ・ 「すべて」：すべてのトラフィック送信元が検証されます。 ・ 「ポートを入力」：0-65535 の範囲で送信元ポート番号を入力します。
送信先	送信先 IP アドレスを指定します。 ・ 「すべて」：すべてのトラフィック送信先が検証されます。 ・ 「IPv4 アドレス」：送信先 IPv4 アドレスを入力します。
送信先ポート	送信先ポートの番号を指定します。 ・ 「すべて」：すべてのトラフィック送信先が検証されます。 ・ 「ポートを入力」：0-65535 の範囲で送信先ポート番号を入力します。
説明	ルールの説明を入力します。

「追加」をクリックして、ルールを追加します。

「クリア」をクリックして、すべての設定値をリセットします。

■ ルールの編集・削除

「アクション」フィールドで、 をクリックしてルールを編集します。設定完了後、「保存」をクリックして設定を保存します。

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

スイッチ - アクセスポリシー

補足 スイッチ製品は未サポートです。

D-Link スイッチは、802.1X 認証、MAC 認証、およびポートセキュリティなどに対応しており、許可されていないクライアントがネットワークにアクセスできないように設定することができます。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > アクセスポリシーの順に移動して設定を行います。

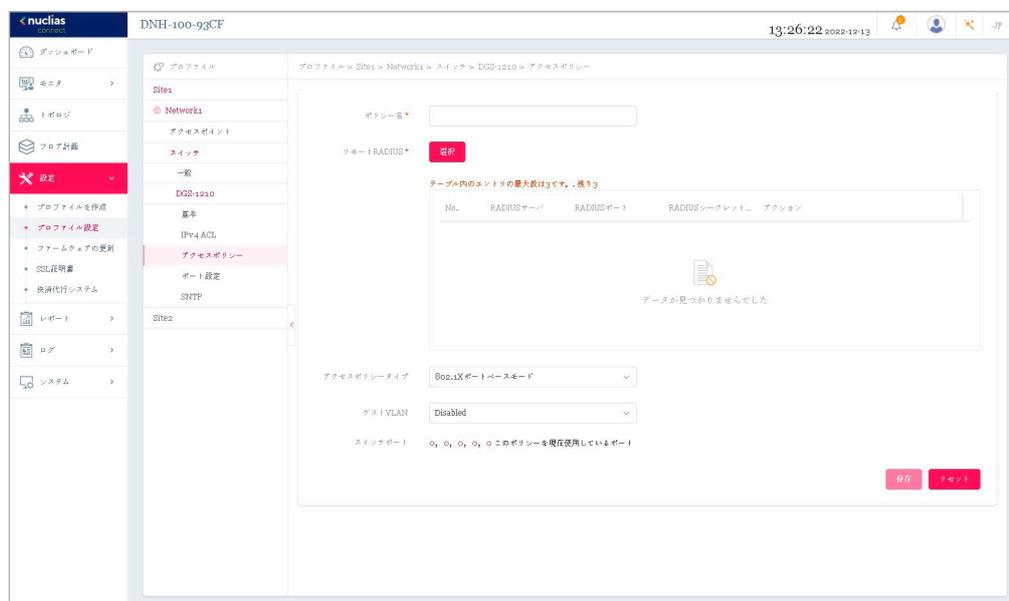


図 9-47 プロファイル設定 - スイッチ - アクセスポリシー

■ アクセスポリシーの作成

次の項目が表示されます。

項目	説明
ポリシー名	ポリシーの名前を入力します。
リモート RADIUS	スイッチがアクセス要求を転送する RADIUS サーバを最大 3 つ指定します。認証要求は、送信された順序で各 RADIUS サーバによって処理されます。 (1) 「選択」をクリックして、「RADIUS サーバ」画面で定義した既存の RADIUS サーバ一覧を表示します。 (2) 選択するサーバにチェックを入れて、「OK」をクリックします。 設定を中断する場合は「キャンセル」をクリックしてウィンドウを閉じます。 (3) 「選択した RADIUS サーバがテーブルに表示されます。エントリの順序を変更する場合、「アクション」欄で、  クリックしてエントリを上に移動し、  クリックしてエントリを下に移動します。エントリを削除する場合は  をクリックします。
アクセスポリシータイプ	「802.1X ポートベースモード」を選択します。このモードでは、リモート RADIUS サーバはポートごとに 1 人のユーザのみを認証します。
ゲスト VLAN	ドロップダウンメニューからゲスト VLAN ID を指定、または「Disabled (無効)」にします。 「基本」画面で定義済みの VLAN ID を指定可能です。1 つのスイッチで 1 つのゲスト VLAN のみをサポートします。 VLAN ID を選択すると、メンバポート情報が表示されます。番号をクリックすると、「ポート設定」画面に移動します。
スイッチポート	ポリシーが適用されているスイッチポートの数が一覧表示されます。番号をクリックすると、「ポート設定」画面に移動します。

「保存」をクリックして、アクセスポリシー設定を保存します。

ポリシー設定をリセットするには、「リセット」をクリックします。保存した設定が初期値にリセットされます。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

スイッチ - ポート設定

補足 スイッチ製品は未サポートです。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > ポート設定の順に移動して、各スイッチポートグループの概要を表示します。ポートグループの数は、スイッチシリーズによって異なります。

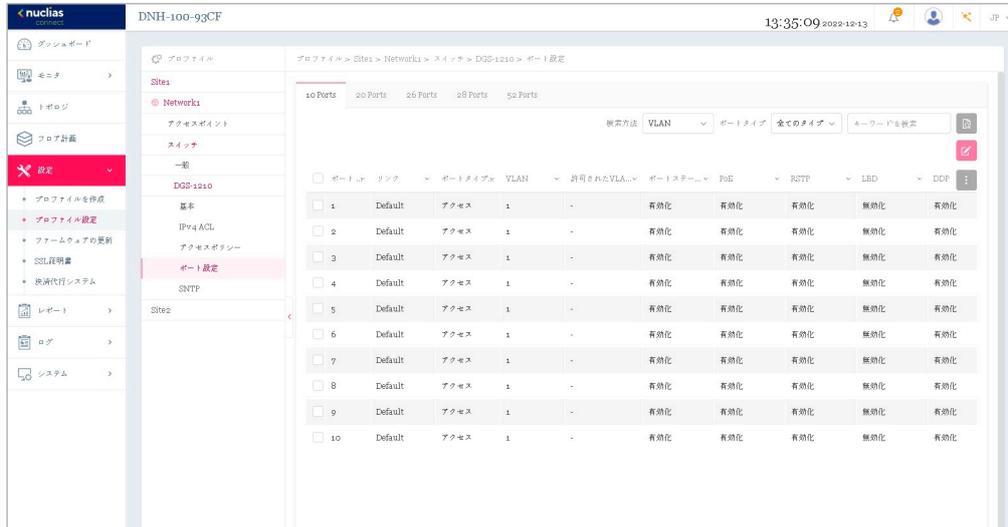


図 9-48 プロファイル設定 - スイッチ - ポート設定

■ 対象範囲の指定 / ポートの検索

- 以下のフィルタリング項目を指定し、関連するキーワードを入力して をクリックして検索を開始します。
 - 「検索方法」: 「VLAN」「Port」「Access Policy」
 - (VLAN を指定した場合) 「ポートタイプ」: 「全てのタイプ」「アクセス」「トランク」

テーブルには以下の項目が表示されます。

- 「ポート (番号)」「リンク」「ポートタイプ」「VLAN」「許可された VLAN」「ポートステータス」「PoE」「RSTP」「LBD」「DDP」「ポートシャットダウンスケジュール」「PoE 供給スケジュール」「アクセスポリシー」

■ ポート設定の変更

- 対象のポートのチェックボックスにチェックを入れ、 をクリックします。
- 画面下部にスクロールして、「ポート設定」セクションで該当のポート設定を編集します。
- 設定が完了したら、「保存」をクリックして変更を保存します。

「リンク」項目の値は「Default」(システムの既定値) であり、「プロファイル設定」では変更できません。

リンクの変更は、**モニタ > スイッチ > スイッチポート** または **モニタ > スイッチ** のアクション欄で をクリックし、デバイス詳細ページのポートタブを開いて当該項目を設定します。スタンドアロンモードでのみ設定可能です。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「[設定のアップロード \(p.56\)](#)」を参照してください。

スイッチ - SNTP 設定

補足 スイッチ製品は未サポートです。

SNTP (Simple Network Time Protocol) 機能を使用すると、スイッチはネットワーク上のクロックを同期できます。

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > SNTP 設定の順に移動します。



図 9-49 プロファイル設定 - スイッチ - SNTP 設定

次の項目が表示されます。

項目	説明
自動時間設定	
SNTP サーバを有効化	チェックボックスをクリックして、SNTP サーバを有効または無効にします。
SNTP サーバ 1	システム時刻を取得するプライマリ SNTP サーバの IPv4 アドレスまたはドメイン名を指定します。
SNTP サーバ 2	セカンダリ SNTP サーバの IPv4 アドレスまたはドメイン名を指定します。
タイムゾーン	
タイムゾーン	ローカルタイムゾーンを選択します。
サマータイムを有効化	チェックボックスをクリックして、サマータイムを有効または無効にします。
DST 開始 (24 時間)	DST (サマータイム) を開始する月、日、時刻を指定します。
DST 終了 (24 時間)	DST (サマータイム) が終了する月、日、時刻を指定します。
DST オフセット	ローカル DST オフセットとして構成する時間を指定します。 <ul style="list-style-type: none"> • 選択肢: 「30」「60」「90」「120」(分) • 初期値: 「60」(分)

「保存」をクリックして、設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード (p.56)」を参照してください。

ファームウェアの更新

「ファームウェアの更新」画面では、ファームウェアのアップグレードを実行できます。ファームウェアをアップグレードすることで、バグを防ぎ、デバイスに新しい機能を追加することができます。弊社 Web サイトで、新しいバージョンのファームウェアが利用可能かどうかを確認してください。

設定 > ファームウェアの更新 > サイト > ネットワーク の順に移動します。

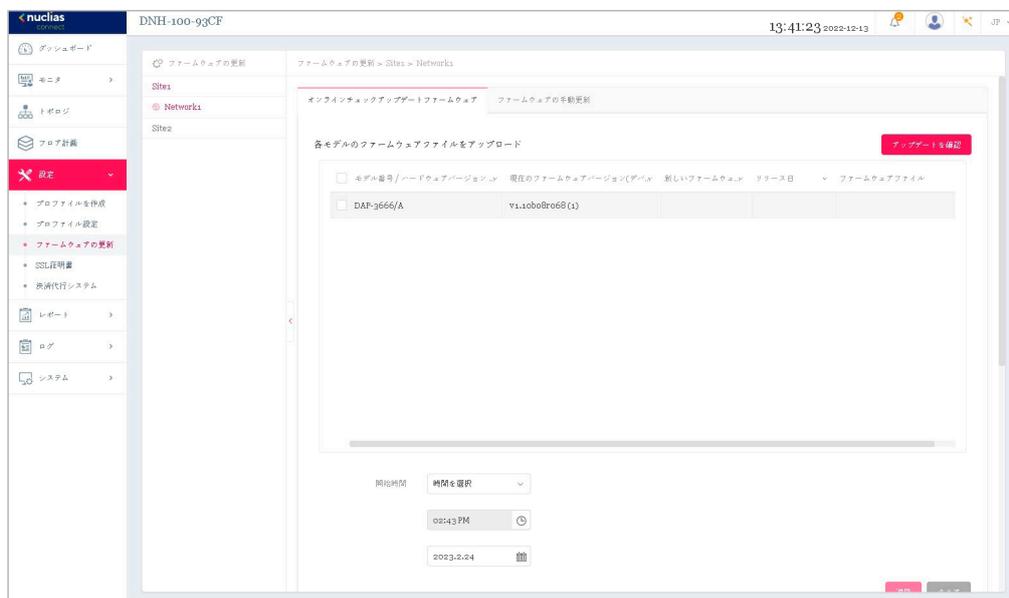


図 9-50 ファームウェアの更新

■ オンラインチェックアップデートファームウェア（日本で未サポートのファームウェアを使用しないために、手動更新を使用することを強く推奨します）

1. 「オンラインチェックアップデートファームウェア」タブをクリックします。
2. 「アップデートを確認」をクリックし、オンラインサーバで新しいファームウェアが利用可能かどうかを確認します。
3. 対象の製品のチェックボックスにチェックを入れます。
4. ドロップダウンメニューをクリックして、アクセスポイントにファームウェアをアップロードする開始時間を指定します。
 - ・「即時」：すぐにファームウェアをアップロードします。
 - ・「時間を選択」：ファームウェアをアップロードする日時を指定します。
5. 「適用」をクリックして、ファームウェアのアップデート設定を保存します。「即時」を指定した場合は、すぐにアップグレードが開始されます。定義済みの設定を削除するには、「クリア」をクリックします。

■ ファームウェアの手動更新

1. 「ファームウェアの手動更新」タブをクリックします。
2. 「変更」をクリックして、アップロードするファームウェアファイルを選択します。ファイルはモデル固有です。
3. ドロップダウンメニューをクリックして、アクセスポイントにファームウェアをアップロードする開始時間を指定します。
 - ・「即時」：すぐにファームウェアをアップロードします。
 - ・「時間を選択」：ファームウェアをアップロードする日時を指定します。
4. 「適用」をクリックして、ファームウェアのアップデート設定を保存します。「即時」を指定した場合は、すぐにアップグレードが開始されます。定義済みの設定を削除するには、「クリア」をクリックします。

注意

ファームウェアは、D-Link Japan ホームページで公開されているファームウェアバージョンのみがサポートされます。適用するファームウェアバージョンにご注意ください。

ファームウェアのアップグレードのステータスと結果は、画面下部の「実行ステータス」に表示されます。結果は、「実行時間」、「名前」、「IP アドレス」、「MAC アドレス」、「モデル番号」、「結果」でソートできます。



図 9-51 ファームウェアアップグレード - 実行ステータス

SSL 証明書

SSL 証明書機能では、ネットワークで使用する SSL 証明書をインストールすることができます。このタスクを実行するには、中間証明書が必要です。中間証明書は、認証局のルート証明書にバインドすることによって、SSL 証明書の信頼を確立するために使用されます。証明書の信頼設定を完了するには、本機能で証明書ファイルをアップロードする必要があります。

設定 > SSL 証明書 > サイト > ネットワークに移動します。



図 9-52 SSL 証明書

「SSL 証明書を更新」セクションでは、以下の設定項目が表示されます。

項目	説明
ファイルから証明書をアップロード	「ブラウザ ...」をクリックして、アップロードする SSL 証明書ファイルを選択します。
ファイルからキーをアップロード	「ブラウザ ...」をクリックして、アップロードする SSL キーファイルを選択します。

「アップロード」をクリックして、ファイルのアップロードを開始します。

アップロードのステータスと結果が画面下部の「実行ステータス」に表示されます。

決済代行システム ※本項目は日本ではサポート対象外となります。

決済代行システムは、ネットワーク内の電子商取引サービスを可能にする機能です。「決済代行システム」画面には、決済サービスを有効にするために必要な決済設定とオプションが表示されます。

設定 > 決済代行システムに移動します。

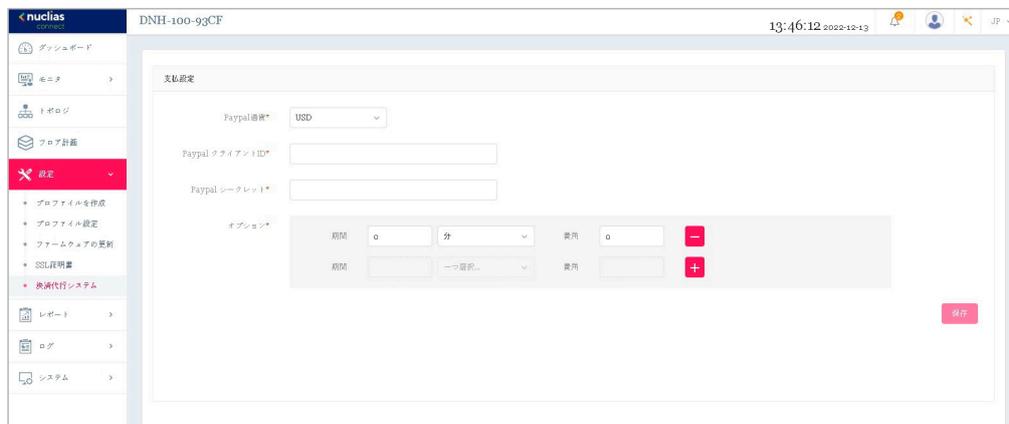


図 9-53 決済代行システム

項目	説明
Paypal 通貨	ドロップダウンメニューをクリックして、PayPal アカウントの通貨コードを選択します。
Paypal クライアント ID	PayPal アカウントのユーザ名を入力します。
Paypal シークレット	PayPal アカウントのパスワードを入力します。
オプション	期間（単位：分 / 時間 / 日）および費用を設定します。エントリを追加するには + をクリックします。

「保存」をクリックして設定を保存します。

第 10 章 レポート

- ・「アクセスポイントのレポート」
 - 「ピークネットワークアクティビティ」
 - 「時間別ネットワークアクティビティ」
 - 「日別ネットワークアクティビティ」
 - 「最もアクティブな AP」
- ・「スイッチのレポート」
 - 「時間別ネットワークアクティビティ」
 - 「日別ネットワークアクティビティ」
 - 「トップランキング」

アクセスポイントのレポート

ピークネットワークアクティビティ

ピークネットワークアクティビティ機能を使用すると、管理者はネットワーク上のワイヤレストラフィックを監視できます。すべてまたは特定のサイトおよびネットワークの無線アクティビティについて、クライアント数とトラフィックの使用状況を表示します。

レポート > アクセスポイント > ピークネットワークアクティビティに移動して、レポートを表示します。

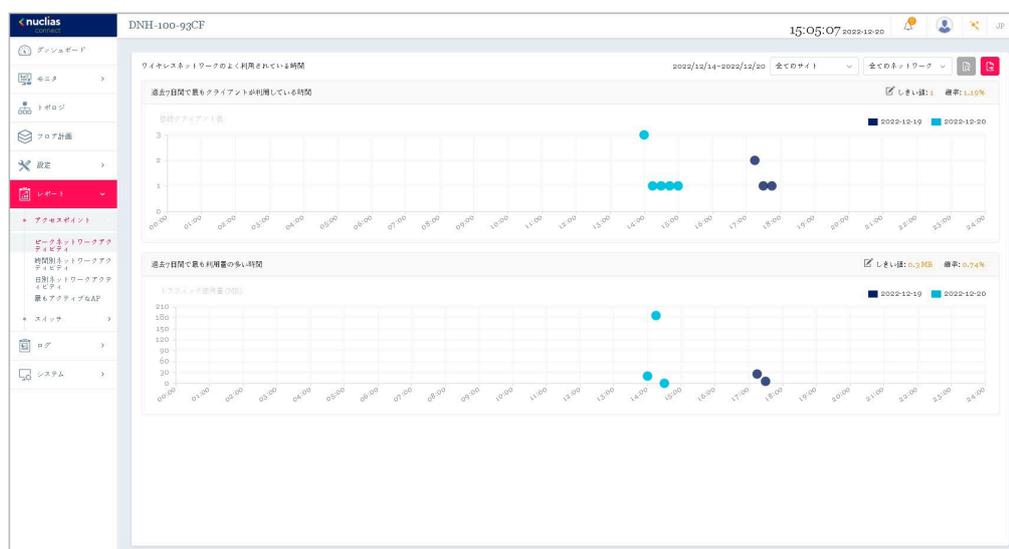


図 10-1 アクセスポイント - ピークネットワークアクティビティ

■ 対象範囲の指定

ドロップダウンメニューからサイトとネットワークを選択し、 をクリックして、対象のサイト/ネットワークのレポートを表示します。

レポートの生成後に、 をクリックしてレポートをローカル PDF ファイルに保存することができます。

■ レポート項目

以下のレポートが表示されます。

- ・ 過去 7 日間で最もクライアントが利用している時間
- ・ 過去 7 日間で最も利用量の多い時間

時間別ネットワークアクティビティ

時間別ネットワークアクティビティ機能を使用すると、管理者はネットワーク上の時間単位でのワイヤレストラフィックを監視できます。すべてまたは特定のサイトおよびネットワークのワイヤレスアクティビティについて、クライアント数とトラフィック使用量を表示します。

レポート > アクセスポイント > 時間別ネットワークアクティビティに移動して、レポートを表示します。

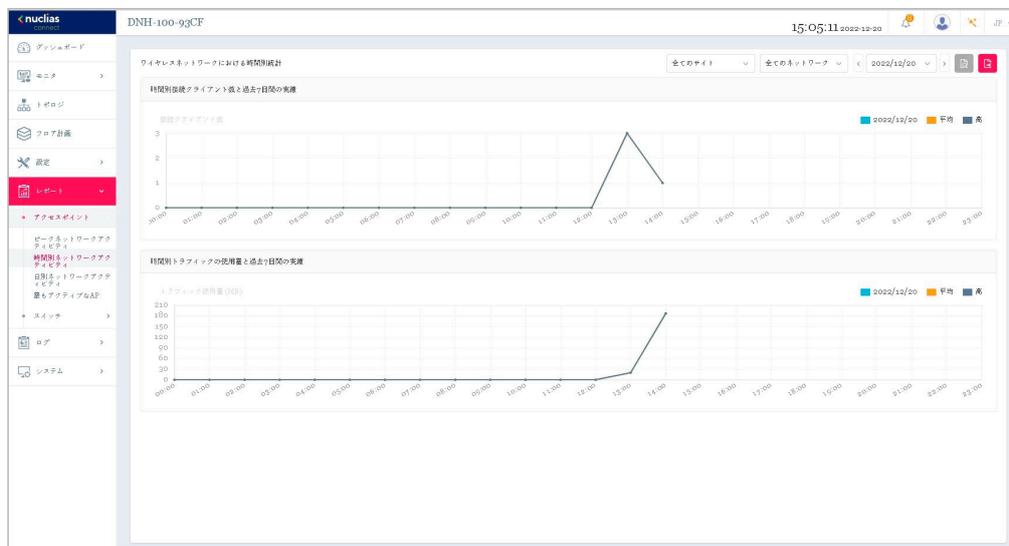


図 10-2 アクセスポイント - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

ドロップダウンメニューからサイトとネットワークを選択し、日付を選択後、 をクリックしてレポートを表示します。

レポートの生成後に、 をクリックしてレポートをローカル PDF ファイルに保存することができます。

■ レポート項目

以下のレポートが表示されます。

- ・ 時間別接続クライアント数と過去 7 日間の実績
- ・ 時間別トラフィックの使用量と過去 7 日間の実績

日別ネットワークアクティビティ

日別ネットワークアクティビティ機能を使用すると、管理者はネットワーク上の日単位のワイヤレストラフィックを監視できます。接続クライアント数とトラフィック使用量が日単位で表示されます。

レポート > アクセスポイント > 日別ネットワークアクティビティに移動して、レポートを生成および表示します。

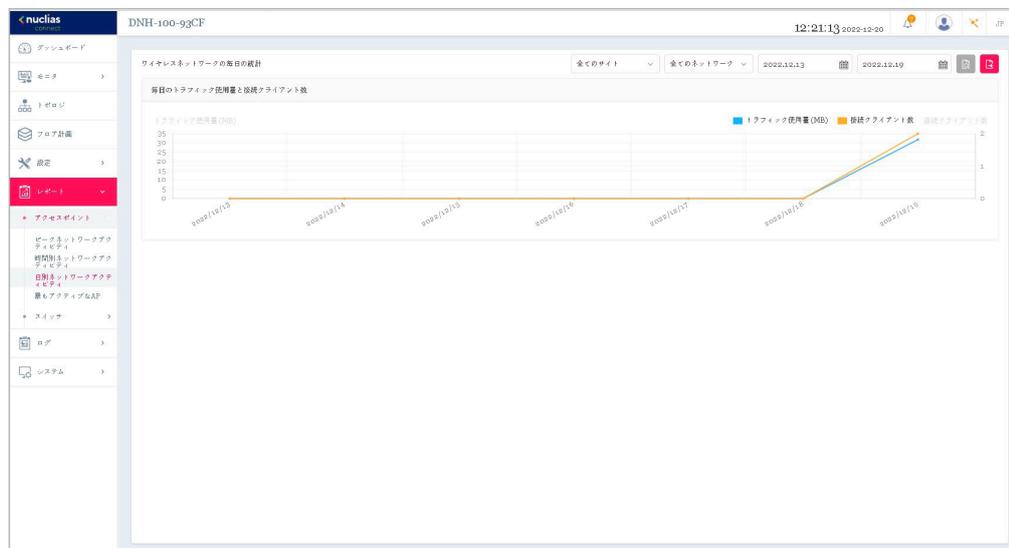


図 10-3 アクセスポイント - 日別ネットワークアクティビティ

■ 対象範囲の指定

特定期間のトラフィック使用量を表示するには、サイト、ネットワークを選択し、検索の開始日と終了日を定義します。検索パラメータを定義したら、 をクリックしてレポートを表示します。レポート生成後、 をクリックしてレポートを PDF ファイル形式で保存することができます。

■ レポート項目

以下のレポートが表示されます。

- 毎日のトラフィック使用量と接続クライアント数

最もアクティブな AP

特定のアクセスポイントのトラフィック使用量を表示します。

レポート > アクセスポイント > 最もアクティブな AP に移動して、レポートを表示します。

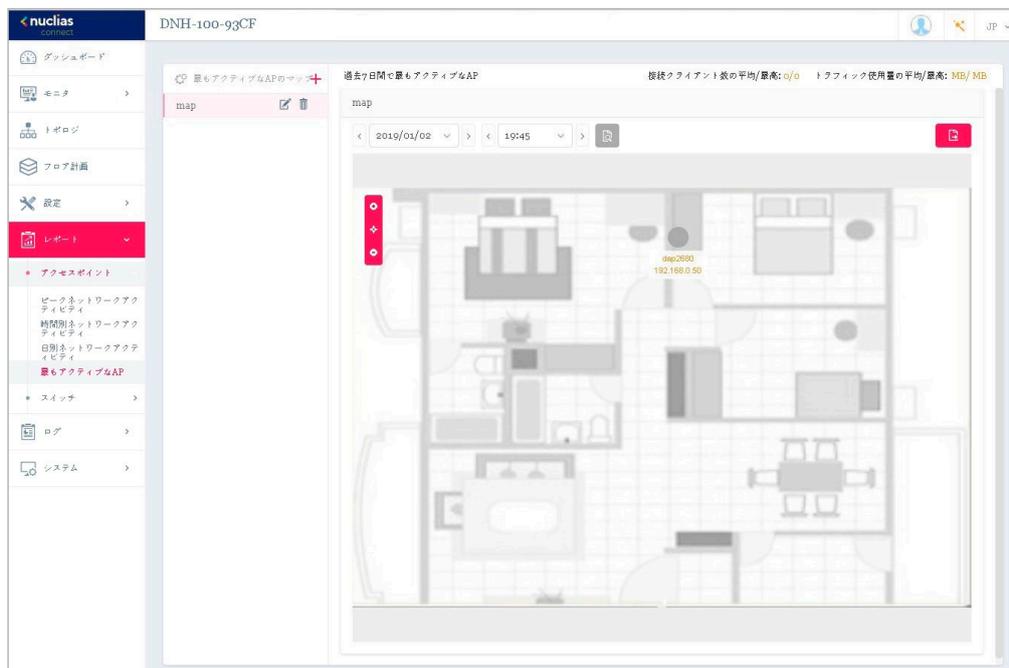


図 10-4 アクセスポイント - 最もアクティブな AP

■ 対象範囲の指定

マップを選択後に日時を指定し、 をクリックしてレポートを表示します。レポートの生成後、 をクリックしてレポートを PDF ファイル形式で保存することができます。

■ レポート項目

以下のデータが画面右上に表示されます。

- ・ 接続クライアント数の平均 / 最高
- ・ トラフィック使用量の平均 / 最高

アクセスポイントにマウスオーバーすることで、アクセスポイント毎の接続クライアント数 / トラフィック量を確認することができます。

■ マップの作成

1. デフォルトの状態から新規でマップを追加する場合、"**ここ**"をクリックします。
1つ以上のフロアプランが定義されている場合、左側にフロア計画の一覧が表示されます。**+** をクリックして、「最もアクティブな AP のマップを作成」画面を開きます。
2. 「最もアクティブな AP のマップ名」にマップ名を入力します。
3. 画像ファイルをドラッグ & ドロップするか、ローカルフォルダを参照して画像ファイルを選択します。(サポートされているファイル形式：PNG または JPG、最大 10MB)
4. 「AP を選択」をクリックして、使用可能な AP のリストからアクセスポイントを選択します。
5. アクセスポイントのアイコンをクリックしたまま、配置したい場所に移動します。
6. 「保存」をクリックして設定を保存します。

■ マップの編集・削除

左パネルのマップリストから、 または  をクリックしてマップを編集または削除できます。

注意

v1.2.0.2b2 をご利用の場合、既知の問題により日本語表示では左側のメニューに「最もアクティブな AP」メニューが表示されません。本レポートを表示、設定するには英語表示に切り替えてください。

スイッチのレポート

時間別ネットワークアクティビティ

時間別ネットワークアクティビティ機能を使用すると、管理者はネットワーク上の時間単位でのトラフィックを監視できます。すべてまたは特定のサイトおよびネットワークのワイヤレスアクティビティについて、トラフィック使用量と PoE 使用量を表示します。

補足 スイッチ製品は未サポートです。

レポート > スイッチ > 時間別ネットワークアクティビティに移動して、レポートを表示します。

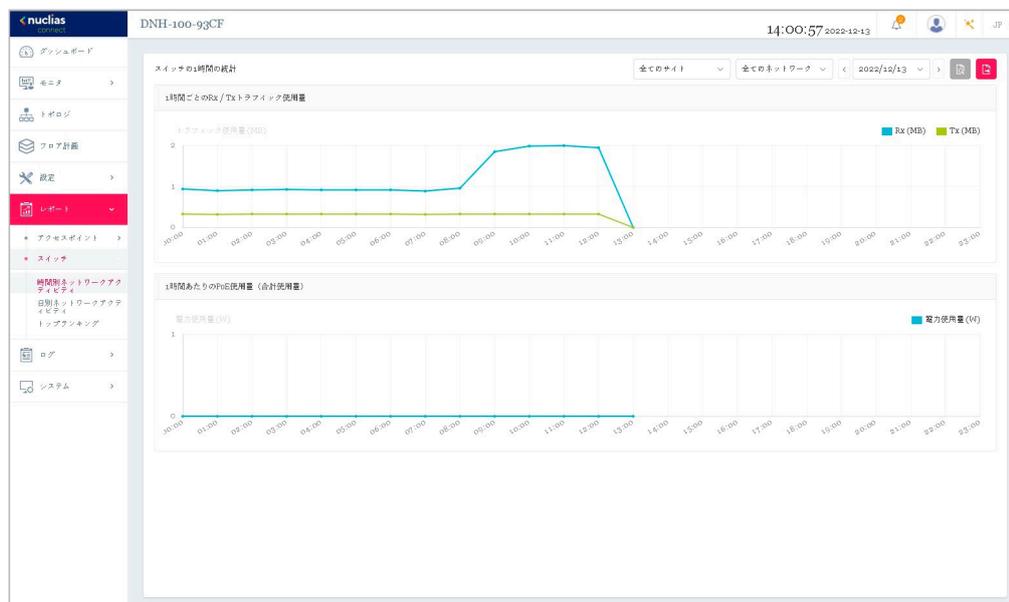


図 10-5 スイッチ - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

ドロップダウンメニューからサイトとネットワークを選択し、日付を選択後、 をクリックしてレポートを表示します。レポート生成後、 をクリックしてレポートをローカル PDF ファイルに保存することができます。

■ レポート項目

以下のレポートが表示されます。

- 1時間ごとの Rx/Tx トラフィック使用量
- 1時間あたりの PoE 使用量 (合計使用量)

日別ネットワークアクティビティ

日別ネットワークアクティビティ機能を使用すると、管理者はネットワーク上の日単位のトラフィックを監視できます。トラフィック使用量と PoE 使用量が日単位で表示されます。



スイッチ製品は未サポートです。

レポート > スイッチ > 日別ネットワークアクティビティに移動して、レポートを生成および表示します。

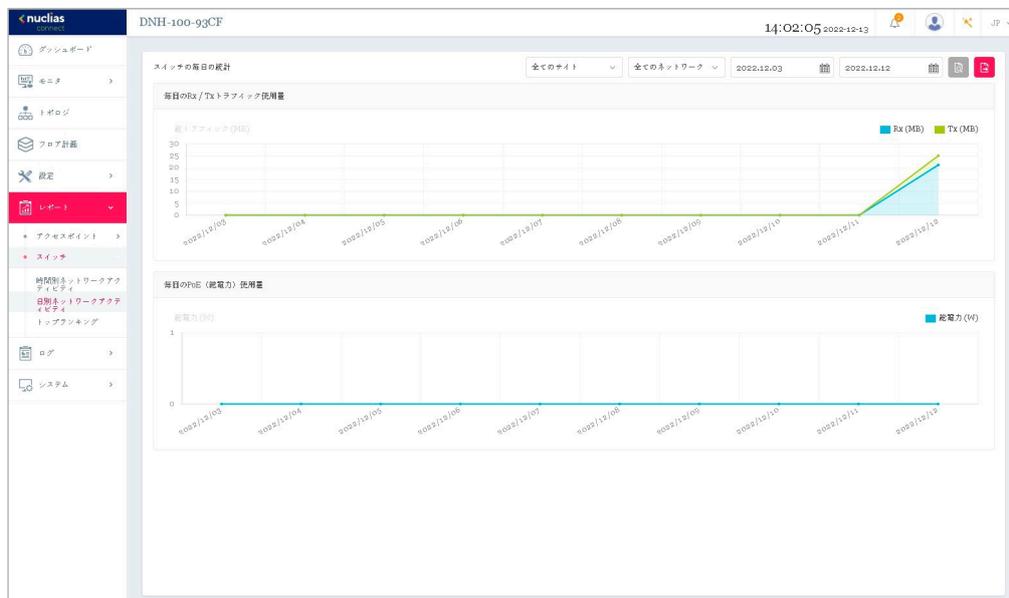


図 10-6 スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

特定期間のトラフィック使用量を表示するには、サイト、ネットワークを選択し、検索の開始日と終了日を定義します。検索パラメータを定義したら、をクリックしてレポートを表示します。レポート生成後、をクリックしてレポートを PDF ファイル形式で保存することができます。

■ レポート項目

以下のレポートが表示されます。

- 毎日の Rx / Tx トラフィック使用量
- 毎日の PoE (総電力) 使用量

トップランキング

トップランキングレポートでは、トップ 10 ランキングでソートされた各種スイッチトラフィックレポートを表示できます。

補足 スイッチ製品は未サポートです。

レポート > スイッチ > トップランキングに移動して、レポートを生成および表示します。

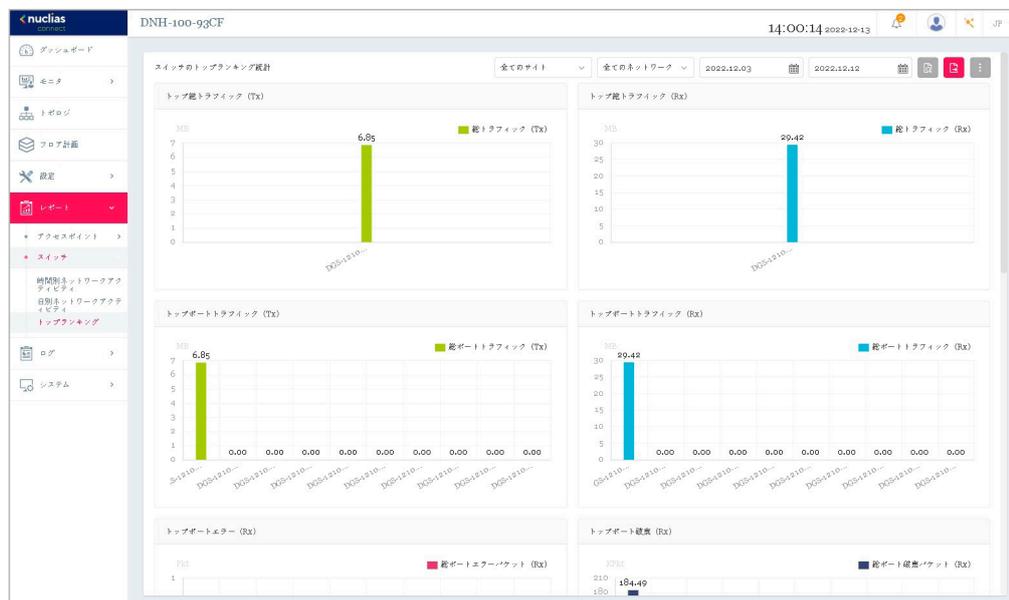


図 10-7 スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

サイト、ネットワークを選択し、検索の開始日と終了日を定義します。検索パラメータを定義したら、 をクリックしてレポートを表示します。レポート生成後、 をクリックしてレポートを PDF ファイル形式で保存することができます。

■ レポート項目

以下のレポートが表示されます。

- トップ総トラフィック (Tx/Rx)
- トップポートトラフィック (Tx/Rx)
- トップポートエラー (Rx)
- トップポート破棄 (Rx)
- トップポートマルチキャスト (Rx)
- トップポートブロードキャスト (Rx)
- トップポート利用率
- トップ PoE 電力消費
- トップ CPU 利用率

第 11 章 ログ

- 「デバイスシスログ」
- 「システムイベントログ」
- 「デバイスログ」
- 「監査ログ」
- 「アラート」

デバイスシスログ

シスログ機能を使用すると、システムログに関するイベントのアラートメッセージを表示できます。システムおよびキャプティブポータルログメッセージを確認することができます。

ログ > デバイスシスログに移動して、ログ情報を表示します。

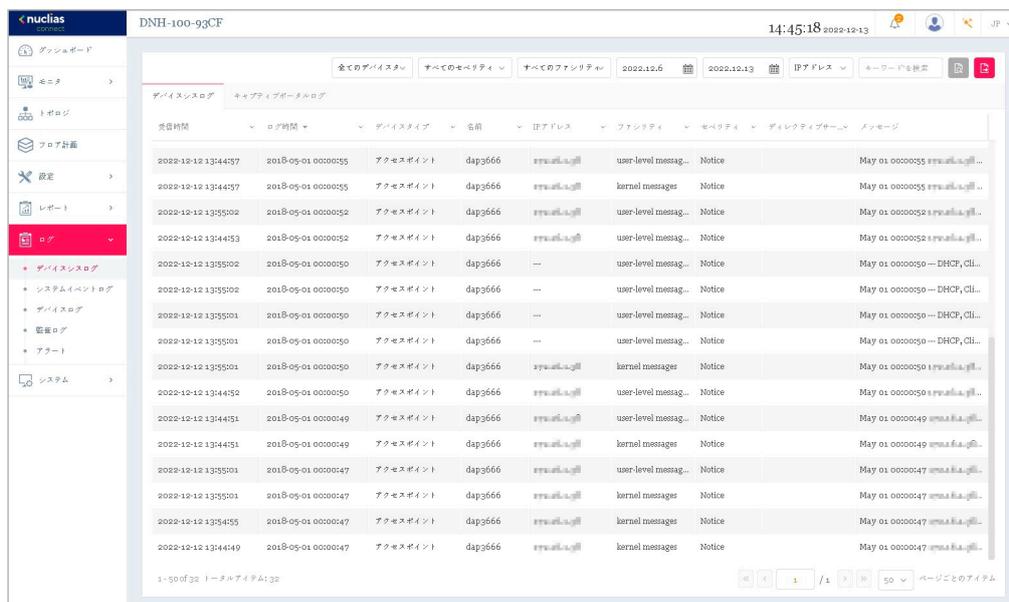


図 11-8 デバイスシスログ

フィルタ条件として以下の項目を指定し、 をクリックして対象を絞り込むことができます。

- デバイスタイプ
- イベントの重大度
- ファシリティシステム
- レポート期間
- IP アドレス / メッセージ、キーワード

レポート生成後、 をクリックしてレポートを PDF ファイル形式で保存することができます。

「キャプティブポータル」タブを選択すると、キャプティブポータルログが表示されます。

注意 Syslog は Network={network UUID} の形式で保存され、SSID へは変換されません。

システムイベントログ

システムイベントログ機能では、重要なアラートやアクションが必要なイベントを確認することで、円滑なオペレーションと障害の防止に役に立てることができます。

ログ > システムイベントログに移動します。

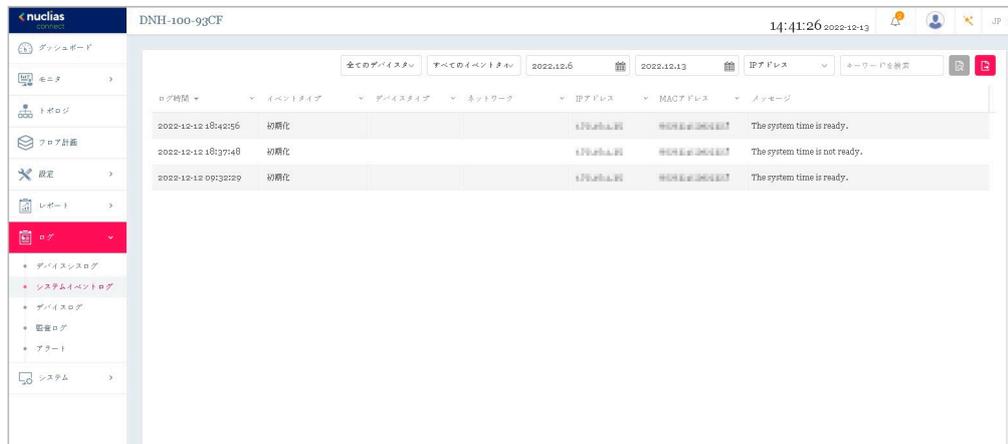


図 11-9 システムイベントログ

フィルタ条件として以下の項目を指定し、 をクリックして対象を絞り込むことができます。

- ・ デバイスタイプ
- ・ イベントタイプ
- ・ レポート期間
- ・ IP アドレス / メッセージ、キーワード

レポート生成後、 をクリックしてレポートを PDF ファイル形式で保存することができます。

デバイスログ

デバイスログには、デバイスの埋め込みメモリからのアラートメッセージが表示されます。システムメッセージとネットワークメッセージには、タイムスタンプとメッセージタイプが含まれます。ログ情報には、デバイス設定の同期、ファームウェアのアップグレード、設定のアップロード、クライアントのブロックなどが含まれます。

ログ > デバイスログに移動して、レポートを表示します。



図 11-10 デバイスログ

フィルタ条件として以下の項目を指定し、をクリックして対象を絞り込むことができます。

- デバイスタイプ
- 動作タイプ
- レポート期間
- IP アドレス/ログ詳細、キーワード

レポート生成後、をクリックしてレポートを PDF ファイル形式で保存することができます。

監査ログ

監査ログには、プロフィールやネットワークの作成や削除など、オブジェクトエンティティに対して実行できるユーザーアクティビティが記録されます。

ログ > 監査ログに移動して、レポートを表示します。

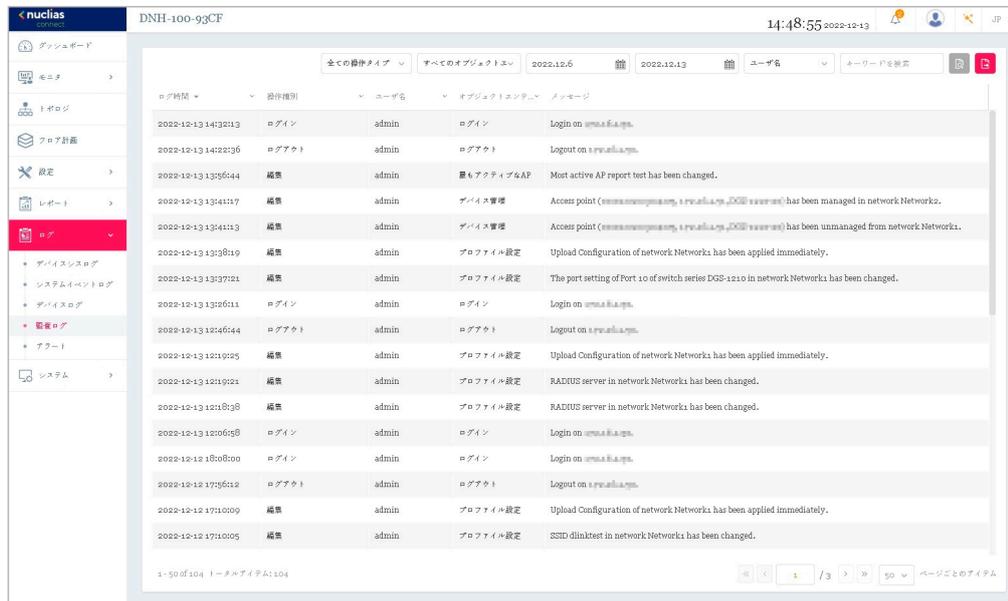


図 11-11 監査ログ

フィルタ条件として以下の項目を指定し、🔍 をクリックして対象を絞り込むことができます。

- 操作タイプ（オブジェクトエンティティで実行された操作）
- オブジェクトエンティティ（左ペインの機能タブに関連付けられたオブジェクト）
- レポート期間
- ユーザ名 / メッセージ、キーワード

レポート生成後、📄 をクリックしてレポートを Excel ファイル形式で保存することができます。

ファイルは、Nuclias_Connect_log type_YYYY_MMDD_HHMMSS という名前でブラウザの所定のダウンロードディレクトリに保存されます。

アラート

アラート画面には、新しいファームウェアリリース、ポートのリンクまたはブロック、デバイスのオンラインステータスなどのアラートイベントが記録されます。

ログ>アラートに移動して、レポートを表示します。

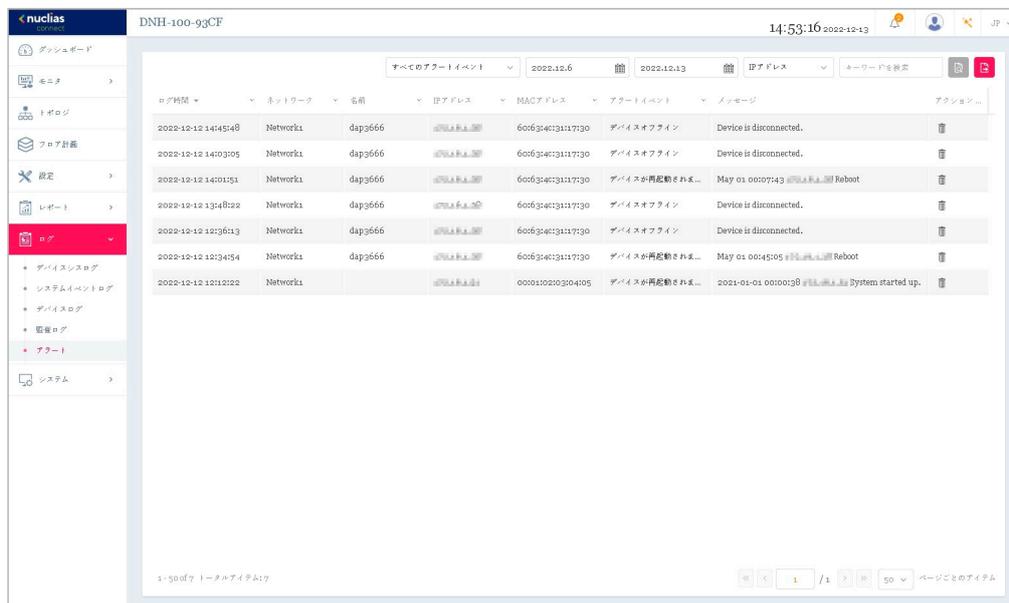


図 11-12 アラート

フィルタ条件として以下の項目を指定し、🔍をクリックして対象を絞り込むことができます。

- アラートイベント
- レポート期間
- IP アドレス / メッセージ、キーワード

レポート生成後、📄をクリックしてレポートを Excel ファイル形式で保存することができます。

ファイルは、Nuclias_Connect_log type_YYYY_MMDD_HHMMSS という名前でブラウザの所定のダウンロードディレクトリに保存されます。

第 12 章 システム管理

- 「デバイス管理」
- 「ユーザ管理」
- 「設定」
- 「リソース」
- 「Nuclias Connect について」

デバイス管理

デバイス管理機能を使用すると、ネットワーク上のすべてのデバイスのリストを管理対象デバイスと非管理対象デバイスの両方で表示できます。

システム > デバイス管理に移動します。

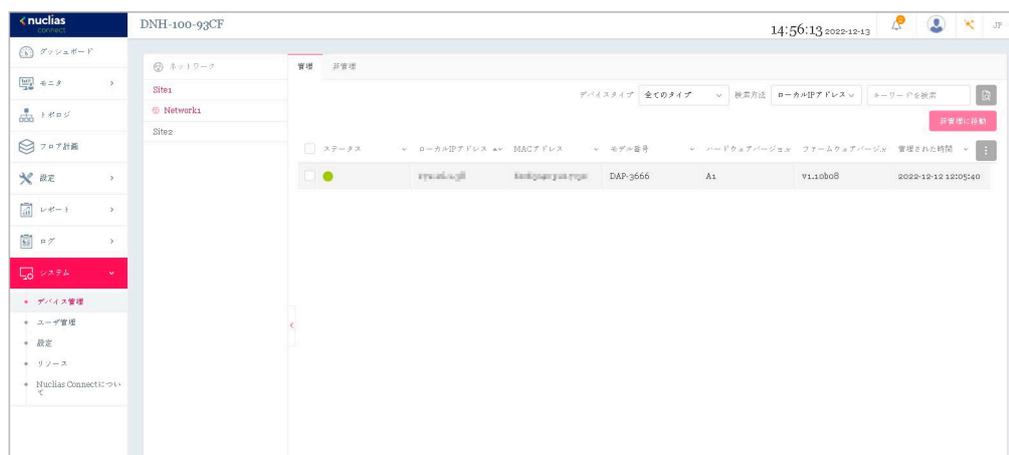


図 12-1 デバイス管理 - 管理タブ

最初にサイトとネットワークを選択し、「管理」「非管理」タブを選択して、管理対象デバイスまたは非管理対象デバイスのリストを表示します。

■ 管理デバイスリスト / 非管理デバイスリストへの移動と削除

各タブの右上隅には、デバイスを「非管理に移動」または「管理に移動」するためのボタンがあります。「非管理」タブの「管理に移動」ボタンの横にある「削除」ボタンを使用して、ネットワーク上のデバイスを削除できます。

■ ネットワークの移動

「非管理」タブに表示されたデバイスは、「管理に移動」右横の▼ボタンをクリックして、別の定義済みネットワークに移動することができます。

■ 表示項目

デバイスのリストには以下の項目が表示されます。各項目のソートボタンをクリックすると、ソートすることができます。

表示項目を変更するには、☰をクリックします。

- ステータス
- ローカル IP アドレス
- MAC アドレス
- モデル番号
- ハードウェアバージョン
- ファームウェアバージョン
- バックアップファームウェアバージョン
- 管理された時間 / 非管理になった時間

補足

管理配下のアクセスポイントに関して、以下の仕様があります。

- アクセスポイントが Nuclias Connect 管理配下になると、DAP 側のローカル UI は機能（表示項目）が限定されます。
- ローカル UI の **Maintenance > Administration Settings** から、「Nuclias Connect Settings」を「Disable」に設定し、UI の読み込み直または再ログインすることにより、DAP 側から設定や状態を確認することが可能です。スタンドアロンに変更されたアクセスポイントを Nuclias Connect 管理に戻すには、DAP ローカル UI を「Nuclias Connect Settings」を「Enable」にした後、状態により、再起動、または "Save and Activate" の実行が必要です。

ユーザ管理

ユーザステータス

ユーザステータス画面では、登録されているユーザプロフィールの現在のステータスを表示したり、プロフィールを編集 / 削除したりすることができます。

システム > ユーザ管理に移動して、ユーザステータス情報を表示します。



図 12-2 ユーザ管理 - ユーザステータスタブ

■ ログインステータスの確認

「ステータス」欄には、ユーザのログイン状態が表示されます。

- はユーザがログイン状態であることを示します。
- はユーザがログオフしていることを示します。

■ ユーザプロフィールの作成 / 編集

1. ユーザプロフィールを作成するには、「ユーザを追加」をクリックします。
既存のユーザプロフィールを編集するには、ユーザのアクション欄で をクリックします。
2. 以下の項目を設定します。
 - 「ユーザ名」
 - 「パスワード」
 - 「メールアドレス」
 - 「メールアラートを受信」
 - 「権限」
 - 「権限ステータス」
 - 「設置場所」
 - 「電話番号」
 - 「説明」

「権限」では、以下のユーザ権限を割り当てることができます。

項目	説明
ルート管理者	このサーバ上のすべてのサイト / ネットワークを管理できます。
ローカル管理者	権限が割り当てられたネットワークを管理できます。
ルートユーザ	このサーバ上のすべてのサイト / ネットワークを表示できます。
ローカルユーザ	権限が割り当てられたネットワークを表示できます。
フロントデスクスタッフ	パスコードを生成および管理できます。

※ 「admin」アカウントは削除不可、ユーザ名や権限の設定を変更することもできません。

3. ユーザ設定が完了したら、「作成 / 保存」をクリックしてプロフィールを保存します。
編集をキャンセルするには、「キャンセル」をクリックして画面を閉じます。

図 12-3 ユーザを作成

ユーザ権限

「ユーザ権限」タブでは、選択したネットワークについて、ユーザを追加、表示、承認 / 承認解除することができます。

システム > ユーザ管理に移動し、「ユーザ権限」タブを選択します。

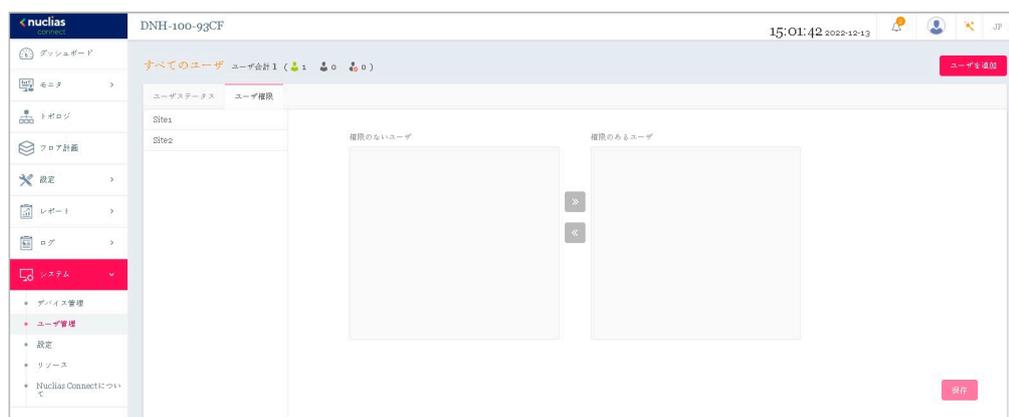


図 12-4 ユーザ管理 - ユーザ権限タブ

■ ユーザの承認 / 承認解除

1. 既存のユーザを承認するには、使用可能なサイトを選択し、対象のネットワークをクリックします。
2. ネットワークで使用可能なユーザが表示されます。
3. 「権限のないユーザ」の一覧から、対象ユーザのチェックボックスにチェックを入れます。
4. ユーザを選択したら、➡をクリックして「権限のあるユーザ」列に移動し、ユーザを承認します。
ユーザの承認を解除するには、同様の手順で「権限のあるユーザ」から「権限のないユーザ」へ対象ユーザを移動します。
5. 「保存」をクリックして設定を保存します。

設定

「設定」画面には、以下のタブが表示されます。

- 「一般」
- 「接続」
- 「SMTP」
- 「バックアップ&リストア」
- 「ファームウェアアップグレード」
- 「システム設定」
- 「シングルサインオン (SSO)」
- 「アラート」
- 「FOTA」

一般

「一般」タブには、組織のロゴや CAPTCHA 機能など、システム設定が含まれます。

システム > 設定に移動して、「一般」タブを表示します。

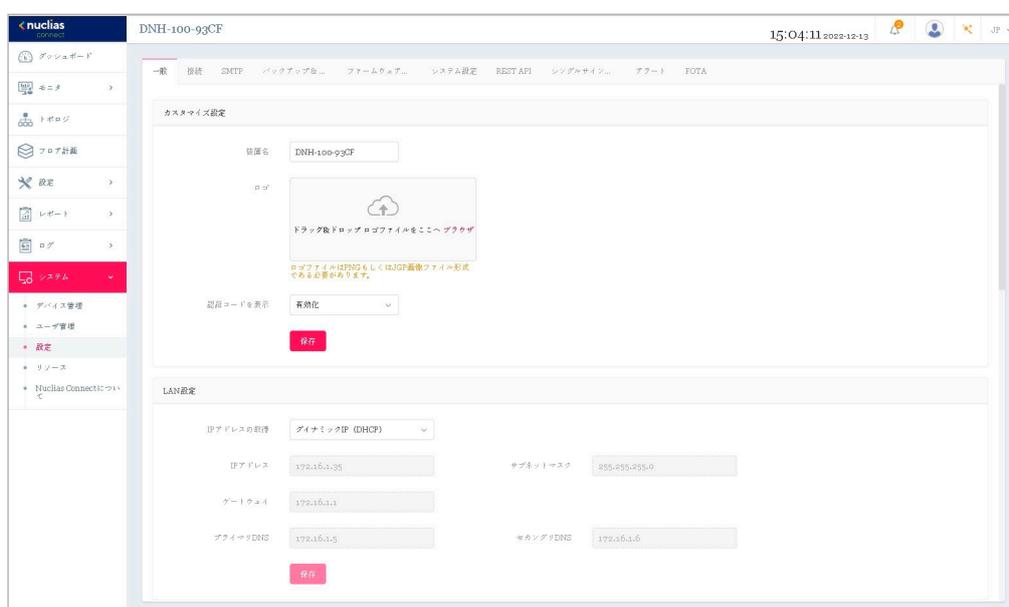


図 12-5 設定 - 一般タブ

「カスタマイズ設定」セクションでは、以下の設定項目が表示されます。

項目	説明
装置名	装置名を入力します。
ロゴ	インタフェースロゴとして使用するファイルを設定します。 「ブラウザ」をクリック、またはドラッグ & ドロップによりファイルをアップロードします。 ・ ファイル形式：PNG または JPG
認証コードを表示	ドロップダウンメニューをクリックして、CAPTCHA 認証機能を有効または無効にします。

「保存」をクリックして設定を保存します。

「LAN 設定」セクションでは、以下の設定項目が表示されます。

項目	説明
IP アドレスの取得	IP インタフェースの IP アドレス取得方法を選択します。 ・ 選択肢：「スタティック IP アドレス (手動)」 「ダイナミック IP (DHCP)」 注意 DHCP サーバは推奨されません。
IP アドレス	IP インタフェースの IP アドレスを入力します。
サブネットマスク	IP インタフェースのサブネットマスクを入力します。
ゲートウェイ	IP インタフェースのゲートウェイを入力します。(オプション)
プライマリ DNS	IP インタフェースの優先 DNS アドレスを入力します。(オプション)
セカンダリ DNS	IP インタフェースの優先 DNS アドレスを入力します。(オプション)

「保存」をクリックして設定を保存します。

「日付と時間」セクションでは、以下の設定項目が表示されます。

項目	説明
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
サマータイムを有効化	チェックボックスをオンにすると、サマータイム機能が有効になります。
DST 開始 (24 時間)	ドロップダウンメニューをクリックして、サマータイム (DST) の開始日時を指定します。
DST 終了 (24 時間)	ドロップダウンメニューをクリックして、サマータイム (DST) の終了日時を指定します。
DST オフセット (分)	ドロップダウンメニューをクリックして、DST オフセット (分) を選択します。
NTP	NTP サーバを使用してデバイスの日時を管理する場合は、本項目にチェックを入れます。
NTP サーバ 1	NTP サーバのアドレスを指定します。
NTP サーバ 2	セカンダリ NTP サーバのアドレスを指定します。
コンピュータの時間をコピー	「NTP」にチェックを入れない場合、手動で時刻を設定するか、本項目をクリックして管理コンピュータの時刻をコピーします。

「保存」をクリックして設定を保存します。

「コンソール設定」セクションでは、以下の設定項目が表示されます。

項目	説明
コンソール	コンソールポート経由での管理を有効にします。
コンソールプロトコル	コンソールプロトコルを選択します。 • 選択肢：「Telnet」「SSH」
タイムアウト	ドロップダウンメニューをクリックして、タイムアウト時間を選択します。

「保存」をクリックして設定を保存します。

「デバイス設定」セクションでは、以下の設定項目が表示されます。

項目	説明
ライブパケット間隔	ドロップダウンメニューをクリックして、ライブパケット間隔を選択します。

「保存」をクリックして設定を保存します。

接続

「接続」タブには、デバイスアクセスアドレス、ポート、および SSL 証明書の設定が表示されます。

システム > 設定に移動し、「接続」タブをクリックします。

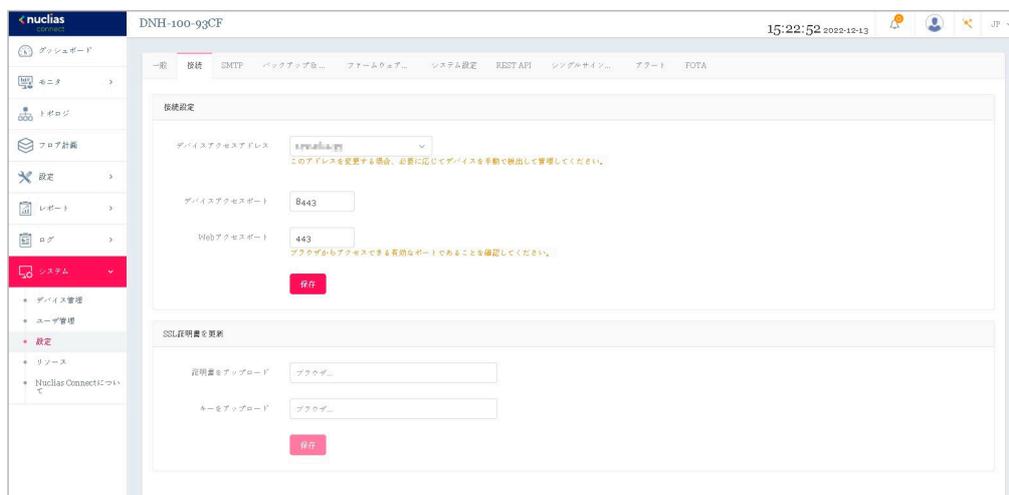


図 12-6 設定 - 接続タブ

「接続設定」セクションでは、以下の設定項目が表示されます。

項目	説明
デバイスアクセスアドレス	Nuclias Connect サーバアプリケーションの IP アドレスを入力します。 リモート AP を管理するには、IP アドレスがパブリック IP アドレスである必要があります。ファイアウォールやルータを介したリモート AP 管理の場合、IP マッピングが必要です。
デバイスアクセスポート	Nuclias Connect サーバアプリケーションのリスニングポート番号を入力します。ファイアウォールやルータを介したリモート AP 管理の場合、受信ポートを開く必要があります。 • 初期値：8443
Web アクセスポート	インストール時に定義された Web アクセスポートが表示されます。

「保存」をクリックして設定を保存します。

注意 デバイスアクセスアドレスが mDNS 名の場合、Android 端末においては、パスコード認証利用時に Chrome ブラウザで認証画面が表示されません。

「SSL 証明書を更新」セクションでは、以下の設定項目が表示されます。

項目	説明
証明書をアップロード	「ブラウザ…」をクリックして、アップロードする SSL 証明書ファイルを選択します。
キーをアップロード	「ブラウザ…」をクリックして、アップロードする SSL キーファイルを選択します。

「保存」をクリックして設定を保存します。

SMTP

「SMTP」タブには、簡易メール転送プロトコル（SMTP）のカスタマイズ可能な設定が表示されます。これは、パスワードのリセット確認メールなど、システムに代わってメールを送信するために必要となるため、必ず設定されることを推奨します。

システム > 設定に移動し、「SMTP」タブをクリックして SMTP 情報を表示します。

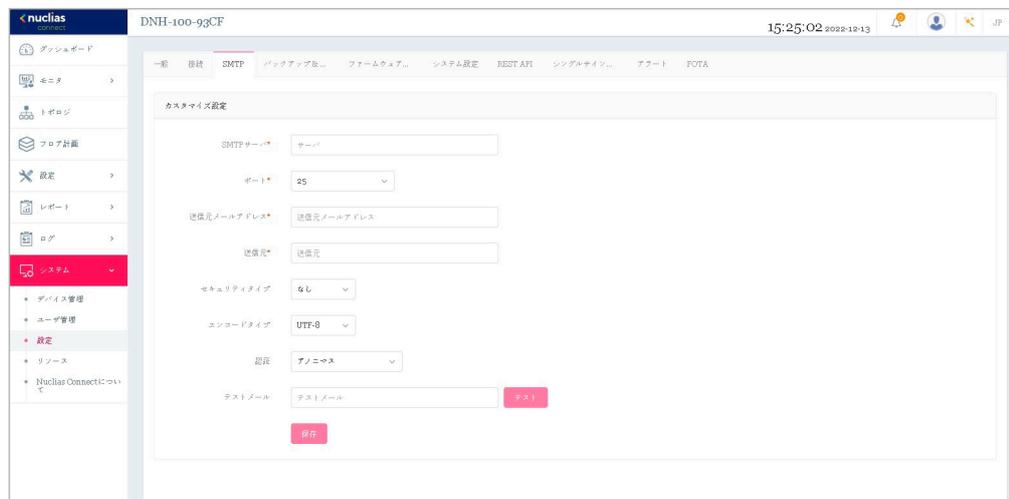


図 12-7 設定 - SMTP タブ

以下の設定項目が表示されます。

項目	説明
SMTP サーバ	SMTP サーバの IP アドレスまたはドメイン名を入力します。
ポート	SMTP サーバのポート番号を指定します。 ・ 選択肢：「25」「465」「587」
送信元メールアドレス	送信者のメールアドレスを入力します。
送信元	送信者の名前を入力します。
セキュリティタイプ	ドロップダウンメニューをクリックして、電子メールシステムで使用するセキュリティタイプを選択します。 ・ 選択肢：「なし」「SSL」
エンコードタイプ	ドロップダウンメニューをクリックして、電子メールクライアントと一致するエンコードタイプを選択します。 ・ 選択肢：「UTF-8」「ASC-II」
認証	ドロップダウンメニューをクリックして、ログイン中の認証メカニズムを選択します。 ・ 選択肢：「アノニマス」「SMTP 認証」
ユーザ名	認証で「SMTP 認証」を選択した場合は、SMTP サーバの認証ユーザ名を入力します。
パスワード	認証で「SMTP 認証」を選択した場合は、SMTP サーバの認証パスワードを入力します。
テストメール	受信者の電子メールアドレスを入力して、SMTP サーバ経由の電子メールのテスト送信を行います。「テスト」をクリックしてテスト送信を開始します。

「保存」をクリックして設定を保存します。

補足 「セキュリティタイプ」で「なし」を指定した場合、SMTP サーバで STARTTLS がサポートされる場合はメールは STARTTLS で送信されます。SMTP サーバで STARTTLS がサポートされない場合、メールはプレーンテキストで送信されます。「セキュリティタイプ」で「TLS」を指定した場合、メールは TLS で送信されます。

バックアップ&リストア

「バックアップ&リストア」タブでは、ログやコンフィグレーションの手動/自動バックアップ、リストアを行うことができます。

システム > 設定に移動し、「バックアップ&リストア」タブをクリックしてバックアップおよびリストア設定を表示します。

■ 自動バックアップ

コンフィグレーションの自動バックアップ設定を行います。

図 12-8 自動バックアップ設定

「自動バックアップ設定」セクションには、以下の設定項目が表示されます。

項目	説明
自動ログバックアップ	自動ログバックアップの種類を選択します。 ・ 選択肢：「無効化」「マイクロ SD」「外部シスログサーバ」
外部シスログサーバ	外部シスログサーバの IP アドレスまたはホスト名を入力します。

「保存」をクリックして設定を保存します。

■ バックアップ設定

コンフィグレーションとログの手動バックアップ、ダウンロード、削除を行うことができます。

図 12-9 バックアップ設定

すぐにバックアップ をクリックしてコンフィグレーションファイルまたはログファイルを保存します。

バックアップファイルのダウンロード

 をクリックし、コンピュータのハードドライブまたは USB ドライブにバックアップファイルをダウンロードします。

図 12-10 バックアップ (ダウンロード)

以下の設定項目が表示されます。

項目	説明
To	バックアップファイルの保存先を指定します。 ・ 選択肢：「自分のコンピュータ」「USB ストレージ」
すべてのバックアップファイル	ダウンロード可能なすべてのファイルが表示されます。ダウンロード対象のファイルを指定します。

「ダウンロード」をクリックして、ファイルをダウンロードします。

バックアップファイルの削除

 をクリックし、デバイスに保存されているバックアップファイルを削除します。

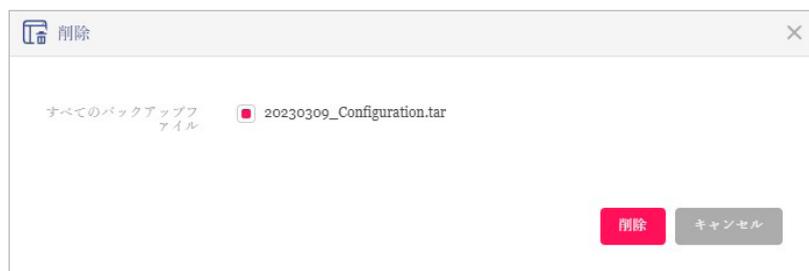


図 12-11 システム-バックアップ (削除)

削除するファイルを選択し、「削除」をクリックします。

■ リストア設定

コンフィグレーションのリストアを行います。



図 12-12 リストア設定

以下の設定項目が表示されます。

項目	説明
設定のアップロード元	アップロードファイルの取得元を指定します。 ・ 選択肢: 「自分のコンピュータ」「USB ストレージ」
ファイル	「ファイルを選択」をクリックして保存済みのバックアップファイルを選択し、「リストア」ボタンをクリックして設定を復元します。

注意 リストアは即時に実行され、Nuclias Connect は再起動されます。

注意 統計データ (ログ、レポート) およびシングルサインオン (SSO) 設定はリストアされません。ログとレポートは必要に応じて、バックアップやエクスポートを行ってください。シングルサインオン設定は、リストア後に再度設定を行ってください。

ファームウェアアップグレード

「ファームウェアアップグレード」タブには、DNH-100のファームウェア更新で使用する設定が表示されます。

システム > 設定に移動し、「ファームウェアアップグレード」タブをクリックして設定を表示します。



図 12-13 設定 - ファームウェアアップグレードタブ

以下の設定項目が表示されます。

項目	説明
ファームウェアのアップロード元	ファームウェアファイルの取得元を選択します。 ・ 選択肢: 「自分のコンピュータ」「USB ストレージ」「FTP サーバー」
ファイル	「ブラウザ ...」をクリックして保存済みのファームウェアファイルを選択します。 「ハードディスク」「USB ストレージ」を選択した場合のみ指定可能です。
FTP サーバー	FTP サーバの IP アドレスまたはドメイン名を入力します。
ポート	FTP サーバのポート番号を入力します。
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力します。
ファームウェアファイル	FTP サーバ上に保存されたファームウェアファイルのパスおよびファイル名を入力します。

「保存」をクリックして設定を保存します。



補足 ファームウェアアップグレードで「USB ストレージ」を選択する場合、ファームウェアファイルを Root Directory に配置する必要があります。

システム設定

「システム設定」タブでは、DNH-100 の再起動、工場出荷時へのリストア、microSD カードのフォーマットを行うことができます。

システム > 設定に移動し、「システム設定」タブをクリックします。



図 12-14 設定 - システム設定タブ

以下の設定項目が表示されます。

項目	説明
デバイスをシャットダウン	「シャットダウン」をクリックして DNH-100 をシャットダウンします。 注意 シャットダウン直後は、DNH-100 の電源を入れても保護機構が作動しているため起動しません。再度起動するには、シャットダウン後、3分以上経過してから DNH-100 の電源を入れてください。
デバイスを再起動	「再起動」をクリックして DNH-100 を再起動します。
工場出荷時設定	「リストア」をクリックして工場出荷時の設定へリストアします。「IP アドレスと Web アクセスポートを除く」にチェックを入れた場合、デバイスの IP アドレスおよび Web アクセスポートの設定は保持されます。
マイクロ SD カードをフォーマット	「フォーマット」をクリックして microSD カードをフォーマットします。フォーマットを実行すると、microSD カードのすべてのデータが消去されます。

注意 microSD カードを抜く際は、システムをシャットダウンする必要があります。

注意 電源ケーブルの抜き差しによるシャットダウンを行うと、microSD カードのアンマウント処理が適切に行われない可能性があります。本画面の「シャットダウン」ボタンからシャットダウンを実施してください。

注意 「マイクロ SD カードをフォーマット」を実行する際、システムは再起動されます。

REST API

REST API は、2つのアプリケーションがインターネットとデバイスを通じて相互に通信するためのソフトウェアインタフェースです。本機能を有効にすると、Nuclias Connect は REST API を介してサードパーティアプリケーションと通信できます。

システム > 設定に移動し、「REST API」タブをクリックします。



図 12-15 設定 - REST API タブ

以下の設定項目が表示されます。

項目	説明
REST API	REST API を有効または無効に設定します。
REST API キー	REST API キーが表示されます。 「キーを再生成」をクリックして REST API キーを再生成します。 「コピー」をクリックして REST API キーをコピーします。

「保存」をクリックして設定を保存します。

シングルサインオン (SSO)

シングルサインオン (SSO) 機能では、1つの Nuclias アカウントにより Nuclias Cloud および Nuclias Connect ポータルの両方にアクセスできるように設定することができます。

システム > 設定に移動し、「シングルサインオン (SSO)」タブをクリックします。



図 12-16 設定 - シングルサインオン (SSO) タブ

Nuclias アカウントを取得していない場合、「アカウントを作成」をクリックしてアカウントを作成します。

■ アカウントの登録

1. 「アカウントを作成」をクリックすると、以下の画面が表示されます。サーバの地域と国を選択し、「次」をクリックします。アカウントは、選択した地域および国のサーバ内に作成されます。



図 12-17 地域 / 国の選択

第12章 システム管理

2. アカウント情報（ユーザ、組織、住所など）の入力画面が表示されます。必要な情報を入力し、利用規約およびプライバシー契約に同意します。アカウント作成ボタンが有効になります。

ステップ 2
Nucliasアカウントを作成する事で、Nuclias Connect又はNuclias Cloudにログインすることができます。

nuclias connect

メールアドレス

フルネーム

パスワード

新しいパスワードの確認

組織名

Japan

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

住所

私はこれら全てを読み、同意します。 : [利用規約](#) [並びにプライバシー](#)

D-Link製品のアップデートやオファーをメールでお知らせします。

私は人間です  hCaptcha
プライバシー - 条項

図 12-18 アカウント情報の入力

3. 入力後、CAPTCHA 認証を行い、「アカウントの作成」をクリックします。
4. アカウント作成後、登録したメールアドレスへ Nuclias (verify@nuclias.com) 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、Nuclias アカウントのアクティベーションを行ってください。

■ シングルサインオン設定

Nuclias アカウントのアクティベーション完了後、**システム > 設定**に移動し、「シングルサインオン」画面で次のパラメータを指定します。

項目	説明
シングルサインオンを有効化	シングルサインオンを有効化します。
Nuclias アカウント	Nuclias アカウントのユーザ名を入力します。
Nuclias パスワード	Nuclias アカウントのパスワードを入力します。

「保存」をクリックして設定を保存します。

■ Nuclias Connect ポータルへの接続

Nuclias アカウントの SSO 設定が完了すると、以下の Nuclias Connect ポータルに接続することができます。

<https://connect.nuclias.com/>

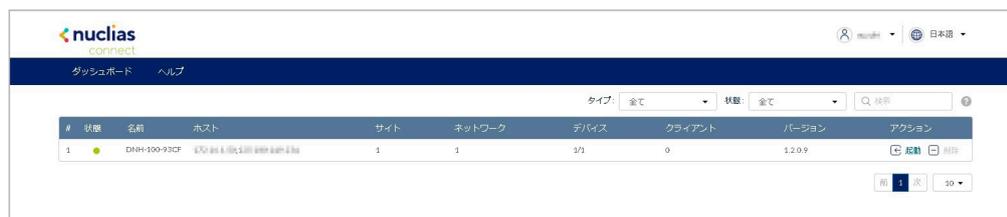


図 12-19 Nuclias Connect ポータル

Nuclias Connect ポータルでは、以下の項目が表示されます。

項目	説明
状態	Nuclias Connect ポータルと DNH-100 間の接続ステータスを表示します。
名前	Nuclias Connect の名前を表示します。
ホスト	デバイスの IP アドレスとパブリック IP アドレスの両方を表示します。
サイト	DNH-100 によって管理されるサイトの数を表示します。
ネットワーク	DNH-100 によって管理されるネットワークの数を表示します。
デバイス	DNH-100 によって管理されるデバイスの数を表示します。
クライアント	DNH-100 によって管理されるデバイスに接続されているクライアントの数を表示します。
バージョン	DNH-100 のソフトウェアバージョンを表示します。
アクション	「起動」をクリックして、DNH-100 のインターフェースを開きます。ファイアウォールやルータを介した通信の場合、IP マッピングが必要です。 「削除」を選択して、Nuclias Connect ポータルから DNH-100 のリンクを解除します。（「削除」は、デバイスがオフラインの場合にのみ使用できます。）

注意 NAT 環境の場合、ルータにおいて DNH-100 のパブリック IP アドレスに対するポートフォワーディングの設定を行う必要があります。

アラート

アラートタブでは、アラート/メール通知を行うイベントの種類を設定できます。

システム > 設定に移動し、「アラート」タブをクリックします。



図 12-20 設定 - アラートタブ

■ アラートの設定

Nuclias Connect 管理画面上で通知されるアラートを設定するには、以下の設定を行います。

1. アラートを生成するイベントの種類について、「アラート」のチェックボックスにチェックを入れます。
2. 「保存」をクリックして設定を保存します。

■ 生成されたアラートの確認

生成されたアラートは、ログ > アラートに移動して確認できます。

■ 電子メールアラートの設定

電子メールでアラートを受信するには、以下の設定を行います。

1. アラートを生成するイベントの種類について、「メールアドレス」のチェックボックスにチェックを入れます。
2. 「保存」をクリックして設定を保存します。
3. システム > ユーザ管理に移動し、ユーザの編集画面で「メールアラートを受信」を有効化して、ユーザが Nuclias Connect から電子メールアラートを受信できるようにします。

補足

「ブロックされたポート」項目はスイッチ製品でサポートされる機能です。(未サポート)

FOTA

FOTA（Firmware Over-The-Air）機能を使用すると、ユーザは最新のファームウェアに無線を介してアップグレードできます。

システム > 設定に移動し、「FOTA」タブをクリックします。



図 12-21 設定 - FOTA タブ

注意 日本では未サポートとなりますので、本機能は有効化せずご利用ください。サポート対象となるには、弊社 HP からファームウェアをダウンロードしてください。

リソース

リソース画面では、Nuclias Connect のインストール手順や各設定画面について、オンラインドキュメントを参照することができます。

システム > リソースに移動して以下の画面を表示します。



図 12-22 リソース

Nuclias Connect について

「Nuclias Connect について」画面には、DNH-100 のシステム情報と、サポートされる製品一覧が表示されます。

システム > Nuclias Connect についてに移動します。

「システムインフォメーション」タブでは、DNH-100 のシステム情報を確認することができます。

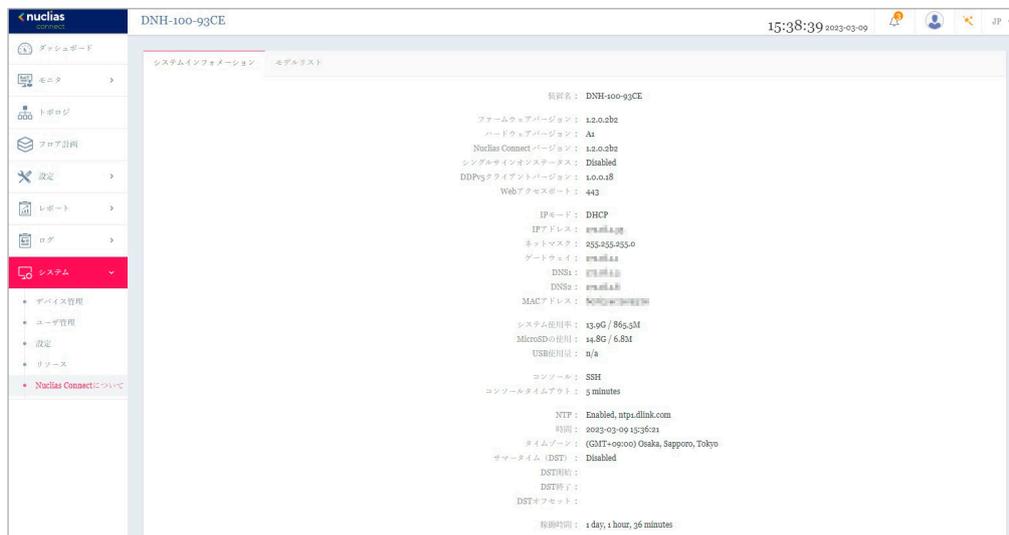


図 12-23 Nuclias Connect について - システムインフォメーションタブ

「モデルリスト」タブには、サポートされるアクセスポイントのリストが表示されます。

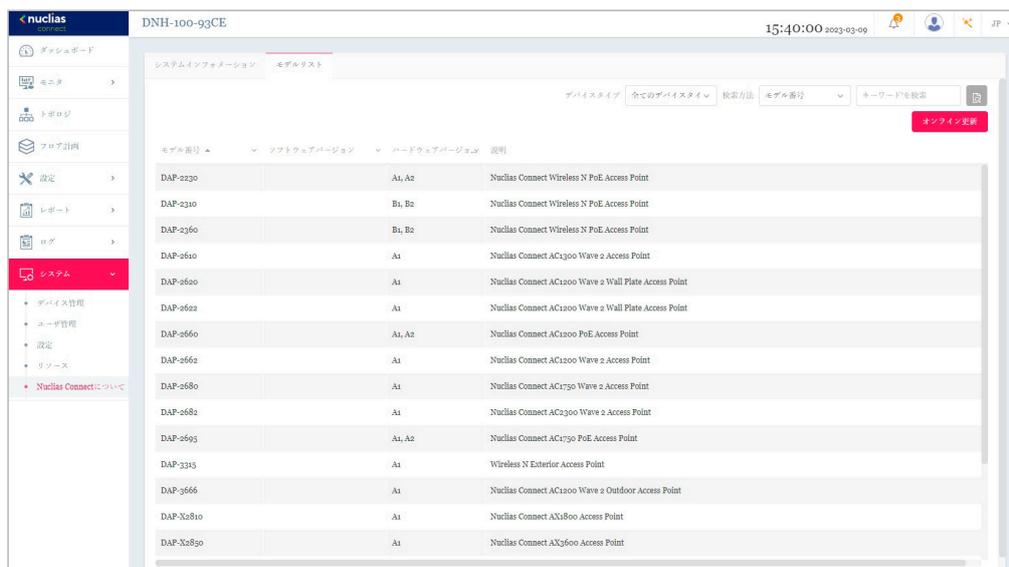


図 12-24 Nuclias Connect について - モデルリストタブ

「オンライン更新」をクリックすると、デバイスのリストを更新できます。新しくデバイスのモデルがサポートされた場合は、リストが更新されます。

注意

現在、日本でサポートされる製品は DAP-X2850、DAP-X2810、DAP-2610、DAP-2680、DAP-3666 のみです。(「Nuclias Connect 対応機器 (p.10)」を参照)

【付録A】機能別サポート製品/バージョンについて

本製品の一部の機能（下記項目）は、管理する製品やバージョンによりサポート可否が異なります。各機能のサポート可否については以下の表を参照してください。

項目	サポートされる製品/バージョン	
	スタンドアロンモード	DNH-100 管理モード
プロファイル設定 - アクセスポイント - SSID - セキュリティ		
高速ローミング (802.11 k/r)	<ul style="list-style-type: none"> DAP-3666 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
Enhanced Open	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上) 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
WPA3	<ul style="list-style-type: none"> DAP-X2850 DAP-3666 DAP-2610 (v2.06B06r097 以上) DAP-X2810 (v1.20r032 以上) 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
ネットワークアクセス保護	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 DAP-2680 DAP-2610 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 DAP-3666 DAP-2680 DAP-2610
プロファイル設定 - アクセスポイント - SSID - ユーザ認証		
外部キャプティブポータル認証 MAC アドレス認証 ソーシャルログイン認証	—	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
クリックスルー認証	<ul style="list-style-type: none"> DAP-X2850 DAP-3666 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
ウォールガーデン	<ul style="list-style-type: none"> DAP-2610 (v2.06B06r097 以上) 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
同時ログイン	—	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
セッションタイムアウト	—	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
リモート RADIUS 認証 - NAS ID	<ul style="list-style-type: none"> DAP-2610 (v2.06B06r097 以上) 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
リモート RADIUS 認証 - アカウンティングサーバ設定	<ul style="list-style-type: none"> DAP-X2850 DAP-2610 (v2.06B06r097 以上) 	<ul style="list-style-type: none"> DAP-X2850 DAP-X2810 (v1.20r032 以上) DAP-3666 DAP-2610 (v2.06B06r097 以上)
プロファイル設定 - アクセスポイント - SSID - Hotspot2.0		
Hotspot2.0	<ul style="list-style-type: none"> DAP-3666 	<ul style="list-style-type: none"> DAP-3666
パフォーマンス設定		
STP (スパンニングツリー) ※1	<ul style="list-style-type: none"> DAP-X2850 DAP-3666 	<ul style="list-style-type: none"> DAP-X2850 DAP-3666

【付録A】機能別サポート製品/バージョンについて

項目	サポートされる製品/バージョン	
WLAN パーティション		
リンクインテグリティ	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 • DAP-2680 • DAP-2610 	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 (v1.20r032 以上) • DAP-2680 (v2.00B08r051 以上) • DAP-2610 (v2.01B05r073 以上)
ワイヤレスリソース		
エアタイムフェアネス	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 (v1.20r032 以上) • DAP-3666 • DAP-2680 • DAP-2610 (v2.06B06r097 以上) 	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 (v1.20r032 以上) • DAP-3666 • DAP-2680 (v2.00B08r051 以上) • DAP-2610 (v2.06B06r097 以上)
隣接 AP	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 • DAP-3666 • DAP-2680 • DAP-2610 	<ul style="list-style-type: none"> • DAP-X2850 • DAP-X2810 (v1.20r032 以上) • DAP-3666 • DAP-2610 (v2.06B06r097 以上)

※ 1 DAP-X2810 の STP (スパンニングツリー) は、v1.20r032 以降でサポートされ、初期値で有効 (設定変更不可) となります。

※ Nuclias Connect 対応製品のみ掲載しています。

【付録 B】 Nuclias Connect アプリのセットアップ

Nuclias Connect アプリを利用することで、スマートデバイス経由でアクセスすることにより、遠隔地から簡単にサイトやネットワークを管理することができます。

このセクションでは、接続されたアクセスポイントを管理するために必要なネットワークプロファイルを Nuclias サーバからエクスポートする方法について説明します。また、Nuclias Connect アプリの機能についても説明します。

ネットワークプロファイルのエクスポート

新しいアクセスポイントを Nuclias Connect に追加するには、まず必要なネットワークプロファイルを Nuclias からエクスポートする必要があります。ネットワークプロファイルには、コントローラの認証キーと IP アドレスが含まれます。

設定 > プロファイルを作成の順にクリックし、「ネットワークプロファイルをエクスポート」(📄) アイコンをクリックして、ネットワークプロファイルをコンピュータにエクスポートします。

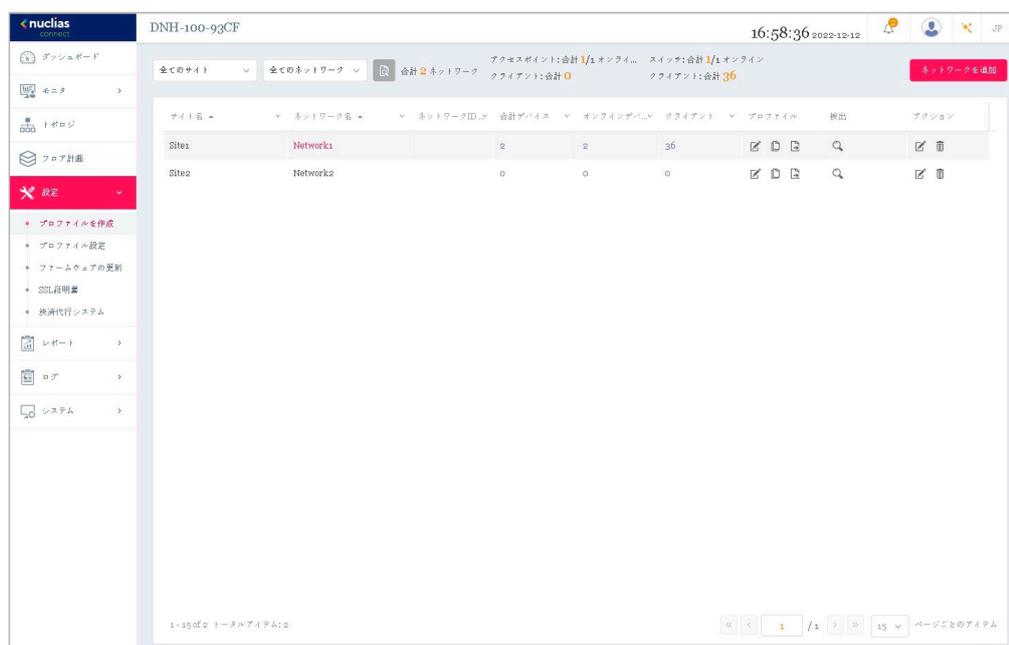


図 13-25 プロファイルを作成

アクセスポイントがパブリックネットワーク上にあり、リモートで Nuclias Connect にアクセスする場合は、Nuclias Connect がパブリック IP アドレスまたはドメイン名を使用していることを確認する必要があります。Nuclias Connect の IP アドレスを確認するには、システム > 設定 > 接続に移動し、「デバイスアクセスアドレス」フィールドを確認します。



図 13-26 設定 - 接続タブ

【付録B】Nuclias Connectアプリのセットアップ

Nuclias Connect アプリケーションを使用した AP の検出と設定

Nuclias Connect アプリは、スマートフォンやタブレットから単一または複数のサイトやネットワークを簡単に管理できるワイヤレスアクセス管理ツールです。Nuclias Connect アプリケーションを使用すると、スタンドアロンのアクセスポイントを Nuclias Connect にすばやくデプロイしたり、D-Link アクセスポイントを検索したり、個別のアクセスポイントを設定したりすることができます。

注意 ネットワークプロファイルをインポートする前に、Nuclias Connect コントローラ（サーバ）にアクセスできることを確認してください。

Nuclias Connect アプリは、iOS と Android の両方のスマートデバイスで使用できます。次の機能を使用できます。

- ・ クイックセットアップ：スタンドアロンのアクセスポイントを Nuclias Connect コントローラ（サーバ）にすばやく簡単にデプロイできます。
- ・ Nuclias Connect：Nuclias Connect を使用して、現行のサイトとネットワークを管理します。
- ・ スタンドアロンアクセスポイント：個々のアクセスポイントの設定を変更し、複数のアクセスポイントにデプロイする設定プロファイルを保存できます。

補足 本セクションにおけるアプリの画面表示のイメージは、端末や OS などにより異なる場合があります。

クイックセットアップ

「クイックセットアップ」では、アクセスポイントを Nuclias Connect の管理デバイスとして設定するクイックセットアップ手順を実行できます。

Nuclias Connect アプリを起動すると、以下の画面が表示されます。「クイックセットアップ」をタップして、セットアッププロセスを開始します。



図 13-27 Nuclias Connect アプリ (iOS)

次の手順を参照し、AP プロビジョニングプロファイルを選択してアクセスポイントにプッシュ送信します。

- ・ ステップ 1：プロビジョニングプロファイルの選択
- ・ ステップ 2：アクセスポイント検出範囲の定義
- ・ ステップ 3：アクセスポイントへのプロファイル適用

ステップ1：プロビジョニングプロファイルの選択

1. 「クイックセットアップ」をタップすると、「ステップ1」画面が表示されます。
2. 「プロビジョニングファイル」をタップして、使用可能なローカルプロファイルのリストを表示します。ローカルに保存されているプロファイルが存在しない場合は、リストをタップしてプロファイルのダウンロードすることができます。
3. Nuclias Connect コントローラへ接続しプロファイルをダウンロードするには、「プロファイルをダウンロード」を選択します。



図 13-28 ステップ1 - プロファイルのダウンロード

4. **+**「+」アイコンをクリックし、Nuclias Connect サーバへの接続情報を入力してログインします。接続に必要な入力項目については、[132 ページの「Nuclias Connect サーバへの接続」](#)を参照してください。
5. サイトとネットワークを選択し、「ダウンロード」をタップしてプロファイルをダウンロードします。
6. 「ダウンロードを続ける」または「戻る」をタップし、「ステップ1」の画面に戻ります。
7. プロビジョニングプロファイルが選択されている状態で「次へ」をタップします。



図 13-29 ステップ1 - プロビジョンプロファイルの選択

【付録B】Nuclias Connectアプリのセットアップ

■ ステップ2：アクセスポイント検出範囲の定義

L2/L3 ワイヤレスネットワークに接続されているスタンドアロンアクセスポイントを検出します。

1. L3 ネットワークでの検出を有効にするには、有効/無効オプションをタップして、L3 ネットワークでの検出をオンにします。
2. L3 ネットワークでの検出をオンにした場合は、「開始」「終了」フィールドに IP 範囲を入力します。追加ボタン (+) をタップして、新しい IP 範囲エントリを作成します。削除ボタン (-) をタップして、定義済みの範囲エントリを削除します。
3. 「次へ」をタップして検出を開始します。



図 13-30 アクセスポイント検出範囲の定義

■ ステップ3：アクセスポイントへのプロファイル適用

1. ネットワーク範囲のスキャンが終了すると、「ステップ3」画面に検出されたアクセスポイントが一覧表示されます。
2. アクセスポイントの横にあるラジオボタンをタップして選択します。
3. 「プロビジョニングファイルをプッシュ」をタップして続行します。ステップ1で選択したプロビジョニングファイルが、選択したアクセスポイントにプッシュされます。



図 13-31 アクセスポイントの選択

4. アクセスポイントのログイン画面が表示されます。選択したアクセスポイントのログインユーザ名とパスワードを入力します。



図 13-32 アクセスポイントへのログイン

5. 「選択したすべてのアクセスポイントに適用」をタップして、ログインプロセスを続行します。
6. ステップ 3 画面に「プッシュ成功」のメッセージが表示されます。
7. 「完了」をタップしてプロセスを完了します。処理に失敗した場合は、「プロビジョニングファイルをプッシュ」をタップして、プッシュ機能を再試行します。



図 13-33 プロファイルの適用

【付録B】Nuclias Connectアプリのセットアップ

Nuclias Connect サーバへの接続

「Nuclias Connect」機能では、サイトとネットワークを管理することができます。

1. 「Nuclias Connect」をタップします。



図 13-34 Nuclias Connect アプリ - トップ画面

2. 「Nuclias Connect へようこそ」画面が表示されます。ペアリング済みの Nuclias Connect サーバが存在しない場合は、新しい Nuclias Connect ペアリングを作成する必要があります。追加 (+) ボタンをタップして、処理を開始します。



図 13-35 Nuclias Connect へようこそ画面

3. 接続する Nuclias Connect サーバの情報を入力しします。



図 13-36 新規サーバへのログイン画面

以下の項目が表示されます。

項目	説明
	Nuclias Connect URL/IP アドレスを入力する
Https://	アプリとペアリングする Nuclias Connect サーバのセキュアな URL/IP アドレスを入力します。
	この Nuclias Connect サーバの名前を作成する
Nuclias Connect サーバー名	ペアになる Nuclias Connect サーバを識別するための名前を入力します。
ユーザー名	Nuclias Connect サーバにアクセスする権限を持つユーザ名を入力します。
パスワード	Nuclias Connect サーバにアクセスする権限を持つユーザのパスワードを入力します。

- 「ログイン」をタップして、ログイン処理を開始します。
- ログインが成功すると、Nuclias Connect のダッシュボード画面が表示されます。ダッシュボードには、現在定義されているサイト/ネットワーク、アクセスポイントおよびクライアントの数と、統計グラフが表示されます。



図 13-37 ダッシュボード

ペアリング済みサーバは、「Nuclias Connect」>「Nuclias Connect へようこそ」画面に一覧表示されます。アプリを使用して、プロフィールをローカルデバイスにダウンロードし、サポートされているアクセスポイントにプッシュすることができます。



図 13-38 Nuclias Connect サーバのリスト

スタンドアロンアクセスポイントの検出と設定

■ アクセスポイントの検出

アクセスポイントの検出機能を使用すると、L2/L3 ワイヤレスネットワーク内のアクセスポイントを検出することができます。スタンドアロンのアクセスポイントを対象に、個別の設定および設定プロファイルの保存（Nuclias Connect 管理とは異なる）を行います。

1. 「アクセスポイントの検出」をタップします。



図 13-39 Nuclias Connect アプリ - トップ画面

2. ページの下部にある「アクセスポイントプロファイル設定」をタップして、ローカルプロファイルを追加または削除します。
3. ページの下部にある「アクセスポイントの検出」をタップして、アクセスポイントの検出を行います。
4. L3 ネットワークでの検出をオンにした場合は、「開始」「終了」フィールドに IP 範囲を入力します。追加ボタン (+) をタップして、新しい IP 範囲エントリを作成します。削除ボタン (-) をタップして、定義済みの範囲エントリを削除します。
5. 「検出」をタップして検出を開始します。



図 13-40 アクセスポイントの検出範囲

6. ネットワーク範囲のスキャンが終了すると、検出されたアクセスポイントが一覧表示されます。

7. アクセスポイントの横にあるラジオボタンをタップして選択します。
8. 「設定をプッシュ」をタップします。

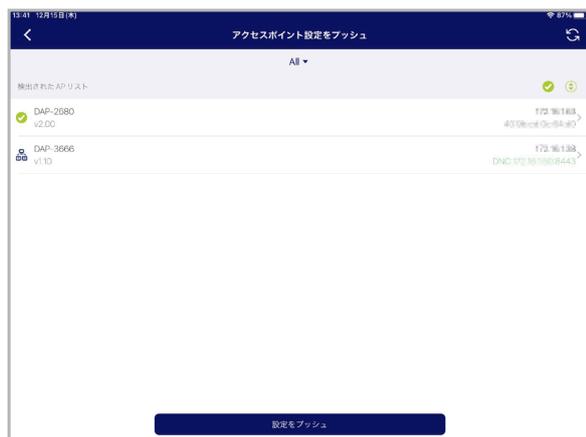


図 13-41 プロファイルの配信

9. アクセスポイントのログイン画面が表示されます。選択したアクセスポイントのログインユーザ名とパスワードを入力します。
10. 「選択したすべてのアクセスポイントに適用」をタップして続行します。

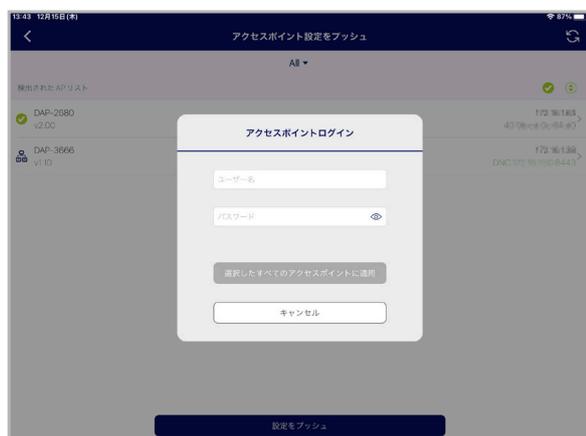


図 13-42 アクセスポイントへのログイン

11. 「アクセスポイント設定リスト」から、定義済みのプロファイルを選択し、「プッシュ」をタップします。
12. 「プッシュ成功」のメッセージが表示されます。
13. アクセスポイントにログインすると、アクセスポイントのインタフェースメニューが表示されます。「IP 情報」「ワイヤレス」「クライアント」タブが上部に表示されます。

「IP 情報」タブには以下の項目が表示されます。

項目	説明
モデル名	アクセスポイントのモデル名が表示されます。
MAC	アクセスポイントの MAC アドレスが表示されます。
DHCP モード	DHCP モードのステータス（有効/無効）が表示されます。
IP アドレス	アクセスポイントの IP アドレスが表示されます。
サブネットマスク	アクセスポイントのサブネットマスクが表示されます。
デフォルトゲートウェイ	アクセスポイントのデフォルトゲートウェイが表示されます。
DNS	アクセスポイントの DNS が表示されます。

「キャンセル」をタップすると、「アクセスポイント設定をプッシュ」画面に戻ります。

【付録B】Nuclias Connectアプリのセットアップ

「Wireless」タブには以下の項目が表示されます。メニューが次のように表示されます。

項目	説明
DAP-xxxx	アクセスポイントの IP アドレスと MAC アドレスが表示されます。
SSID 設定	
2.4G/5G	項目をタップして、SSID 設定を表示します。 上部の「SSID-#」をタップして各 SSID の設定を確認することができます。(# の文字は、SSID の識別番号) <ul style="list-style-type: none"> 「SSID を有効化」: SSID のステータス (有効 / 無効) が表示されます。 「SSID 名」: SSID 名が表示されます。 「セキュリティ」: SSID で使用されるセキュリティプロトコルが表示されます。
ワイヤレス情報	
周波数帯	無線帯域が表示されます。
周波数帯 2.4G/5G モード	2.4G/5G の無線モードが表示されます。
国コード	アクセスポイントに割り当てられている国名が表示されます。
設定をコピーして保存	
設定を適用	検出された別のアクセスポイントを選択し、この設定をプッシュします。
設定を保存	プロファイルに名前を付けてローカルの設定プロファイルリストに保存します。

「キャンセル」をタップすると、「アクセスポイント設定をプッシュ」画面に戻ります。

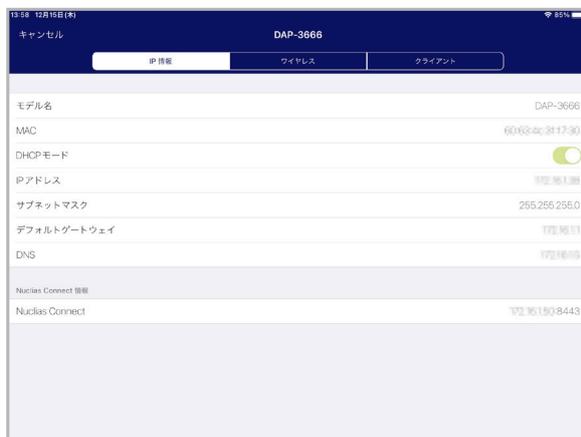


図 13-43 IP 情報の設定

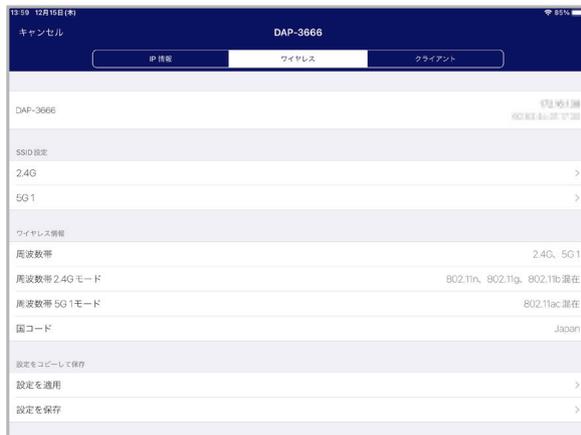


図 13-44 ワイヤレス設定

ネットワークプロファイルの削除

ネットワークプロファイルを削除するには、以下の手順を実行します。不要なプロファイルを削除することができます。

1. 左上のメニューをタップします。



図 13-45 Nuclias Connect アプリ - トップ画面

2. 「AP プロビジョニングプロファイル」を選択します。

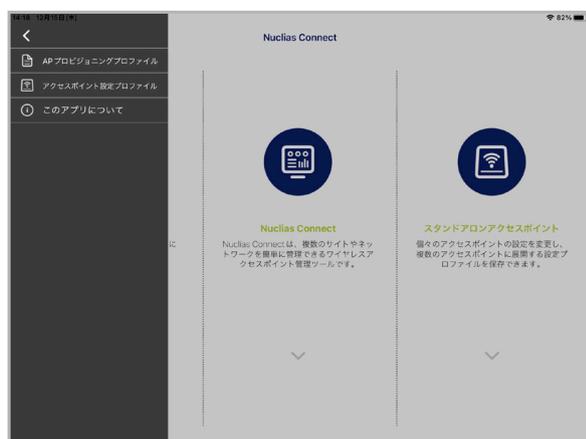


図 13-46 Nuclias Connect アプリ - メニュー項目

3. 右上の削除ボタン (⊖) をタップします。
4. 対象プロファイルの横の削除ボタン (⊖) をタップ選択し、「削除」をタップします。



図 13-47 Nuclias Connect アプリ - プロファイル選択