# **D-Link DNH-100** Nuclias Connect Hub





## 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 <u>全</u> 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「 <b>指示」</b> の内容です。
	危険
<ul> <li>◇ 分解・改造をしない</li> <li>☆ 止 火災、やけど、けが、感電などの原因となります。</li> <li>◇ ぬれた手でさわらない</li> </ul>	☆ 止 法気、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 いい、かけど、けば、感費、独院の原用となります。
☆ 止 感電の原因となります。	◇ 内部に金属物や燃えやすいものを入れない
○ 水をかけたり、ぬらしたりしない 素 止 内部に水が入ると、火災、感電、故障の原因となります。	☆ 止 火災、感電、故障の原因となります。
水などの液体(飲料水、汗、海水、ペットの尿など) でぬれた状態で触ったり、電源を入れたりしない 火災、やけど、けが、感電、故障の原因となります。	● 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。     ●
各種端子やスロットに水などの液体(飲料水、汗、海ガ ペットの尿など)をいれない。万が一、入ってしまった場合に 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。	K、 素 止 火災、やけど、けが、感電、故障の原因となります。
	警告
落としたり、重いものを乗せたり、強いショックを 与えたり、圧力をかけたりしない 故障の原因となります。	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。
発煙、焦げ臭い匂いの発生などの異常状態のまま 使用しない 感電、火災の原因になります。 使用たいな、 「類なせいス」「「類なせいス」「「「「」」」」であった。」」	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。
使用を止めて、ケーノルノコート類を扱いて、陸が出なくなって から販売店に修理をご依頼ください。	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。
<u>※</u> 止火災、感電、または故障の原因となります。 <u>、</u> 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	◆ 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。
<ul> <li>▲ 原因となります。</li> <li>● 設置、移動のときは電源プラグを抜く</li> <li>● 設置、移動のときは電源プラグを抜く</li> </ul>	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。
へ次、窓电、または00月のとなります。      雷鳴が聞こえたら、ケーブル/コード類にはさわらない     葉止 感電の原因となります。	無線製品をご使用の場合、医用電気機器などを 装着している場合は、医用電気機器メーカーもしくは、 販売業者に、電波による影響について確認の上使用する 医療需要機器に更影響を取ぼすもとれなきします。
ケーブル / コード類や端子を破損させない     無理なねじり、引っ張り、加工、重いものの下敷きなどは、     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。	こ 「「「「「」」」」     「「」 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     電子機器が認作動するなど、要影響を及ぼすおそれがあります。
本製品付属のACアダプタもしくは電源ケーブルを 指定のコンセントに正しく接続して使用する 火災、感電、または故障の原因となります。	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。
各光源をのぞかない ※ 止 とD 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	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。
会種端子やスロットに導電性異物(金属片、鉛筆の芯など)を 接触させたり、ほこりが内部に入ったりしないようにする 火災、やけど、けが、感電または故障の原因となります。	スレイントに 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。     マロン アン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン・マン
使用中に布団で覆ったり、包んだりしない ☆ 止 火災、やけどまたは故障の原因となります。	<ul> <li>AC アタフ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</li> <li>発火、発熱、感電または故障の原因となります。</li> </ul>



#### 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、ご使用の前にご確認ください。 製品保証、保守サービス、テクニカルサポートご利用について、詳しくは弊社ホームページのサポート情報をご確認ください。 https://www.dlink-jp.com/support

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。

<u>.</u>	目次	
安	そ全にお使いいただくために	2
2	。使用上の注意	4
静	<b>浄電気障害を防止するために</b>	4
電		
本	Σマニュアルの対象者	
衣制	<記規則についく	۵ ع
第11	草本製品のご利用にあたって	9
バ	<b>パッケージの内容</b>	9
シュ	/ステム要件	
サ	アភートする機能 Juglias Connact 対応機器	
	Netras connect 対応機器	
	背面パネル	
LE	ED 表示	
第2:	章 機器の設置	12
Ż	なットワーク接続前の進備	12
ጥ 19	9インチラックへの取り付け	
	ブラケットの取り付け	
	19 インチラックにスイッチを取り付ける	
第3:	章 機器の接続	14
-		14
-	コントロー ノハの夜祝	
	コンソール経由で接続する(簡易設定のみ)	
笋 4	音 Nuclias Connet の管理インタフェーフ	16
<u>, r ck</u>		10
N	luclias Connect への接続	
	Nuclias Connect 設定ウィザード (初回ログイン時)	
	Nuclias Connect 設定ウィザード	
ב	Lーザプロファイル	
	個人情報	
奋	セキュリティ	
E		
<u>第5</u>	章 タッシュボード	24
第6	章 モニタ	25
7	マクセスポイント	25
, ワ	ッ こへが ( ) イ	
	接続しているクライアント	
	ブロックされたクライアント	
第7	章 設定	28
	プロファイルの作成	28
	ネットワークの追加	
プ	プロファイル設定	
	SSID	
	VLAN	
	VLAN リスト	
	ッー Γ ソ ∧ Γ VI ΔN を追加 / 編集	
	PVID 設定	
	帯域幅の最適化	
	RF 最適化	
	スケジュール	
	デバイス設定	
	ハノォーマンス設定	
	WLAN ハーティンヨン	

"Lpi

rБ

cŀ

ファームウェアアップグレード	53
SSL 証明書 ※サポート予定	54
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。	
8章 レポート	57
ピークラットロークマクニッピーン	57

<u>. q.ľ</u>

Ξŋ

SSL 証明書 ※サポート予定	
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。	55
第8章 レポート	57
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	59
最もアクティブな AP	
第9章 ログ	61
SNMP トラップ	61
シスログ	62
システムイベントログ	
デバイスログ	
<u>第 10 章 システム管理</u>	65
デバイス管理	65
ユーザ管理	
ユーザステータス	66
ユーザ権限	67
設定	
一般	
接続	69
SMTP	70
バックアップ	71
ファームウェアアップグレード	
システム設定	74
シングルサインオン(SSO)	75
Nuclias Connect について	
【付録】Nuclias Connect アプリのセットアップ	79

ネットワークプロファイルのエクスポート	79
Nuclias Connect アプリケーションを使用した AP の検出と設定	80
ネットワークプロファイルの削除	90

Ъp

\_\_\_\_\_\_

## 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
Гј	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
- ・ 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®、Macintosh®、Linux
- イーサネット接続

#### ブラウザ要件

• Microsoft Edge、Safari 7、Firefox 28、Google Chrome 33 以上

## 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
- SNMPv1/v2c/v3
- ・ 日本語 GUI
- ・ 最大 100 台までの AP 管理
- サーバ・クライアント型
- チャネル・出力自動調整
- ・ Syslog/Trap サーバ<sup>\*\* 1</sup>
- ・ 外部 syslog サーバ<sup>\*\*2</sup>
- ・ 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/Trap 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-2610	DAP-2610/A1	R2.01B05r073
DAP-2680	DAP-2680/A1	R2.00B08r051

## 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。

袖足 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ない可能性があります。「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
-		点灯	緑	電源が供給され正常に動作しています。スタンド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。
1	Power	点灯	橙	Nuclias サーバに接続し、シングルサインオンが利用可能です。
		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		点灯	橙	10/100Mbps でリンクが確立しています。
	Link/Act/Speed (10/100Mbps)	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。
		点灯	緑	1000Mbps でリンクが確立しています。
3 Link/Act/	Link/Act/Speed (1000Mbps)	点滅	緑	1000Mbps でデータを送受信しています。
(1000111005)		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充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ないで製品を設置すると、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。



#### 機器の接続 第3章

- 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。



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。
- 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。 2.

#### 管理画面への接続

- 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。 1.
- 2. 管理インタフェースにログインします。
  - ユーザ名初期値: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 Connet 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」
- 「ユーザプロファイル」

## 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。

< nuclias connect	
Login to your account	
Your E-mail / User Name	
Your password	Ŷ
Please input the captch 1 5 5 7	
Login	
© 2019 D-Link Corporation English. V	

図 4-1 Nuclias Connect ログイン画面

2. 各フィールドに、ユーザ名とパスワードを入力します。また、画面に表示されている Captcha コードを入力します。

## 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。
- ・「Remember me」オプションを選択して、パスワード情報を記憶することができます。
- ・「Forgot password?」オプションでは、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。

	Your password	
	Please input the captch 1557	
	Achienter ne	ringle burnings
	© 2019 D-Link Corporation En	gish v
☑ 4-2	アカウント信却入	カオプシュン

3. Web ブラウザが開き、サーバに正常に接続すると、パスワード変更ダイアログが表示されます。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5~16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。

You i login	need to change your password after the first
Stro	ng password consisting of 5 - 16 characters is required. Combine ercase letters, lowercase, letters, numbers and symbols. Do not include amon words or names.
þ	d password
n	ew password
	onfirm password
	Modify

図 4-3 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。「Modify」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。

LAN設定				
IPアドレスの取得	スタティックIPアドレス(羊動) ッ			
IPアドレス*	192.168.0.200	サブネットマスク	255.255.255.0	
ゲートウェイ				
プライマリDNS		セカングリDNS		
ブライマリDNS	<ul> <li>デバイスアクセスアドレスの同利</li> </ul>	セカンダリDNS 明		
ブライマリDNS 日付と時間	✓ デバイスアクセスアドレスの同員	セカングリDNS 明		
ブライマリDNS 日付と時間 タイムブーン*	<ul> <li>デバイスアクセスアドレスの同)</li> <li>(GMT) Greenwich Mean Time : Dubl</li> </ul>	セカンダリDNS 例 in,Edinburgh,Lisbon,	v	
ブライマリDNS 日村と時間 タイムゾーン*	<ul> <li>デバイスアクセスアドレスの同時</li> <li>(GMT) Greenwich Mean Time : Dubl</li> <li>NTP</li> </ul>	モカングリDNS 明 in,Edinburgh,Lisbon,	~	
ブライマリDNS 日付と時間 タイムゾーン* NTPサーバ1	<ul> <li>デバイスアクセスアドレスの同じ</li> <li>(GMT) Greenwich Mean Time : Dubl</li> <li>NTP</li> <li>ntpi.dlink.com</li> </ul>	モカングリDNS 列	×	
ブライマリDNS 日付と時間 タイムブーン* NTPサーバ1 NTPサーバ2	<ul> <li>デバイスアクセスアドレスの(前)</li> <li>(GMT) Greenwich Mean Time : Dubl</li> <li>✓ NTP</li> <li>ntp1.dlink.com</li> <li>IPアドレス/ドメイン会</li> </ul>	±カングリDNS 9	×	

図 4-4 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。

TLU ADY VC				
IPアドレスの取得	スタティックIPプドレス(手動)、			
IPアドレス*	192.168.0.200	サブネットマスク	255.255.255.0	
ゲートウェイ				
プライマリDNS		セカングリDNS	<u></u>	
	デバイスアクセスアドレスの	同期		
日付と時間 タイムゾーン*	<ul> <li>デバイスアクセスアドレスの</li> <li>(GMT) Greenwich Mean Time : D</li> <li>NTP</li> </ul>	同期 ublin,Edinburgh,Lisbon,	v	
日付と時間 タイムゾーン* NTPサーバ1	<ul> <li>✓ デバイスデクセステドレスの</li> <li>(GMT) Greenwich Mean Time : D</li> <li>✓ NTP</li> <li>ntp1.dlink.com</li> </ul>	同期 ublin, Edinburgh, Lisbon,	~	
日付と時間 タイムゾーン* NTPサーバ 1 NTPサーバ 2	<ul> <li>デバイスデクセステドレスの</li> <li>(GMT) Greenwich Mean Time: D</li> <li>NTP</li> <li>ntp1.dlink.com</li> <li>IPアドレス/ドメイン名</li> </ul>	同朔 ublin, Edinburgh, Lisbon,	<ul> <li></li> </ul>	

図 4-5 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	
	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)」「ダイナミック 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	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
レスの同期	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。

## 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。

1 📶 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。

デバイスアクセスボート 8443	114011201100	192.168.0.200	~	
Mab 7 A + Z + - h	デバイスアクセスポート	8443		
443	Webプクセスポート	443		
国 Japan ~	国	Japan	$\sim$	

図 4-6 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。

説明
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。ファイアウォールまたはルータの後方にあるインスタンスには IP マッピングが必
要です。
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。ファイアウォールまたはルータの後方
にあるリモート AP 管理の場合は、受信ポートを開く必要があります。
<ul> <li>初期値:8443</li> </ul>
インストール時に定義された Web アクセスポート。値は事前定義されています。
国を選択します。

「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。

🗙 ネットワークを追加		×
サイト	newSite v	
ネットワーク名	Networkı	
		戻る 次~ 終了

図 4-7 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。

3. 「ネットワーク設定」画面が表示されます。ワイヤレス設定とデバイス設定を入力して、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「×」ボタンをクリックします。

Ҟ ネットワーク設定		×
ワイヤレス設定		
SSID名	dlink	
セキュリティ	WPA-自動-パーソナル 。	
SSIDバスワード*	\$	
	□ ゲストSSIDを追加(オブション)	
ゲストSSID名		
デバイス設定		
国	Japan 🗸	
タイムブーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸 🗸	
ユーザ名	admin	
新しいバスワード*	Ś	
		戻 8 次~

図 4-8 ネットワークの設定

**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。

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。 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。

V1+	2			
レイヤ:	3 (IP)			
IP	~	192.168.1.150	- 192.168.1.200	
つ選択	~		- +	

図 4-9 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一覧表示します。デバイスが検出さ れた場合は、そのデバイスを選択して「適用」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。「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。

IX AL HIE	能 管理					
	ステート 、	IPアドレス ~	MACアドレス ~	モデルタイプ:	NMS URL ~	ネットワーク
	スタンドアロ	192.168.0.50	40:9b:cd:0c:64:d0	DAP-2680	192.168.0.60:8443	

図 4-10 AP を検出

注意 異なるセグメントの「管理」ステータスの AP については再検出されません。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。

## ユーザプロファイル

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、「ユーザプロファイル」を選択して、以下の画面を表示します。

$\bigcirc$	個人情報 セキュリ	₹ 1	
	情報		
	ユーザ名*	admin	
admin	設置場所		
ルート管理者	電話番号		
▲ メールアドレス情報なし			
	說明		
			更新

図 4-11 ユーザプロファイル - 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。

$\bigcirc$	個人情報 セキュリティ	
	パスワードを変更	
	バスワード*	
admin	新しいバスワード*	
ルート管理者	パスワード確認*	
▲ メールアドレス情報なし		保存
	メールアドレスを変更	
	新しいメールアドレス *	
		保存
		終了

図 4-12 ユーザプロファイル - 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、接続されているすべてのアクセスポイントとワイヤレ スクライアントの情報の概要が表示されます。



図 5-1 ダッシュボード

#### 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合計数が表示されます。
アクセスポイント	利用可能なアクセスポイントとオンラインアクセスポイントの合計数が表示されます。
クライアント	ネットワークに接続されているワイヤレスクライアントの合計数が表示されます。
直近1時間の情報	クライアント数、トラフィック使用量、ダウンリンク / アップリンクトラフィック使用量、および SSID ごとのトラフィッ
	ク使用量の履歴情報を表示します。
チャネル利用率	2.4GHz 帯域幅と 5GHz 帯域幅の両方の使用率を表示します。
直近のイベント	すべてのサイトまたは選択したサイトの最新イベントの省略されたログを表示します。

## 第6章 モニタ

- 「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

左側のパネルからモニタ>アクセスポイントをクリックすると、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が表示され ます。

この画面では、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アクセスポイントのレポートを表示できます。 また、「サイト」、「ネットワーク」などの検索条件を使用して、要件に沿ったレポートを生成できます。

次の画面は、一般的なレポートを示しています。このレポートは、最初のドロップダウンメニューから特定のサイトを選択し、2番目のドロップダ ウンメニューでネットワークを選択することでデバイスを絞り込むことができます。

sonnect	dnh-100	) 🔀 JP
<ul><li>(法) ダッシュボード</li></ul>		
	全てのサイト v 全てのネットワーク v R 合計:1/1アクセスポイント	
• アクセスポイント	会計 ダウンロード: o Byte 合計 アップロード: o Byte	
• ワイヤレスクライアント	МВ. ● ダウンロード(МВ) ● アップ1	n− F (MB)
🗙 設定 >	1	
■ ¤ // >>		
G >274 →	ע לאינה	AR A
	アクセスポイント	
	教育方法 ローカルほアドレス シーワードを教育	
	No ステータエ アクション ローカルPアドレード MACアドレス * モデルタイプ エ ネットワーク * クライアエ 24Gチャネル * 5Gチャネル	~
	1 🕐 🗇 🕞 💬 192.168.0.50 🗰 DAP-2680 Network1 0 11 104	201'

図 6-1 モニタ - アクセスポイント

表の各項目の説明は下記の通りです。

項目	前月
使用量	指定されたサイトおよびネットワークのダウンロード/アップロードトラフィック使用量を表示します。
アクセスポイント	検出されたすべてのワイヤレスクライアントの一覧を表示します。

「検索方法」のドロップダウンメニューで、属性(「ローカル IP アドレス」、「ローカル IPv6 アドレス」、「NAT IP アドレス」、「MAC アドレス」、「モデ ルタイプ」、「ファームウェアバージョン」など)を選択して検索オブジェクトを指定するか、「検索」フィールドに検索対象のデバイスに関連するキー ワードを入力します。



注意 モニタ > アクセスポイント画面において、ファームウェアの詳細バージョンで検索した場合、表示されているバージョンに含まれない文 字列で検索できてしまう問題が存在します。

## 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>ワイヤレスクライアントをクリックすると、「接続しているクライアント」画面が表示されます。この画面では、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できます。

「サイト」、「ネットワーク」、「クライアント」などの検索条件を使用して、要件に沿ったレポートを生成できます。

次の画面は、一般的なレポートを示しています。このレポートは、最初のドロップダウンメニューから特定のサイトを選択し、ネットワークとクラ イアントを選択することでデバイスを絞り込むことができます。

<pre>shuck is a second second</pre>	dnh-100 🕼 Ҟ JP 🗸
(j) # 7 % = # - F	複枝しているクライアント ブロックされたクライアント
₩ <= 9 ×	合計 0 仮読しているクライアント
• アクセスポイント	全てのサイト ◇ 全てのネットワーク ◇ 全てのクライアント ◇ 根索方法 MACプドレス ◇ キーワードを根本 段
• ワイヤレスクライナント	
🗙 設定 🔹 👌	INOTE A A THE LEAVER A REMEATING A REPORT OF A A A A A A A A A A A A A A A A A A
「「レポート >	
50 xx74 >	
	クライアントがまだ接続されていませ ん。
	1-20±0 K-ダルアイテム。0 ページことのアイテム

図 6-2 モニタ-ワイヤレスクライアント(接続されたクライアント)

この画面には、接続されているワイヤレスクライアントによって生成されたレポートが表示されます。このレポートは、「サイト」「ネットワーク」「クライアント」を選択した後、「検索方法」で「MAC アドレス」または「IP アドレス」を選択し、表示されたテキストボックスに「キーワード」を入力することでデバイスを絞り込むことができます。

「検索」フィールドに検索対象のデバイスに関連するキーワードを入力し、 <br/>
<br/>
<br/>
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

このレポートには、このアプリケーションによって管理されるアクセスポイントに接続されているワイヤレスクライアント接続の一覧が表示されま す。レポートには「ネットワーク」、「IP アドレス」、「IPv6 アドレス」、「MAC アドレス」、「認証タイプ」、「OS(キャプティブポータルクライアント でのみ使用可能)」、「アップロード」、「ダウンロード」、「チャネル」、「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」などの情報が、ワイヤレスクライアントごとに表示されます。

注意 クライアントの最終更新情報が1日前となる /IP フィールドが 0.0.0.0 と表示される問題があります。

ワイヤレス機能を無効化した場合、モニタ>クライアント画面のクライアント情報は更新されません。

#### 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**をクリックすると、「接続しているクライアント」画面が表示されます。「ブロックされたクライ アント」タブをクリックします。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 「サイト」、「ネットワーク」の検索条件を使用して、要件に沿ったレポートを生成できます。

次の画面は、一般的なレポートを示しています。このレポートは、最初のドロップダウンメニューから特定のサイトを選択し、ネットワークを選択 することでデバイスを絞り込むことができます。

< nuclias connect	dnh-100			) 🔀 ле ч
()) I v v = t = V	指接しているクライアント プロックされたクライアント			
	会計 0 ブロックされたクライアント	全てのサイト	◇ 全てのネットワーク	
<ul> <li>アクセスポイント</li> <li>ワイヤレスクライアント</li> </ul>	No. アクシュ ネットワーク × MACアドレス × ×	周波数号 Y SSID	- 「線証タイプ	~
🗙 RE >				
「「」 レポート >				
<u>ار م</u>				
50 × X74 >				
	ブロックされた j	クライアントは存在し させん。		
	1-20 of 0 トータルアイテム: 0		1 /1 > > 20 v	ごとのアイテム

図 6-3 モニタ - ワイヤレスクライアント(ブロックされたクライアント)

「検索」フィールドで、ドロップダウンメニューをクリックし、サイトを選択してから、ネットワークを選択します。 🔯 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

このレポートには、ブロックされたワイヤレスクライアント接続の一覧が表示されます。レポートには、「No.」、「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」の情報が表示されます。

## 第7章 設定

- 「プロファイルの作成」
- 「プロファイル設定」
- 「ファームウェアアップグレード」
- 「SSL 証明書 ※サポート予定」
- 「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

「プロファイルの作成」機能を使用すると、新しいサイトやネットワークを追加できます。

設定>プロファイルを作成をクリックすると、「Default」フレームに利用可能なすべてのサイトとネットワークが表示されます。

<nuclias< th=""><th>dnh-100</th><th></th><th></th><th></th><th></th><th></th><th></th><th>🚺 🔫 ле ч</th></nuclias<>	dnh-100							🚺 🔫 ле ч
ガッシュボード	全てのサイト 🗸 合計 📘	ネットワーク 合計 <mark>0/1</mark> オンライン AP	合計 <mark>0</mark> クライア :	< F				ネットワークを追加
₩ €=9 >	サイト名・	ネットワーク名 🔺 🔹 🗸	合計デバイス…>	オンラインデヾ	クライアントニン	プロファイル	検出	アクション
🗙 872 🔹 👻	site1	Network1	1	0	0	e o e	Q	2 1
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> <li>ファームウェアアップゲレード</li> <li>SSL証明書</li> <li>決済代行システム</li> <li>ごレポート &gt;</li> </ul>								
<b>⊡</b> ¤7 →								
<u>,</u> ≥274 →								
	1-15of1 トータルアイテム:1					1 /1	> > 15 v	ページごとのアイテム

図 7-1 プロファイルを作成

「ネットワークの追加」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。

「「「」」「「」」」「「」」」」」「「」」」」」」」」」「「」」」」」」」」	武····································
プロファイルの編集 🗹	サイトの詳細ページを開き、選択したサイトのセキュリティ、アクセスコントロール、ユーザ認証の設定を編集できます。
このネットワークにプ	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。
ロファイルをコピー 🗋	
ネットワークプロファ	選択したプロファイルをローカルディレクトリのファイル(*.dat)にエクスポートします。
イルをエクスポート 📑	
検出〇	「検出ネットワーク設定」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。条件を定義したら、「次へ」をクリックします。「検出開始」 をクリックして、検索の結果(「設定可能」「管理」タブのデバイス)を見つけます。
ネットワークの編集 🗹	「ネットワークを編集」面画を開きます。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。
ネットワークの削除 💼	選択したネットワーク設定を削除します。

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。

П

#### 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。「ネットワークを追加」 画面が表示されます。

🗙 ネットワークを追加		×
サイト	newSite v	
ネットワーク名	Networkı	
		次~ 終了

図 7-2 ネットワークを追加

- 2. 「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。
- 3. 「ネットワーク名」フィールドに、新しいネットワークを識別する名前を入力します。「次へ」をクリックして続行するか、「終了」をクリック して前の画面に戻ります。

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。

**4.** 「ネットワーク設定」画面が表示されます。ワイヤレス設定とデバイス設定を入力して、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「終了」をクリックします。

🗙 ネットワーク設定		×
ワイヤレス設定		
SSID名	dlink	
セキュリティ	WPA-自動-パーソナル ~	
$SSID$ $\rtimes$ $\neg$ $\neg$ $\vdash$ $"$ *	Ø	
	│ ゲストSSIDを追加(オブション)	
ゲストSSID名		
デバイス設定		
国	Japan v	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo $\qquad \lor$	
ユーザ名	admin	
パスワード*	ø	
		<b>戻</b> る 次へ

図 7-3 ネットワークの設定

#### 第7章 設定

5. 「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。 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。

<ul> <li>レイヤ3(IP)</li> <li>IP ✓ 192.164</li> </ul>	Petro			
IP V 192.100				
	5.1.150	2.108.1.200		
	J - (			

図 7-4 ネットワーク設定を検出

6. 「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一覧表示します。デバイスが検出さ れた場合は、そのデバイスを選択して「適用」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。「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。

ステート 、	IPアドレス ×	MACアドレス ~	モデルタイプ:	NMS URL	× ネットワーク
スタンドアロ	192.168.0.50	40:9b:cd:0c:64:d0	DAP-2680	192.168.0.60:8443	
	ステート ヾ スタンドアロ	ステート Y IPアドレス Y スタンドアロ 192.168.0.50	ステート VIPアドレス VMACアドレス V AQンドアロ 192.168.0.50 40:9b:cd:0c:64:d0	ステート * IPアドレス * MACアドレス * モデルタイプ.:       スタンドアロ     192.168.0.50       40:9b:cd:0c:64:d0       DAP-2680	ステート v IPアドレス v MACアドレス v モデルタイプ.:: NMS URL       スタンドアロ     192.168.0.50       40:9b:cd:0c:64:d0     DAP-2680       192.168.0.60:8443

図 7-5 AP を検出

注意 異なるセグメントの「管理」ステータスの AP については再検出されません。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。

## 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。
  - 「SSID」、「VLAN」、「帯域幅最適化」、「RF 最適化」、「スケジュール」、「デバイス設定」、「パフォーマンス」、「WLAN パーティション」、「ワイ ヤレスリソース」

< nuclias	dnh-100		🚺 🌂 JP 🗸
(i) ダッシュボード	19 50774N	プロファイルト siter > Network1	
₩ €= <i>\$</i> >	site1		
🗙 RE -	Ø Networki	設定をアップロード	
<ul> <li>プロファイルを作成</li> <li>プロファイル数定</li> <li>ファームウェアアップグレード</li> <li>SSL雇明書</li> <li>マックレード</li> </ul>	SSID VLAN 界域編展適化 RF最適化 スケジュール	间径的作为 <b>即时</b> ~	а <b>н</b> 297
<ul> <li>決済代行システム</li> </ul>	デバイス設定	実行ステータス	
	アイオンARE パフォーマンス WLANパーティション く	週月ステーチス 1/1 く	
	71177777	■ ************************************	果 v 功: Failed to cre

図 7-6 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。 「設定をアップロード」セクションフレームで、「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。「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。

#### ■ ネットワークの各種ワイヤレス設定

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ワイヤレ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。

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。

#### 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。

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

< nuclias connect	dnh-100							<b>(</b> ) ×	JP ~
(j) ダッシュボード	Q プロファイル	プロファイル > site1 > N	etworkı > SSID						
$\begin{bmatrix} hat p \\ hat p \end{bmatrix} \neq = \beta$ >	site1								
🗙 ate 🗸 🗸	Networki	インデックス 🔺 👻	周波数带 🔺 🔻 🖌	SSID ×	セキュリティー・	アクセスコントロッ	ユーザ認証 ~	アクション	
● プロファイルを作成	SSID	プライマリ	2.4GHz	dlink	WPA-自動-パーソ	無効化	無効化	Ø	
• プロファイル設定	VLAN	プライマリ	SGHz 1	dlink	WPA-自動・パーソ	無効化	無効化	Ľ	
<ul> <li>ファームウェアアップダ レード</li> <li>SSL証明書</li> </ul>	帯域構築適化 RF最適化 スケジュール	プライマリ	5GHz 2 (トライパ	dlink	WPA-自動-パーソ	無効化	無効化	Ľ	
	デバイス設定 パフォーマンス								
<u>ه</u> ۲۰۰۰ ۲۰۰۰	WLANパーティション ワイヤレスリソース	<							
Ld VX7A		セキュリティ							~
		アクセスコントロール							~
		ユーザ認証							~
		ホットスポット2.0							~
								通加 クリア	

図 7-7 プロファイル設定 - SSID

#### セキュリティ

4111-100					
Q プロファイル	プロファイル > site1 > Network1 >	> SSID			
siteı					
🐵 Networkı	セキュリティ				^
SSID	ワイヤレス設定				
VLAN	周波效带	2.4GHz v	インデックス	SSID 1 V	
蒂城幅最適化	SSID *		$\hat{X} \hat{Z} = i'$	UTE-8	
RF最適化					
スケジュール	SSIDブロードキャスト	有効化 🗸	WMM (Wi-Fiマルチメデ イブ)	有効化 🗸	
デバイス設定	セキュリティ	オープンシステム 🗸			
WLAN/*- ディション	高速ローミング(809.11	無効化 シンニの巻続は	写教性のあるモデルの特定のファームウェア	バージョンでのみ利用可能	
ワイヤレスリソース	k/v/r)	······ .			
	セキュリティ設定				
	暗号化	無効化 ~	$*- \not \forall \not \prec \not \prec$		
	キータイプ				
	01 92 °				
	寺————————————————————————————————————				
	アクセスコントロール				~
	ユーザ認証				~
	ホットスポット2.0				~
				ia	01 297

#### 図 7-8 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:「2GHz」「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 index」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

項目	説明
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、選択した接続先
	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します。
文字コード	ドロップダウンメニューをクリックして、SSID エンコーディングで使用する文字コードを選択します。
	・ 選択肢:「UTF-8」「GB2312」
	注意 現在の対応アクセスホイントでは UIF-8 はサホートされません。
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。
WMM(Wi-Fi マルチメ	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。
ディア)	
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。
	・ 選択肢:「オープンシステム(事前共有キーは不要)」
	「WPA2- パーソナル」
	「WPA2- エンタープライズ(RADIUS サーバが必要)」
	「WPA- 自動パーソナル」
	「WPA- 自動エンタープライズ(RADIUS サーバが必要)」
	Г802.1X」
802.11 k/v/r	802.11 k/v/r 機能を有効または無効にします。
	<b>注意</b> DAP-2610、DAP-2680 は未サポートです。

「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。

#### ■ 「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 V
キータイプ	HEX ~		
キー値*		der.	

図 7-9 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。
	・ 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。
	・ 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「WPA2- パーソナル /WPA2- 自動パーソナル」に設定した場合

*+-更新問隔 3600	

図 7-10 プロファイル設定 - SSID (WPA2-パーソナル /WPA2- 自動パーソナル)

項目	説明
	セキュリティ設定
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」「AES」「TKIP」
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。
パスフレーズ	使用するシークレットパスフレーズを入力します。

## 第7章 設定

■「セキュリティ」項目を「WPA2-エンタープライズ /WPA2- 自動エンタープライズ」に設定した場合

暗号化タイプ	TKIP 🗸	グループキー更新問題	3600
プライマリRADIUSサーバ語	受定		
RADIUSサーバ★		<i></i> ∜− ⊦*	1812
RADIUSシークレット <sup>★</sup>	See		
バックアップRADIUSサーノ	べ設定(オブション)		
RADIUSサーバ		#- F	1812
RADIUSシークレット	ø		
	24° - 1 4.20.4° 7		
ノフィマリノカワンティン	クサーハ設定		
アカウンティングモード	無効化 ~		
アライマリア カリンティングモード アカウンティングモード アカウンティングサーバ	(二)	アカウンティングポート	1813
アカウンティングモード アカウンティングモード アカウンティングサーバ アカウンティングシーク レット	グザーハ設定 無効化 ∨	アカウンティングポート	1813
アライマリアカリンティングモード アカウンティングモード アカウンティングサーバ アカウンティングシーク レット	グサーハ設定 無効化 ∨ ※ ※ ングサーバ設定(オプション)	アカウンティングポート	1813
アカウンティングモード アカウンティングモード アカウンティングサーバ アカウンティングシーク レット バックアップアカウンティ アカウンティングサーバ	グサーハ設定 無効化 ∨ ※ ※ ングサーバ設定(オブション)	アカウンティングポート アカウンティングポート	1813 1813

図 7-11 セキュリティ (WPA2-エンタープライズ /WPA2- 自動エンタープライズ)

項目	説明
	セキュリティ設定
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」「AES」「TKIP」
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。
	プライマリ RADIUS サーバ設定 / バックアップ RAIUS 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。
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ティングサーバ設定 / バックアップアカウンティングサーバ設定(オプション)
アカウンティングモー	ドロップダウンメニューをクリックして、アカウンティングモードを有効または無効にします。
ブガウンティンウリー バ	
アカウンティングポー	アカウンティングサーバのポート番号を入力します。
+	
アカウンティングシー	アカウンティングサーバのシークレットを入力します。
クレット	

■「セキュリティ」項目を「802.1X」に設定した場合

キー更新間隔	300		
プライマリ RADIUSサーバ語	<b>投定</b>		
RADIUSサーバ <sup>★</sup>		☆- ▶ *	1812
RADIUSシークレット <sup>★</sup>	See		
ベックアップRADIUSサーィ	*設定(オプション)		
RADIUSサーバ		ಸೇ — ト	1812
RADIUSシークレット	Se and a second		
プライマリアカウンティン:	ゲサーバ設定		
プライマリアカウンティン アカウンティングモード	ゲサーバ設定 無効化 ~		
<b>ブライマリアカウンティン</b> : アカウンティングモード アカウンティングサーバ	グサーバ設定 無効化 ~	アカウンティングポート	1813
<b>ブライマリアカウンティン</b> プカウンティングモード アカウンティングサーバ アカウンティングシーク レット	ゲサーバ設定 無効化 ~	アカウンティングポート	1813
プライマリアカウンティンジ アカウンティングモード アカウンティングサーバ アカウンティングシーク レット バックアップアカウンティ:	ゲサーバ設定 無効化 ∨ ≪ × × × × × × × × × × × × ×	アカウンティングポート	1813
プライマリアカウンティンジ アカウンティングモード アカウンティングサーバ アカウンティングシーク レット ギックアップアカウンティ アカウンティングサーバ	グサーバ設定 無効化 ∨ ※効化 ∨ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	アカウンティングポート アカウンティングポート	1813

図 7-12 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 RAIUS 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。
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ティングサーバ設定 / バックアップアカウンティングサーバ設定(オプション)
アカウンティングモー ド	ドロップダウンメニューをクリックして、アカウンティングモードを有効または無効にします。
アカウンティングサー バ	アカウンティングサーバの IP アドレスを入力します。
アカウンティングポー ト	アカウンティングサーバのポート番号を入力します。
アカウンティングシー クレット	アカウンティング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

アクセスコントロール		^
ACL		
アクション	無効化 ~	
MACアドレス	XX:XX:XX:XX:XX 說明 max.l	ength 32 (optional) 道加
MACアドレスリストをア ップロード	参照	アップロード
	メワンロート 2.4GH2帯のMACアドレスリストの最大数は512です。後り	512
	No. MACアドレス ▲	✓ 削除
	データが見つかり	ませんでした
IPフィルタ設定		
アクション	無効化 ~	
IPプドレス	サブネットマスク	ì£ha
	IPフィルタの最大エントリ数は64です。,残り64	
	IPアドレス ▲ ゲーサブネットマ	スク ~ 削除

図 7-13 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、「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	「参照…」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	
アップロード	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、「追加」をクリックします。	
### ユーザ認証

ザ認証					^
認証タイプ	Webリダイレクトのみ ∨	アイドルタイムアウト (2~1440)	60	分	
IPインタフェース設定					
IPIFステータス	無効化 ~				
$\mathrm{VLAN}\mathcal{I}\mathcal{N}-\mathcal{I}$	1				
IPアドレスの取得	スタティックIPアドレス(手動) 🗸 🗸				
IPアドレス		サブネットマスク			
ゲートウェイ		DNS			
✓ Webリダイレクション					
Webサイト*	http:// ~				

図 7-14 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。
	・ 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」「SLA ログイン」
	注音 SLA ログイン(オーDAD 2610 DAD 2690 で/オキサポートです
	「二記」 SEA ロッキンは、DAF-2010、DAF-2000 とは米リホードとす。
アイドルタイムアウト	セッションタイムアウト値を入力します。
(2~1440)	
	ホワイトリストを有効化(認証タイフが「Web リタイレクトのみ」以外の場合)
ホワイトリストを有効	チェックを人れると、ホワイトリスト機能が有効になります。この機能は、「認証タイプ」が「Web リタイレクトのみ」
	以外の場合に使用でさより。   キロノトリストに恐得せてき…トローケデボノスの MAC スドレスたみたし、「白地」たちに…ちしてスドレスたちロノ
MACTIVA	ホワイトリストに豆球するネットワークデバイスの MAC アトレスを入力し、「追加」をクリックしてアトレスをホワイ   トリストニーゴルに追加します
ホワイトリストファイ	「ワストリーフルに迫加しより。   「
   小をアップロード	$  \psi_{\text{max}} = \psi$
	$    = \frac{1}{2} \sum_{i=1}^{n} \frac{1}{2} \sum_{i=1}^$
	IP インタフェース設定
IRIF ステータス	ドロップダウンメニューをクリックして、IP インタフェースの使用を有効または無効にします。
VLAN グループ	VLAN グループ名を入力します。
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 アドレス(DHCP)」
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。
DNS	IP インタフェースの優先 DNS アドレスを入力します。
	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、「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。
	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	RADIUS サーバのタイプを選択します。(認証タイプで「リモート RADIUS」を選択した場合のみ)
プ	・ 選択肢:「SPAP」「MS-CHAPv2」
	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。

11日	説明
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」
ユーザー名	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、Web ログインページからパスコードがすでに生成されている構成済みのフロントデ
	スクユーザアカウントを表示します。 
	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」を選択します。選択後、ホームページの 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」を選択します。選択後、ホームページの URL を入力します。
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)
テンプレートの選択	ドロップ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。
	・「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。
	・「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。
	・  屁をクリックすると、選択したスタイルが削除されます。
	<ul> <li>         ・         ・         ・</li></ul>

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。

# ホットスポット

ホットスポット2.0			^
ホットスポット			
ホットスポット2.0	有効化 ~	この機能は、互数性のあるモデルの特定のファームウェアバージョンで のみ利用可能です。	
OSEN	無効化 🗸		
クロス接続を許可	無効化 ~		
P2Pを管理	無効化 ~		
DGAF	有効化 ~		
プロキシARP	無効化 ~		
L2TIF	無効化 ~		
インターワーキング			
インターワーキング	無効化 🗸		
アクセスネットワークタ イプ	プライベートネッ	× F ∇ − 2	
インターネット	無効化 ~		
ASRA	無効化 🗸		
ESR	無効化 ~		

図 7-15 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)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。			
	インターワーキング			
インターワーキング	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	アクセスネットワークのタイプを選択します。			
タイプ	・ 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	ネットワークに対し、インターネットアクセス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。			
USEA	ドロップダウンメニューをクリックして、USEA(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。			
Venue タイプ	Venue タイプの値を入力します。			
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。			
	・ 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」			
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			
	しじ速度になります。			

-= -	200					
	記明					
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 メトロックダウン	WAN 接続のダウンロードフピードを Uhne 単位で入力」ます。ダウンロードフピードが不明を提会け 0 を指定します					
U-FXE-F (Kps)						
WAN メトリックアップ	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。					
リンクスピード (kps)						
	リスト					
ネットワーク認証タイ	接続タイプを選択します。					
	、選切時・「利田坦約への同音」「オンライン登録をサポート」「http://http://l/ダイレクション」「DNS リダイレクション」					
	・ 医小胶・利用が研究 VOIPIS」 コンジアン 豆球を サハードコー ITUL/ITULS サライレフンヨンコーロ IS サライレフンヨンコー					
	「Inttp/nttps リタイレクション」「DNS リタイレクション」の場合は、URL を入力する必要かめります。					
利用可能な IP アドレス	利用可能なIPアドレスタイフを選択します。ネットワークへの認証後、 ホットスボットのオペレータやモバイルデバイ					
タイプ	スによってこのアドレスタイプが使用されます。					
	• 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 ID/A アドレフ」「利用可能たポート判問された ID/A アドレフレミン/ガル NAT された ID/A アドレフ」「利用可					
	「、「「IIIV+ノ」アレス」「利用り起なか」「前見なもか」にメリアドレスとシンフル IVAL された IV+フィアレム」「利用り					
	能なホート制限された IPV4 アトレスとダブル NAT された IPV4 アトレスダイブの 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。					
	リービスノロハイタや、ローミングハートナーのグルーノを入力し、「道加」をグリッグします。ネットワークに接続す					
74	る際に、それらのセキュリティ認証が使用されます。6 桁または 10 桁の 16 進数が人力可能です。					
	NAIレルムリスト					
NAI LILL	↓ ■ をクリック」て NALレルムを入力します。BSS で利用可能た全ての NAL レルムを設定します。入力した NALレルムを					
	削除する場合は、 - をクリックします。					
FAP 方式	FAP 方式を入力します。					
	· 2)					
	- 🛨 をクリックして、認証ID(0-255)とバラメータタイフ(0-4294967295)を人力します。人力値を削除する場合は、					
	をクリックします。					
	「追加」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					
	マクセスポイントで利田可能た 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					
	「ノーン・ステレート」「「「「「「「「」」」」「「「」」」「「「」」」「「」」」「「」」」」「「」」」「「」」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」「」」」」					
	● 設定可能範囲:00-999					
IP プロトコル	IP プロトコルを選択します。					
	・ 選択肢:「ICMP」「TCP」「UDP」					
ポート番号	ポート番号を入力します。					
7-47						
	┃ ・ 選択肢・「クロース」「オーノノ」「不明」					
オペレータフレンドリ	言語を選択し、オペレータフレンドリ名を入力します。Hotspot Venue オペレータの識別名です。					
名						
	OSU (Onlin Sign-Up)					
OSU SSID	OSU SSID を入力します。					
	OSU 方式リスト					
OSU 方式						
OSU コンフィグ	OSU コンフィグ選択します。					
	<ul> <li>・ 選択時・「コンフィグ1」「コンフィグ2」</li> </ul>					
OSU フレンドリ名	言語を選択し、OSU フレンドリ名を入力します。					
OSU Nai	OSU NAI を入力します。					
OSUサービス説明	OSUサービス説明を入力します。					
	へいし アイコン 言語 コードを 躍切し キオ					

	r
項目	
OSU アイコンファイル	OSU アイコンのファイルパスを入力します。
パス	
OSU アイコンファイル	OSU アイコンのファイル名を入力します。
名	
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	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 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「追加」をクリックします。

### ■ 既存ルールの変更

ルールを変更する場合は、対象 SSID のごをクリックします。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。

「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。

注意 設定が更新されたら、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.31)」 を参照してください。

### VLAN

「VLAN」ページには、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。設定に移動します。設定>

プロファイル設定>サイト>ネットワーク>VLANの順に移動して、現在の設定を表示します。

# VLAN リスト

VLAN リスト」タブを選択すると、以下の設定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」をクリックして値を保存し、画面を更新します。「VLAN リスト」タブには、作成されたすべての VLAN の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。

#### nをクリックして、既存の VLAN を削除します。

<nuclias< th=""><th>dnh-100</th><th></th><th>🔨 л</th></nuclias<>	dnh-100		🔨 л
S Ørvan-F			
₩ €= 9 >	(P 2 0 2 7 4 1P	2 D 2 7 4 P > SIBI > NEWWORKI > VLAN	
	Networks		
× 82 ~	WELWOLK1	VLANステ ータス 無効化 VLANステ	
• プロファイルを作成	SSID		
• プロファイル設定	VLAN	VLANリスト ポートリスト VLANを追加/編集 PVID設定	
<ul> <li>ファームウェアアップグ レード</li> <li>SSL証明書</li> </ul>	带軟幅壓迫化 RF最適化	VLAN VID ★ - VLAN名 - タグVLANポート	> アンタグVLANポート > アクション
• 決済代行システム	スケジュール	1 default	管理, LAN1, LAN2, プライマリ (2.4G), SSID1 (2 📝 🍵
	デバイス設定		
	パフォーマンス		
9 P7 >	WLAN /*- ? + > = >		
0 2274 >	ワイヤレスリソース	<	
		1-15 of 1 トータルアイテム: 1	《 〈 1 /1 〉 》 15 ッ ページごとのアイテム

図 7-16 プロファイル設定 - VLAN

### 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。

「ポート名」列の横にある列の「タグ VID」「アンタグ VID」列には、ポートが VLAN のタグ付メンバであるか、タグなしメンバであるかが示されます。 最後の列の「PVID(ポート VLAN ID)」には、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。

### 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。



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.31)」を参照してください。

### 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>帯域幅最適化の順に移動して、現在の設定を表示します。

< nuclias	dnh-100			🚺 🤫 JP 🗸
ダッシュボード	19 20771N	プロファイル > site1 > Network1 > 帯#	(結果)進化	
1000 €=∮ >	site1			
🗙 872 -	Networki	带城幅跟迪化を有効化	無効化 ~	
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> </ul>	SSID VLAN	グウンリンク 帯域幅	80 Mbps	
<ul> <li>ファームウェアアップグ</li> </ul>	带城幅蒙迪化	アップリンク 夢試師	So Mhree	
レード • SSL証明書	RF最適化	A A A A A A A A A A A A A A A A A A A	14059	
● 決済代行システム	スケジュール	帶域幅最適化ルールを追加		
→     →	デバイス設定	ルールタイプ	各クライアントの平均新城镇を割り当て 🗸	
<u>∎</u> ¤∕ →	WLAN- 7 イション	周痰效蒂		
C AFRY OL	ワイヤレスリソース	<ul> <li>SSID インデックス</li> </ul>		
		ダウンリンク スピード	80 Mbps ~	
		アップリンク スピード	80 Mbps ~	
			通加	
		周波数× \$SID ▲ × タイプ	< ダウンリンクスピーヾ アップリンクスピーヾ	アクション

図 7-17 プロファイル設定 - 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。
	・「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。
	- 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、ルールで使用される無線周波数帯域を選択します。
	<ul> <li>選択肢:「2.4GHz」「5GHz 1」「5GHz 2(トライバンド)」</li> </ul>
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、ルールで使用される 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 のいずれか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 のいずれか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。

#### ■ 既存ルールの変更

ルールを変更する場合は、対象ルールのごをクリックします。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。

「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。



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.31)」を参照してください。

### 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 > RF 最適化に移動して、現在の設定を表示します。

snuclias connect	dnh-100		×	JP 🗸
1 Jy va K- F	10 - Martin 1 - 4	warraw Josephia - Mahanaha - TPEWA		
	site1	クロリナオル > Sitel > NetWork1 > Rr 都通信		
🗙 az 🗸 -	Ø Networki	RF 戰適化		
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> <li>ファームウェアアップグレード</li> <li>SSL証明書</li> </ul>	SSID VLAN 带岐國憲適化 RF <b>尿癌化</b>	<ul> <li>2010年年月前日</li> <li>2010年年月日</li> <li>2010年年月日</li> <li>2010年年月日</li> <li>2010年日</li> <li>20</li></ul>		
<ul> <li>・ 鉄病代行システム</li> <li>□ レギー1 →</li> <li>□ のグ →</li> <li>□ システム →</li> </ul>	スケジュール デバイス設定 パフォーマンス WLAN <i>パーライシ</i> ヨン ワイオレスリソース		<b>2</b>	

図 7-18 プロファイル設定 - 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。
自動チャネル調整	ラジオボタンをクリックして、RF 干渉を回避するためにクライアントのチャ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	「自動チャネル調整」が有効な場合に使用できます。ラジオボタンをクリックして、干渉が存在する場合にカバレッジを
	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.31)」を参照してください。

# 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>スケジュールに移動して、現在の設定を表示します。

< nuclias	dnh-100					*	JP v
(▲) ダッシュポード	(2) プロファイル	プロファイル > site1 > Net	tworks > スケジュール				
$\begin{bmatrix} \underline{\operatorname{Int}}_{\beta} \\ \underline{\mathtt{A}} \\ \end{array} \Leftrightarrow = \mathcal{I} \qquad \qquad >$	site1						
🗙 設定 🗸 🗸	Ø Networki	ワイヤレススケジュ	無効化 ~				
<ul> <li>フロフィイル設定</li> <li>フロフィイル設定</li> <li>フレームウェブアンブグ</li> <li>SSL度明算</li> <li>決消代行ンステム</li> <li>レポート &gt;</li> <li>レポート &gt;</li> <li>ログ &gt;</li> <li>システム &gt;</li> </ul>	SSID VLAN 帯場構置適化 R7原動化 スケジュール デバイス設定 パフォーマンス VILANパーティション ワイキレスリソース	スケジュールルール 衣崩 インデックス SSID 電日 く	を追加 デフィークSSID 3.40> dlink ・ 1個簡件 ● 程名を選択 日曜日 月曜日 大曜日 大曜日 大曜日 土曜日 ・ 日日中 ● 時間を選択 07:22 2 M ④ 07:22 3 FM ④				
		ステーター~ 名前 ▲	ax クリア * SSIDインデックスと、日	* \$1470-1 * 9170_*	アクション		

図 7-19 プロファイル設定 - 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	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。
ル	
	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、スケジュールのアクティブな日を設定します。
	・「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、スケジュールのアクティブ時間を選択します。
	・「1日中」:終日ルールを有効にします。
	<ul> <li>「時間を選択」:ルールの開始時刻と終了時刻を指定します。</li> </ul>
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。

### ■ 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。

### ■ 既存ルールの変更

ルールを変更する場合は、対象ルールのごをクリックします。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 mをクリックします。

「クリア」をクリックすると、設定が初期値に戻ります。



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.31)」を参照してください。

# 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。 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。

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

connect	dnh-100			😍 💌
③ ダッシュボード	19 JP7712	プロファイル > site1 > Network1 > デ	(イス設定)	
₹=9 >	site1			
V 82 .	Setwork1	管理者		
~ ***	SSID	ユーザ名	admin	
<ul> <li>プロファイルを作成</li> </ul>	VLAN			
<ul> <li>フロファイル改定</li> <li>フロートローズアーデダ</li> </ul>	带城幅豪適化	×*スワード		
レード ・ SSL証明書	RF最適化	コンソール設定		
<ul> <li>決済代行システム</li> </ul>	スケジュール		✓ 有効化	
	デバイス設定	コンソールプロトコル	Telnet      SSH	
	パフォーマンス			
<u>ه</u> ۲ ۲	WLANN-FASSY	タイムアウト	337 ~	
50 VZ76 >	94+0299-2	< 自動時間設定		
			NTPサーバを有効化	
		NTP #	IPブドレス/ドメイン名	
		国設定		
		国を選択	Japan マ 現時に基づき、デバイスさってにおいて、 国政定が、米国、日本、韓国またはイスラスルとして政定さ	れている場
		タイムブーン	(GMT+09:00) Osaka, Sapporo, Tokyo	
			サマータイム産育効化	
		DST開始 (24時間)	第1 ~ 目曜日 ~ in 1月 ~ at 00 ~ 5	

図 7-20 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を入力します。
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を入力します。
	- 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。
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。
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。
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
   (キャプティブポータルログ)	しています。

「保存」をクリックして設定を保存します。





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.31)」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。

# 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。

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

<nuclias connect</nuclias 	dnh-100		Ç	🔊 🔨 л
(3) ダッシュボード	the starting to	efteret e d'un altan Matanalan area anare		
🖳 e=3 🔹 >	dta:	7 B 7 7 4 7 > SIGE1 > INEUWORK1 > 7 7 * - 47 X		
¥ 82	Network1	2.4GHz 5GHz 1 5GHz 2(トライバンド)	LAN	
<ul> <li>プロファイルを作成</li> </ul>	SSID VLAN	ワイキレス	*2 ~	
<ul> <li>フロノナイル数定</li> <li>ファームウェアアップグ</li> </ul>	蒂城幅最適化	ワイヤレスモード	802.11N、802.11g、802.11b混在 ~	
レード SSL証明書 ・ 決済代行システム	RF最適化 スケジュール	$\mathcal{T} = \mathcal{I} \; \nu - 1$		
	17+	ビーコン間際 (40-500)	100	
<u>ت</u> ۲ >	WLANパーティション ワイヤレスリソース	DTIM間稿 (1-15)	1	
50 ××74 >		< WMM (Wi-Fiマルチメディア)	有効化 ~	
		ACKタイムアウト (2.4GHz, 48~200)	<b>4</b> β μ <i>s</i>	
		> $=$ + GI	無効化 ~	
		$\operatorname{IGMP} \nearrow \mathbb{X} - \mathbb{C} > \mathcal{I}$	無効化 ~	
		マルチキャストレート	無効化 ~	
		マルチキャスト常城幅コントロール	無効化 ∨ 変更すると、別の周級装置にも適用されます。	
		最大マルチキャスト帯城幅	100 kbps 変更すると、別の間疾炎帯にも適用されます。	
		* **** = = 1 · = +** ***	Are held for	

図 7-21 プロファイル設定 - パフォーマンス設定

### 「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
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。
	ドロップブランズニューをクリックして、ホットフークで使用されるフィアレスと一下を選択します。 - 選択時・(2.4CHzの担合)「002.11g_002.11g_002.11b 泪左」「002.11g_002.11b 泪左」「002.11b 河左」
	・ 医小成 ・ (Z.+GHZ 00%日) 「002.111、002.113、002.110 混任」「002.113、002.110 混任」「002.111、002.110 に任」「002.111、005」 (5CHz 1/5CHz 2 の堤合)「802 11a 802 11a 現在「802 11a のみ」「802 11a のみ」「802 11a 現在(3c/n/a 現在)」
   データレート	(JOHZ 17 JOHZ 2 00場日) 1002.111(002.11a ルビ) 1002.111(0005) 1002.111(0005) 1002.114(ルビ(aChi/a ルビ))
	10////2010年1/2010年1/2010年1/2011年1
ビーコン間隔	ビーコン間隔の値を入力します。
	<ul> <li>初期値:100</li> </ul>
DTIM 間隔	DTIM intterval 値を入力します。
	<ul> <li>初期值:1</li> </ul>
WMM(Wi-Fi マルチメ	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。
ディア)	
ACK タイムアウト	ACK タイムアウト値を入力します。
	<ul> <li>初期値:48</li> </ul>
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。
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。
マルチキャスト帯域幅	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。
コントロール	
最大マルチキャスト帯	マルチキャスト帯域幅の最大値を入力します。この機能は、「マルチキャスト帯域幅コントロール」が有効の場合にのみ
域幅	使用できます。
	<ul> <li>初期値:100</li> </ul>
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。
DHCPOFFER をマルチ	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。
キャストからユニキャ	
ストに変更	
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

# 第7章 設定

項目	説明
チャネル幅	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ネル幅を選択します。
	・ 選択肢:(「802.11n、802.11g、802.11b 混在」「802.11n のみ」「802.11n、802.11a 混在」の場合)「20MHz」「自動 20MHz/40MHz」
	(「802.11ac 混在」の場合)「20MHz」「自動 20MHz/40MHz」「自動 20MHz/40MHz/80Mhz」

「保存」をクリックして設定を保存します。

### スパニングツリー

tworks 2 AN	ファイル > site1 > Net .4GHz 9GHz 1 STP (スパニングツ ター)	worki > パフォー・ 5GHz 2(トライバ 無効化 、	マンス ンド) LAN					
twork1 2	.4GHz 5GHz 1 STP (スパニングツ ター)	5GHz 2(トライバ 無効化 、	> F) LAN					
twork1 2 ND LAN	.4GHz 5GH2 1 STP (スパニングツ リー)	5GHz 2(トライベ 無効化 ッ	> F) LAN					
ID LAN	STP (スパニングツ リー)	無効化 ~	Mr.M. ovt. A. S.T. at					
LAN			Max of Park 4- 6	を持ったアクセスポイントにの。	み、この設定を適用できます。			
城嶺蒙迪化 - 蒙適化 ケジュール							保存	
マキーマンス								
LANパーティンヨン								
<pre></pre>								
	●御化 インス定定 ・オーマンス AN/パーティンユン ・オレンスリソース C	●命化 ダジュール イス及差 キャーマンス AN/バーティション ・ キレンスリソース く	₩値に ダジュール イメス版E キャーマンス AN/バーティション ・ + レンスリソース く	₩値に ダジュール イメス酸 キーマンス AN/バーティション ・ +レンメリソース く	#@C ジュール イス型: * → → > ス AN / ← ティション - *レンメリソース <	○グユール ・グユール ・ → マンス トレーンティション ・ → レスリソース ・	#@化 ジュール イス設定 キャーシスス AN/バーティション - インスリソース	#@ft (ジュール) (イス版定 (オーマンス) AN/バーティション (キレスリソース) (キレスリソース)

図 7-22 プロファイル設定 - パフォーマンス設定(スパニングツリー)

「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			

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.31)」を参照してください。

### 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。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。

設定>プロファイル設定>サイト>ネットワーク>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。

< nuclias	dnh-100		×	JP v
(★) グッシュポード	() JOTTAN	プロファイル > siter > Network: > WLANパーティンヨン		
±;	site1			
🗙 872 -	🐵 Networkı	2.4GHz 5GHz 1 5GHz 2 () 74 × × × × )		
<ul> <li>ブロファイル安作成</li> <li>ブロファイル安定</li> <li>ブロファイル設定</li> <li>フレートのコアファング</li> <li>SEL展明着</li> <li>決済代行システム</li> <li>レモート 、</li> <li>レモート 、</li> <li>レモート 、</li> <li>レモート 、</li> <li>レモート 、</li> <li>レズーム 、</li> </ul>	SSID VLAN 形成最高化 RP最適化 スケジュール アバイス設定 パフォーマンス VVLANパーライション ワイホレスリソース	リンクインテブララ     単助化       市成LANA-5 世報会     有効化       カラブモマン     有効化       クライアント防盗信       ブクイマンSSID     ● 有効化       サントモード       マルプSSID2     ● 有効化       ● 有効化     無効化       ゲストモード       マルプSSID3     ● 有効化       ● 有効化     無効化       ゲストモード       マルプSSID3     ● 有効化       ● 有効化     無効化       ゲストモード       マルプSSID5     ● 有効化       ● 有効化     無効化		
			禄召	

図 7-23 プロファイル設定 - WLAN パーティション

#### 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、ワイヤレスリンクインテグリティ機能を有効または無効にします。	
有線 LAN から無線への	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。	
アクセス		
クライアント間通信		
プライマリ SSID/ マル	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	
チ SSID1-7	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.31)」を参照してください。

# 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。

設定>プロファイル設定>サイト>ネットワーク>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。

sonnect	dnh-100		91. 🗡
<ul> <li>デッシュボード</li> <li>第 キニタ &gt;</li> </ul>	ǰ 7¤771₽	プロファイル > sites > Networks > ワイキレスリッース	
<b>X</b> RE -	site1	2.4GHz 5GHz1 5GHz2(トライバンド) エブタイムフェブネス バンドステブリング	
・ プロフィルを作成     ・ プロフィルを作成     ・ プロフィル数     ・ プロフィル数     ・ グロフィル 数     ・ グロフィル 数     ・ グロクィール 数     ・ グロール 3     ・ グロール 3	SSID VLAN 単純酸層道化 対策量化 スケジュール デバイス設定 パフォーマンス WLANパーテイション フィキレスリソース	<ul> <li>△ ACL RSSIL \$\u03e4\u03e4 10 \u03e4 \u03e4</li> <li>ニージングプウト</li> <li>エージングプウト</li> <li>RSSIL \$\u03e4\u03e4 10 \u03e4 \u03e4</li> <li>アーメレート</li> <li>6 Mbps</li> <li>ブーダ助限(0-64)</li> <li>20</li> <li>11.0使先</li> <li>床⇒1+ワーク使用率</li> <li>10 \u03e5 \u03e4</li> </ul>	
			<b>8</b> 7

図 7-24 プロファイル設定 - ワイヤレスリソース

「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	ラジオボタン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 RRSI を設定しま				
	す。決定された値が、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	ラジオボタン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。				
	<ul> <li>初期値:20</li> </ul>				
	<ul> <li>・ 設定可能範囲:0-64</li> </ul>				
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.31)」を参照してください。

## 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配分します。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 WiFi 通信速度が遅いデバイスは、物理的な距離が長い場合や、信号強度が弱い場合、古いレガシーハードウェアの場合などにより、速度 の低下が発生している可能性があります。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>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。

< nuclias	dnh-100				JP 🗸
(ii) グッシュボード	CP プロファイル	プロファイル > site1 > Network1 > ワイヤレスリソー	z		
1000 €=9 >	site1				
🗙 &E 🗸 🗸	🐵 Networki	2.4GHz 5GHz1 5GHz2((774/777)	2/2/2/2/2/4×	////A7/9/9	
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> </ul>	SSID VLAN 茶城幅置消化	一 有効化			
<ul> <li>ファームウェアアップグ レード</li> <li>SSL証明書</li> <li>決済代行システム</li> </ul>	RF最適化 スケジュール				保存
	デバイス設定 パフォーマンス WLANパーティション				
G 2774 >	タイキレスリソース	<			

図 7-25 プロファイル設定 - エアタイムフェアネス

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.31)」を参照してください。

# 第7章 設定

# 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>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。

<nuclias< th=""><th>dnh-100</th><th></th><th>🔳 🔀 JE 🗸</th></nuclias<>	dnh-100		🔳 🔀 JE 🗸
Contract     Contract     Contract     Contract     アッシュボード     デュ     マンシュボード     マンシュボー     マンフフイルを作成     プロフフイルを     アー     アンフィー     アンファン     マンファン	dnh-100 ダア プロファイル・ site: ③ Network: SSID VLAN 素域最厚値化 取算最低 取算最低	プロファイル > sites > Networks > ワイキレスタソース 2.4GHz g3Hz1 g3Hz2(トライバンド) エアタイムフェアネス パンドステアリング 二 客助化	
<ul> <li>SSLEP第</li> <li>決済代行システム</li> <li>ゴレゼート 、</li> <li>ゴレゼート 、</li> <li>ログ 、</li> <li>ログ 、</li> <li>ワステム 、</li> </ul>	スケジュール ゲバス政定 パフォーマンス WLAN <i>ペ</i> ーティション ワイヤレスリソース		

図 7-26 プロファイル設定 - バンドステアリング

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.31)」を参照してください。

# 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」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、将 来のバグを防ぎ、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 > ファームウェアアップグレード > サイト > ネットワークの順に移動します。

< nuclias	dnh-100		JP
🕥 Xv V a K - F	977-69=77079	$\mathcal{T} \mathcal{T} - \mathcal{L} \mathcal{D} = \mathcal{T} \mathcal{T} / \mathcal{T} / \mathcal{V} - \mathcal{V} > \text{Network1}$	
111 1↓ €=9 >	site1		
🗙 &E 🗸 🗸	Ø Networki	各モデルのファームウェアファイルをアップロード	
• プロファイルを作成		モデル名/ハードウェアバージ× ファームウェアバージ× ファームウェアファイル アクション	
• プロファイル設定		DAP-2680/2A1G	変更
・ ファームウェアアップグ レード			
■ SSL証明書			
決済代行システム			
記 レポート >			
P7 >>			
0 2754 )		ć	
		BR(%2%) PA <b>EDH</b> ( 🗸	
			1 295
		実行ステータス	

図 7-27 ファームウェアアップグレード

#### 以下の設定項目が表示されます。

項目	説明
変更	「変更」ボタンをクリックして、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。
開始時間	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日時を指定、または
	即時にアップロードを行います。
	・「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。

「適用」をクリックして、上記の構成設定を保存します。「クリア」をクリックして、定義済みの設定を削除します。

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」、「モデルタイプ」、「結果」でソートできます。

実行ステータス							
適用ステータス	0/1						
結果	実行時間 ▼	~ 名前	≚ IPアドレス	≚ MACアドレス	Y モデルタイプ	✓ 結果	
			利用可能な結果	はまだありません。			

図 7-28 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 ※サポート予定

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。証明書の設定を完了するには、 SSL 証明書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 証明書に移動します。

<nuclias< th=""><th>dnh-100</th><th></th><th></th><th></th><th>×</th><th>JP v</th></nuclias<>	dnh-100				×	JP v
() ダッシュボード	♥ SSL范明書	SSL証明書 > sitei > Networki				
₩ <u>₩</u>	site1					
🗙 872	Setworki	SSL証明書を更新				
<ul> <li>プロファイルを作成</li> <li>プロファイルを作成</li> </ul>		ファイルから証明書をアッ	₹¤- F	参照		
<ul> <li>ファームウェアアップグレード</li> <li>ロアアービウェアアップグレード</li> </ul>		ファイルかちゃーをアップ	p- ŀ	<b></b>		
<ul> <li>SSLate明書</li> <li>決済代行システム</li> </ul>				52	- 15	
∎ ¤7 →		実行ステータス				
50 ××74 >		く 適用ステータス (	o/o			
		結果	实行的	周▼		
				利用可能な結果はまだありません。		

図 7-29 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	「参照 …」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。
アップロード	
ファイルからキーを	「参照」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	

「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。

<nuclias< th=""><th>dnh-100</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>×</th><th>JP v</th></nuclias<>	dnh-100									×	JP v
(f) 9 × × = # - F											
$[\underline{\operatorname{hup}}_{24}] \not = \beta \qquad \rightarrow$	支払設定										
🗙 設定 🗸 🗸	Paypal通衡*	USD	~								
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> </ul>	Paypal クライアントID*										
<ul> <li>ファームウェアアップグ レード</li> <li>SSL証明書</li> </ul>	Paypal >- 2 > 2 **										
• 決済代行システム	オプション*	101Pd1	0	分	~	費用	D				
「」 - * - * 、 、		101124		- つ遊択		費用		Ŧ			
50 VZF4 >									1	≹存	

図 7-30 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	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 <mark>+</mark> 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8章 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」
- 「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」

# 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の使用状況を表示します。

レポート>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。

< nuclias connect	dnh-100		×
デッシュボード			_
$\frac{1}{10} \neq = \beta$ >	ワイヤレスネットワークのよく利用されている時間 全てのサイト ◇ 全てのネットワーク ◇ 民 2018/12/27~2019/01/02		3
K RE >	過去7日間で最もクライアントが利用している時間  C report.threshold: 0	確容: <mark>0.0</mark>	10%
] v#−t v			
<ul> <li>ビークネットワークアク ディビディ</li> <li>時間別ネットワークアク ディビディ</li> <li>日別ネットワークアクテ イビディ</li> <li>最もアクティブなAP</li> </ul>			
1	ດກາດ ດາະດາ ດະດາ ດະດາ ດະດາ ດະດາ ດະດາ ດຳລາ ດຳລາ ດຳລາ ດາະດາ ກາດ ກະດາ ກະດາ ກະດາ ກະດາ ກະດາ ກະດ		-
		- 13100 I	:4:0C
10 VZ74 )		. 13:00 1	:4:0C
10 VX7A )	道去7日間で見た利用量の多い時間 「Pepert.threshold: o MB	確容: 0.0	10%
→ 20	道金7日間で最も利用量の多い時間 ビーマロのT-threshold: 0 MB ・・・パ注用量 (10)	權 <b>卒: 0.0</b>	10%

図 8-1 ピークネットワークアクティビティ

以下のレポートが表示されます。

- ・ 過去7日間分で最もクライアントが利用している時間
- ・ 過去7日間分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 > 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。
```

<nuclias< th=""><th>dnh-100 🔍 🔀 a</th></nuclias<>	dnh-100 🔍 🔀 a
(デ) ダッシュボード	
10 <sup>2</sup> 3.00 €= 9 →	ワイヤレスネットワークにおける時間別読計 全てのサイト ◇ 全てのネットワーク ◇ < 2019/01/02 ◇ > 良
🗙 設定 ,	時間別接後クライアント放と過去?目間の実績
	- 2019/01/02 🗧 平均 🔳 高
<ul> <li>ビークネットワークアク ティビティ</li> <li>         ・ 時間別をフトワークアク     </li> </ul>	
<ul> <li>日別ネットワークアクティビディ</li> <li>最もアクティブなAP</li> </ul>	
<u>و</u> مر ا	0,00 01.00 05.00 05.00 05.00 05.00 05.00 05.00 05.00 05.00 05.00 10.00 15.00 1
50 x72 >	
	時間別トラフィックの決測量と過去?日間の実績
	(#28) 문 (molefined) - 2019/01/02 - 부터 一 (K
	موروو مورو مورو مورو مرور مرور ورور ورو

図 8-2 時間単位のネットワークアクティビティ

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。





図 8-3 日別ネットワークアクティビティ

特定のクライアント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、 園をクリックしてレポートを表示します。レポート生成後、 と 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。

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 > 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 8-4 最もアクティブな AP

最もアクティブな AP のレポートを表示するには、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。

以下のデータが画面右上に表示されます。

- 過去7日間の接続クライアント数の平均
- ・ 過去7日間のトライフィック使用量の平均

#### ■ マップの編集

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。

☑ をクリックすると、「最もアクティブな AP のマップを編集」画面が開きます。マップの名前を編集し、「AP を選択」をクリックして、使用可能 な AP のリストから AP を選択します。定義したら、「保存」をクリックして設定を保存します。

#### ■ マップの追加

新しいマップを追加するには、 🕂 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。 「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。画像(サポートされているファイル形式: PNG または JPG、最大 10MB)をドラッグ&ドロップするか、ローカルフォルダを参 照してイメージを選択し、マップをカスタマイズします。



注意 設定のリストア後に、最もアクティブな AP レポートのデバイスアイコンは更新されません。

# 第9章 ログ

- 「SNMPトラップ」
- 「シスログ」
- 「システムイベントログ」
- 「デバイスログ」

# SNMP トラップ

SNMP トラップ機能を使用すると、管理者は、ネットワークデバイスに関するイベントが発生したときにアラートメッセージを表示できます。

ログ > SNMP トラップに移動して、レポートを生成および表示します。

<b>∢ nuclias</b>	Default Q 🗴 yp
(i) ダッシュポード	サペマのSNBFバージョン サペマの汎用タイプ ∨ 2020.1.3 簡 2020/01/10 箇 IPアドレス ∨ キーワードを検索 Q Q
1117 €=Ø >	受信時間 × トラップ時間 × × 名前 × IPアドレス × SNMPバーニ トラップタイプ × トラップ詳細
🗙 設定 🔹	2020-01-09 17:42:37 2020-01-09 18:41:44 D-Link DA 192.168.0.50 V1 enterpriseSpecific ['TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
レポート >	2020-01-09 17:03:01 2020-01-09 18:02:08 D-Link DA 192.168.0.50 V1 enterpriseSpecific ['TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7';Binding Variable: 1.3.6.1
🖬 ¤# 🗸 🗸	2020-01-09 17:03:01 2020-01-09 18:02:08 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7",Binding Variable: 1.3.6.1
<ul> <li>SNMPトラップ</li> </ul>	2020-01-09 17:03:00 2020-01-09 18:02:07 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
・ シスログ	2020-01-09 17:02:55 2020-01-09 18:02:02 D-Link DA 192.168:0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7,"Binding Variable:1.3.6.1
<ul> <li>システムイベントログ</li> </ul>	2020-01-09 17:02:50 2020-01-09 18:01:57 D-Link DA 192.168:0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7",Binding Variable:1.3.6.1
• デバイスログ	2020 01-09 17:02:26 2020 01-09 18:01:34 D-Link DA 192.168.050 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13",Binding Variable: 1.3.6.1
50 ×274 >	2020-01-09 16:52.02 2020-01-09 17:51.09 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;"Binding Variable:1.3.6.1
	2020-01-09 16-52-01 2020-01-09 17-51:09 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;Binding Variable:1.3.6.1
	2020 01-09 16:52:01 2020 01-09 17:51:08 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13",Binding Variable: 1.3.6.1
	2020-01-09 16:51:56 2020-01-09 17:51:03 D-Link DA 192.168.050 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7";Binding Variable:1.3.6.1
	2020-01-09 16:51:51 2020 01-09 17:50:58 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.57.2.0.7;"Binding Variable:1.3.6.1
	2020-01-09 16:51:27 2020-01-09 17:50:34 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13",Binding Variable: 1.3.6.1
	2020-01-09 16:51:25 2020-01-09 17:50:32 D-Link DA 192:168:0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
	2020-01-09 16-51:10 2020-01-09 17:50:17 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7";Binding Variable:1.3.6.1
	2020-01-09 16:51:10 2020-01-09 17:50:17 D-Link DA., 192.168.0.50 V1 enterpriseSpecific ['TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;'Binding Variable: 1.3.6.1
	2020-01-09 16:51:06 2020-01-09 17:50:13 D-Link DA., 192.168.0.50 V1 coldStart ["TrapOID: "Binding Variable:1.3.6.1.4.1.171.10.37.60.2.1.1.1.1.5=40.9 v
	1-50 at 25 トータルアイテム:25 (1)/1 > )) 50 v ページごとのアイテム

図 9-1 SNMP トラップ

トラップレポートのフィルタ条件として、SNMP バージョン、イベントタイプ、およびレポート期間を選択することができます。さらに、検索条件のタイプとして「IP アドレス」または「トラップ詳細」を選択し、キーワードフィールドに値を入力することもできます。 図をクリックしてフィルタを適用します。

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。

注意 SNMP トラップは OID で記録され、コンパイルや変換は未サポートです。

# 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のログメッセージを確認することができます。

**ログ>シスログ**に移動して、ログ情報を表示します。



図 9-2 シスログ

シスログレポートのフィルタ条件として、イベントの重大度、ファシリティシステム、レポート期間を選択することができます。さらに、検索条件のタイプとして「IPアドレス」または「メッセージ」を選択し、キーワードフィールドに値を入力することもできます。 📓 をクリックしてフィルタを適用します。

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。

「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。

<ul> <li>         ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>	・ × イベントタイプ 21:98:27 デバイス管理 21:01:55 初期化	イベントタイッ 2018 × ネットワーク × Network1	3.12.26 🇰 IPアドレス Y	2019.1.2 MAC7Fレス ~		8
○ 4=2 ) ○ 10%用・ ○ 10%用・ ○ 20%0101 ○ 20%0	<ul> <li>イベントタイプ</li> <li>21:38:27 デバイス管理</li> <li>21:01:55 初期化</li> </ul>	× ネットワーク × Network1	IP7Fレス ×	масряих ч	メッセージ	
<ul> <li>         ・ 訳         ・ に         ・ に         ・ に</li></ul>	. 21:38:27 デバイス管理 . 21:01:55 初期化	Network1				
<ul> <li>○ レポート → 20190101:</li> <li>○ DIVE 1.2 x x 7</li> <li>○ SINE 1.2 x x 7</li> <li>○ X X D X</li> <li>○ X X D X</li> <li>○ X X Z X</li> <li>○ X X X X X</li> <li>○ X X X X X</li> <li>○ X X X X X X</li> <li>○ X X X X X X</li> <li>○ X X X X X X<td>21:01:55 初期化</td><td></td><td>192.168.0.50</td><td>40.01 (0.01 (0.00))</td><td>Force change the device status to offline due to the keep-alive</td><td>messages is ab</td></li></ul>	21:01:55 初期化		192.168.0.50	40.01 (0.01 (0.00))	Force change the device status to offline due to the keep-alive	messages is ab
E     20190101       ■     SNMF17ップ       ■     >>37       ■     >>37       ■     >>37       ■     >>37			192.168.0.200	10.00 -0.00	The MicroSD card is ready.	
• SNMF17.y7 • ≥×8.b7 • >×7.54.4×>1.b7 • ₹<4.3.b7	21:01:55 ファームウェアアッ.		192.168.0.200	0.0040404	Firmware Version (1.0.1.3b3, Success)	
<ul> <li>&gt;&gt; &gt;&gt; &gt;&gt;</li></ul>	. 21:01:55 初期化		192.168.0.200	10.12 m (m/Co.)	The system time is not ready.	
<ul> <li>システムイベントログ</li> <li>デバイスログ</li> <li>ジステム &gt;</li> </ul>						
₩ 2774 >						
<u> Lo xxx</u>						
1-50 of 4						

図 9-3 システムイベントログ

システムイベントログレポートのフィルタ条件として、イベントタイプおよびレポート期間を選択することができます。さらに、検索条件のタイプ として「IP アドレス」または「メッセージ」を選択し、キーワードフィールドに値を入力することもできます。 図をクリックしてフィルタを適用 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。

# デバイスログ

「デバイスログ」機能を使用すると、管理者は AP の埋め込みメモリからのアラートメッセージを表示できます。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。

<nuclias< th=""><th>dnh-100</th><th></th><th></th><th></th><th></th><th></th><th>0</th><th>🜔 🔀 JP 🤊</th></nuclias<>	dnh-100						0	🜔 🔀 JP 🤊
<ul> <li>ディシュポード</li> </ul>		すべての動作タイプ	r v	2018.12.26	2019.1.2	(111)	<b>IFブドレス ッ</b> キーワードを検索	R 🖸
$\begin{bmatrix}  z  \\ z \\ z \\ z \\ 0 \end{bmatrix} \in \exists \beta $	ログ時間 👻 🗠 🗠	名前    ~	IPアドレス	<ul> <li>маст ких ч</li> </ul>	操作種別 ~	结果 丶	ログ詳細	
🗙 設定 🔹 >	2019-01-01 21:35:46	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz 11, Channel. 5 GHz 132	
	2019-01-01 21:35:36	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく…		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36	
Ē •/ →	2019-01-01 21:34:56	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 132	
■ SNMPトラップ	2019-01-01 21:34:45	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz 11, Channel. 5 GHz: 36	
• シスログ	2019-01-01 21:34:03	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	設定をアップロ	Success	Failed to create SSIDs for some of your APs because th	ese APs may
• システムイベントログ	2019-01-01 21:30:26	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz 11, Channel. 5 GHz: 132	
• 7×1205	2019-01-01 21:30:16	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36	
50 ×274 >	2019-01-01 21:29:26	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 132	
	2019-01-01 21:29:16	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36	
	2019-01-01 21:28:39	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	デバイス設定を…	Success	Configuration Failed to create SSIDs for some of your A	APs because t
	2019-01-01 21:28:30	dap2680	192.168.0.50	40:9b:cd:0c:64:d0	登録デバイス	Success	Network1	
	1-50 of 11 トータルア	イテム: 11					« < 1 /1 > » 50 v <-	ジごとのアイテム

図 9-4 デバイスログ

デバイスログレポートのフィルタ条件として、動作タイプおよびレポート期間を選択することができます。さらに、検索条件のタイプとして「IPアドレス」または「ログ詳細」を選択し、キーワードフィールドに値を入力することもできます。 🗟 をクリックしてフィルタを適用します。

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。

# 第10章 システム管理

- 「デバイス管理」
- 「ユーザ管理」
- 「設定」
- 「接続」

# 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。

<nuclias< th=""><th></th><th>dnh-100</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Q</th><th>) 💘 ле</th></nuclias<>		dnh-100								Q	) 💘 ле
(b) # # # = # = #		0.4.17.2	100 019	11 44 14							
₩ €=9	>	site1	H AL	9F 8 - 72							
🗙 設定	>	Ø Networki		7=_h v		NATIO 7 KL 7	MACZELT	モデルカメイトッ	1-KA-744	77-10-74	#目生に得動
a v#-1	>				192.168.0.50	192 168 0 50	ately unions at	DAP-2680	2A1G	v2.00808	2019-01-01 2:
Ē ₽/				. 250							
- UNEA											
<ul> <li>デバイス管理</li> </ul>	-										
<ul> <li>ユーザ管理</li> </ul>											
• Nuclias Conne	ct12-344		¢								
			1.	50 of 1 トータ	ルアイテム:1				L /1 > ×	50 🗸	ッニとのアイテム

図 10-1 デバイス管理 - 管理デバイス

「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

デバイスのリストは、以下の基準によってソートすることができます。

 ステータス、ローカル IP アドレス、NAT IP アドレス、MAC アドレス、モデルタイプ、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

「メニュー」ボタンをクリックし、表示する項目を追加/削除することもできます。

# ユーザ管理

## ユーザステータス

ユーザステータス機能を使用すると、登録されているすべてのユーザプロファイルの現在のステータスを表示したり、プロファイルを編集したり、 削除したりすることができます。「ログインステータス」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、 ●はユーザが ログオフしていることを示します。

システムトコーザ管理に移動して	コーザステータス情報を表示します
ノヘノムノユ ノ自生に物動して、	ユ リヘノ ノヘ旧報を採加しより。

< nuclias	dnh-100	) 🔫 JP ~
(i) Sysatt-r	すべてのユーザ ユーダ会計1(▲1 ▲0 ♣0)	ユーザを追加
$ \begin{array}{c} [117] \\ \hline 1 \\ \hline 2 \\ \hline 2 \\ \hline \end{array} \end{array} \hspace{0.1 cm} \in = \mathscr{I} \hspace{0.1 cm} > \hspace{0.1 cm} $	ユーザステータス ユーザ爆発	
X RE >	ユーザ名 - ・ メールアドレス ・ ログインス	アクショ
Image:	admin ・ システム管 特効化 2020-02-2012-05:13 2019-01-02 2011-55	C
ē •/ >		
• デバイス管理		
<ul> <li>ユーザ管理</li> </ul>		
* Muclias Connecticoux		
	1-10of1 h-\$47474;1	ごとのアイテム

図 10-2 ユーザ管理 - ユーザステータス

#### ■ ユーザプロファイルの編集

ユーザプロファイルを編集するには、ユーザを選択して 「をクリックし、「ユーザの編集」面画を表示します。「ユーザ名」、「パスワード」、「メー ルアドレス」、「権限」、「権限ステータス」、「設置場所」、「電話番号」、「説明」は、変更ページから編集できます。管理者アカウントは削除できません。 また、管理者アカウントのユーザ名と権限の設定を変更することもできません。

ユーザ設定が完了したら、「保存」をクリックして確認するか、「キャンセル」をクリックして前のメニューに戻ります。

使用可能なユーザプロファイルは以下の通りです。

- ・ ルート管理者 (admin): これはオペレータアカウントであり、削除することはできません。
- 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:自分の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:自分の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。

### ユーザ権限

ユーザ権限機能を使用すると、管理者は、選択したネットワーク上のユーザを追加、表示、および承認 / 承認解除できます。

システム>ユーザ管理に移動し、「ユーザ権限」タブを選択して関連情報を表示します。

sonnect	dnh-100	💽 🔀 JP 🗸
S オッシュボード	すべてのユーザ ユーザ合計1(▲1 ▲0 ▲0)	ユーザを追加
₩₽ €=\$ >	ユーザスラータス ユーザ館限	
🗙 設定 >	sitei	
副 レポート シ	確決のないユーザ <sup>*</sup> 構決のあるユーザ <sup>*</sup>	
<b>國</b> 中グ >>		
	»	
<ul> <li>デバイス管理</li> </ul>	· · · · · · · · · · · · · · · · · · ·	
• ユーザ管理		
<ul> <li>設定</li> </ul>		
		<b>祭</b> 宿

図 10-3 ユーザ管理 - ユーザ権限

### ■ ユーザの追加

選択したネットワークにユーザを追加するには、「ユーザを追加」をクリックして「ユーザを作成」画面を開きます。この画面で、新しいユーザ情報を入力します。新規エントリを作成して完了するには、アスタリスク(\*)が付いているフィールドの入力が必須です。必要情報を入力後、「作成」をクリックして新しいユーザプロファイルを保存します。または、「キャンセル」をクリックして、保存せずに前の画面に戻ります。

#### ■ ユーザの承認 / 承認解除

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。ネットワークで使用可能なユーザが表示されま す。「権限のないユーザ」列で、ターゲットユーザのラジオボックスをクリックします。ユーザを選択したら、「シをクリックして「権限のあるユーザ」 列に移動し、ユーザを承認します。同様の手順で、ユーザの承認を解除することもできます。

# 設定

## 一般

「設定」画面には、「一般」、「接続」、「SMTP」、「バックアップ」「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)」タ ブが表示されます。「一般」タブには、カスタマイズ可能なシステム設定が表示されます。これらのパラメータには、ロゴの追加とキャプチャ機能 の有効化が含まれます。デバイスの時刻と日付、およびライブパケット間隔の設定も使用できます。

#### システム>設定に移動して、システム情報を表示します。

snuclias connect	dnh-100				, 🗶 ле -
<ul> <li>デッシュボード</li> <li>モニタ &gt;</li> </ul>	一般 接続 SMTP パック	フアップ 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)	
X RE >	カスタマイズ設定				
「」 レポート 、 、	菱蘆名	<u>dnh</u> -100			
■ P7 >	n 3'	Â			
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>		ロゴファイルをここにドラッグ&ドロップ、ま 参照 ロゴファイルをここへ ブラウザ ロゴファイルは、PNGまたはJPG画像ファイハ であり、500代を超えてはなりません	5 しくは		
・ 就定 ・ Nuclias Connectについ て	ログインキャプティ	有効化 >			
	LAN設定				
	IPアドレスの取得	スタティックIPブドレス(手動) 〜			
	IPアドレス*	192.168.0.200	サブネットマスク*	255.255.255.0	
	ゲートサエイ				
	プライマリDNS		セカングリDNS		
		操在			

図 10-4 システム - 一般

「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。

装置名を入力します。
「ブラウザ」をクリックして、インタフェースロゴとして使用するファイルを選択します。ローカルファイルは、ファイ
ルのパスを指定するか、ファイルをフレームにドラッグアンドドロップして選択できます。PNG または JPG 形式のファ
イルがサポートされます。
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。



注意 システム名に '[]{#%^\*+=\_ '[]}#%^\*+=\_\\|~<>|~<> €£ ¥を指定した場合、WebGUI にログイン不可となりエラー画面が表示されますの でご注意ください。

「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 アドレス(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)
ブライマリ DNS 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) 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。

項目	説明
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	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。または手動で時刻を設定します。
コピー	

「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」タブをクリックしてこれらの情報を表示します。

s nuclias	dnh-100	*	JP v
(k) # y ∨ a # − Y	一般 接続 SMTP バックアップ 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 (SSD)		
1 $1$ $1$ $1$ $1$ $1$ $1$ $1$ $1$ $1$			
🗙 設定 🔹 >	族統設定		
	ダバイスアクセスアドレス 192.168.0.200 v		
1 of >	PridX79eX4-1 8443		
50 X74 ×	Web7.2+2.2+++ 443		
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>	87		
<ul> <li>設定</li> </ul>			
<ul> <li>Nuclias Connect について</li> </ul>	SSL投明書を更新		
	ファイルから伊明島をデッ デロー・ デロー・		
	ファイルからキーをアップ 参照		
	<b>#</b> #		

図 10-5 システム - 接続

「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	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
レス	クIPアドレスである必要があります。ファイアウォールまたはルータの後方にあるインスタンスにはIPマッピングが必
	要です。
デバイスアクセスポー	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。ファイアウォールまたはルータの後方
F	にあるリモート AP 管理の場合は、受信ポートを開く必要があります。
	<ul> <li>初期値:8443</li> </ul>
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。値は事前定義されています。

「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
ファイルから証明書を	「参照…」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。
アップロード	
ファイルからキーを	「参照…」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	
	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。

<pre>sinuclias connect</pre>	dnh-100		🚺 🗙 JP 🗸
(f) ダッシュボード	一般 接続 SMTP ××>>	・アップ 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)	
$\begin{array}{c} [11] \\ 12 \\ 3 \\ 3 \\ \end{array} \end{array} \in = \beta \qquad \qquad > \qquad \qquad$			
🗙 設定 🔹 >	カスタマイズ設定		
園 レポート シン	SMTPホスト*	<i>#</i> × <i>F</i>	
	±		
50 x74 ×	送信元メールアドレス*	送信元メールアドレス	
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>	送信元名*	这儒元名	
<ul> <li>設定</li> <li>Nuclias Connectがつい て</li> </ul>	セキュリティタイプ	2 L v	
	コンコードタイプ	UTF-8 v	
	12.7E	ブノニマス ~	
	$\neq \lambda + \lambda - \nu$	₹ <b>ス</b> + <i>λ</i> − <i>μ</i>	
		##	

図 10-6 システム - SMTP

### 以下の設定項目が表示されます。

項目	説明
SMTP ホスト	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入力します。
	・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。
送信元名	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。
	・「なし」- SMTP サーバが STARTTLS をサポートしていない場合、メールは平文で送信されます。SMTP サーバが
	STARTTLS をサポートしている場合、メールは STARTTLS 暗号化方式で送信されます。(Explicit モード)
	・「SSL」- メールは TLS 暗号化方式で送信されます。(Implicit モード)
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、サポートされている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、電子メールサーバでサポートされているロギング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。

# バックアップ

「バックアップ」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」タブをクリックしてバックアップ設定を表示します。

<nuclias< th=""><th>dnh-100</th><th></th><th>🤱 🗙 JP 🗸</th></nuclias<>	dnh-100		🤱 🗙 JP 🗸
(i) #2%=#-F	一般 磁読 SMTP バックテップ	プ ファームウェブアップグレード システム設定 シングルサインオン(SSO)	
$\begin{bmatrix} \underline{w}_{\beta}^{*} \\ \underline{a} \Psi \end{bmatrix} \in = \beta $ >			
🗙 設定 >	自動ログバックアップ設定		
	自動ログバックアップ 無効	防化 シスログフェイルを保持したい場合、シスログをパックアップするための外部シスロとを復興します。	ダサーバを使用するこ
<b>a</b> •/ •/ •	外部シスログサーバ IPア	アドレス/ドメイン名	
50 x74 ×	保護	<b>操在</b>	
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>			
• 設定	バックアップ設定		
• Nuclias Connect (273) T	設定 🕇	eccivezzez 📴 🖫	
	₽ <i>7</i> /	r Clusty of y of G	
	リストア設定		
	設定のアップロード元 💿 🖍	ハードディスク 🔿 USBストレージ	
	7712 77	アイルを選択	
		PALT .	

図 10-7 システム - バックアップ

### ■ 自動ログバックアップ設定

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設定
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

### 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。

🕽 ダウンロード	×
To	● ハードディスク ○ USBストレージ
すべてのバックアップフ アイル	20190101_configuration.tar

図 10-8 システム - 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	
То	バックアップファイルの保存先を指定します。
	・ 選択肢:「ハードディスク」「USB ストレージ」
すべてのバックアップ	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。
ファイル	

「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

**ほ**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。

☐ 削除		>
すべてのバックアップフ 🔳 20190101_configuration.tar アイル		
	削除 キャンセル	

図 10-9 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

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:「ハードディスク」「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。

「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。

補足 リストアは即時に実行されます。
# 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。

snuclias	dnh-100		×	JP ~
ガッシュボード		アップ フォームターデアップグレード ジェラム録音 シングルサインオン (SSD)		
[10] € = ∮ →				
🗙 設定 >	ファームウェアのアップロ ードデ	N= V₹ 4 3.2 v		
「 レポート >	7712	<b>奈昭</b>		
		and a second sec		
* 47×× 02	FTF#=×=	<i>x</i> −1 21		
● デバイス管理	ユーザ名			
<ul> <li>ユーザ管理</li> <li>設定</li> </ul>	$\sim z  \bar{\eta} - \bar{r}$	<i>g</i> ø		
• Nuclias Connect (C -> % ) C	ファームウェアファイル	バスとファイル名		

図 10-10 システム - ファームウェアアップグレード

#### 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	ファームウェアファイルの取得元を選択します。
プロード元	・ 選択肢:「ハードディスク」「USB ストレージ」「FTP サーバー」
ファイル	「参照…」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	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。
ル	

「保存」をクリックして設定を保存します。



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。

注意 ファームウェアアップグレードにおいて、FTP サーバ側でバイナリモードに指定されていない場合、ファイルのアップロードに失敗します。

## システム設定

「システム設定」タブでは、システムの再起動、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。

<nuclias< th=""><th>dnh-100</th><th>×</th><th>JP ~</th></nuclias<>	dnh-100	×	JP ~
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	- 20 1814 CHITD バークチーナ フィートル・フィーブグリード (パキー1.20支 リングルーメンキン (CCD)		
₩₽ ★● += % >			
🗙 RE >	Shutdown the Device Shutdown		
	グバイスを再足前 角形動		
⊑ ¤7 →	工造出局特徴定にリストプ リストプ [ 17 ドレスを除く		
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>	<i>∞4 𝔅</i> 𝔅 𝔅 𝑘 <i>ϵ</i> − − − − − − − − − − − − − − − − − − −		
• 設定 • Nuclias Connectについ て			

図 10-11 システム - システム設定

以下の設定項目が表示されます。

項目	説明
Shutdown the Device	「Shutdown」をクリックして DNH-100 をシャットダウンします。
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。
工場出荷時設定にリス	「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 アドレスを除く」にチェックを入れた場合、デバ
トア	イスの IP アドレス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」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
フォーマット	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「Shutdown」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。

## シングルサインオン (SSO)

「シングルサインオン」タブでは、Nuclias アカウントを Nuclias Cloud および Nuclias Connect ポータルの両方でアクセス可能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)」タブをクリックして設定を表示します。

<nuclias< th=""><th></th><th>dnh-100</th><th></th><th></th><th></th><th>🚺 🌂 JP 🗸</th></nuclias<>		dnh-100				🚺 🌂 JP 🗸
·····································	8		17.17 77-14-77.1781-5	(17日1時空		
₩ <b>₩</b>	>	NK BEAL GIGIT / /	//////////////////////////////////////	277 MIRLE		
🗙 設定	>	シングルサインオン(SSO)では	は、1つのNucliasアカケントを使用して、Nuc	liasクラウドポータ)	vまたは Nuclias Connect ポータルにアクセスできます	- にアクセスできます。
a v*-+	>	このコントローラーが7日以上オ Nucliasアカウントに再度ログイ	·フラインの場合、シングルサインオン(SSO) ンする必要があります。	(オプションは自動的	に無効になることに注意してください。 シングルサイ	ンオン(SSO)オプションを有効にして、
<b>i</b> •7	>	Nucliasシングルサ	インオンを有効にする			
GO UNFA	~	Nuclias アカウント*				
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>		Nuclias ≠スワード*			長さは、8~64文字です。	
<ul> <li>設定</li> </ul>			アカウントを作成			
• Nuclias Connec T	ticon		通用			

図 10-12 システム - シングルサインオン (SSO)

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。 アカウント登録手順は以下の通りです。

## アカウントの登録

1. サーバの地域と国を選択し、「Next」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。

TEP 1 Hect server region a	and country. nuclias by D-Link
Hect server region a	nuclas by D-Link
Your new account a	
Your new account a	by D-Link
Your new account a	
within the region se to the country you :	and organization will be created on servers elected. The customer service will be forwards selected.
Server region	
	7
Country	
	-
	Next
Ali	ready have an account? Log in

図 10-13 地域 / 国の選択

 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。

「Create account」をクリックして続行します。

novascriptor@gmail.com	
D-Link	
	۲
	٢
D-Link Test	
Taiwan	
Asia/Taipei(UTC+08:00, DST)	

図 10-14 アカウント情報の入力

3. 登録が成功した場合は、「Finish」面画が表示されます。「Close」をクリックして処理を完了します。これで、登録されたアカウントが使用可能 になります。アカウントの登録 E メールアドレスに、確認用のメールが配信されます。

TEP 3	•
inish	
Your ac email ir verifica	count has been created successfully. Please check your ibox. An email has sent to your email address for tition.
	Close

図 10-15 完了画面

**4.** Nuclias アカウントは、使用前に検証される必要があります。verify@nuclias.com から、認証リンクが記載された電子メールが届きます。認証リ ンクをクリックして、Nuclias アカウントをアクティベートしてください。 認証完了後、シングルサインオン画面の設定を行います。 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。

s nuclias		dnh-100						JP ~
🛞 Øysan-r			フテップ フォ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(850)			
	>							
🗙 設定	>	シングルサインオン(SSO)では	、1つのNucliasアカウントを使用して、Nucli	asクラウドボータル	または Nuclias Connect ポータルにアクセスできます i	こアクセスできます。		
園 レポート	>	このコントローラーが7日以上オ Nucliasデカウントに再度ログイ:	フラインの場合、シングルサインオン(SSO) ンする必要があります。	オプションは自動的	に無効になることに注意してください。 シングルサイン	オン(880)オプションを	有効にして	
₽ ₽ 17	->	Nucliasシングルサイ	(ンオンを有効にする					
LO XFA	•	Nucliasブカウント*						
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> </ul>		Nuclias≁⊅ワー ₽▼			長さは、8~64文字です。			
<ul> <li>設定</li> </ul>			アカウントを作成					
• Nuclias Connect T	1000		適用					

図 10-16 システム - シングルサインオン (SSO)

#### 以下の設定項目が表示されます。

項目	説明
Nuclias シングルサイン	シングルサインオンを有効化します。
オンを有効にする	
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

Nuclias Connect ポータルではすべての Nuclias Connect ハブを確認、接続することができます。ポータルを使用するには以下の準備が必要です。
・ Nuclias アカウント

• DNH-100 デバイスでシングルサインオンを有効化

## ポータル URL:

https://connect.nuclias.com/

	DASHBOAR								
						Туре :	Ali -	Status : All	Q. Starch
	Status	Name	Host	Sites	Networks	Devices	Clients	Version	Actions
1		dnh-100	172.17 5.225,61.220.144.151	1	ï	0/0	0	1.0.0.10	E LAUNCH - FORGET

図 10-17 Nuclias Connect ポータル

#### 以下の設定項目が表示されます。

項目	説明
番号	DNH-100 のリスト番号が表示されます。
Status	DNH-100 への接続状態が表示されます。
Name	Nuclias Connect Hub の名前が表示されます。名前を変更する場合は該当項目をクリックします。
Host	デバイスの IP アドレスとパブリック IP アドレスが表示されます。
Sites	DNH-100 によって管理されるサイトの数が表示されます。
Networks	DNH-100 によって管理されるネットワークの数が表示されます。
Devices	DNH-100 によって管理されるデバイスの数が表示されます。
Clients	DNH-100 によって管理されるクライアントの数が表示されます。
Version	DNH-100 のファームウェアバージョンが表示されます。
Actions	「LAUNCH」をクリックして Nuclias Connect インタフェースを開きます。ファイアウォールまたはルータ後方のインス
	タンスに対しては IP マッピングが必要です。「Forget」をクリックすると Nuclias Connect ポータルから DNH-100 ヘリ
	ンクが解除されます。(デバイスがオフラインの場合のみ利用可能です)

# 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、サポートされるアクセスポイント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。

< nuclias		dnh-100		×	JP v
6 899=#-	F"				
1 S = 4	,	システムインフォメーション	モグルリスト		
-10					
🗙 設定	>	题	道名: dnh-100		
100		ファームウェアバージ	z ×: 1.0.1.3b7		
1-*-1 1	>	ハードウェアバージ	εν: A1		
		Nuclias Connect 🖉 🚽	a 2 : 1.0.0.19b5		
55 P /	>	DDPv5クライテントバージ	π <sup>γ</sup> : 1.0.0.8		
50 2274		IP-6-	- F : static		
		IP ア ド	LA : 192.168.0.200		
• デバイス管组		ネットマ	スク: 255.255.255.0		
• ユーザ管理		グートウ	#A :		
		DI	NS1 :		
<ul> <li>設定</li> </ul>		DI	82:		
• Nuclias Conne	ectic the	MAC7 F	να: monijarimijjod		
		システム使	用率: 17.8G/664.1M		
		MicroSD 0	送用: 14.8G/3.2M		
		USB®	메플 : n/a		
		1	YTP: Enabled_ntpi.dlink.com (このDMH-in-op時期設置は行くく始めやまません。 近しいネットワーク設定があることを確認してください。)		
			時間: 2010-01-01 12:11:08		
		タイムブ	- > : (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London		
		線衝	475 : 11 minutes		

図 10-18 Nuclias Connect について - システムインフォメーション

「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。

< nuclias		dnh-100										×	JP ~
🛞 Øv92#-	r	システムインフォメーション	モデルリスト										
100 = 9	>										+271	ン東新	
🗙 設定	>	モデルタイプ 🔺	◇ 周波数帯タイプ	Ŷ	ハードウ	ェアパージ	з×	~ 說明					
「」 レポート	-												
E 07	•												
G VAFA	*												
<ul> <li>デバイス管理</li> <li>ユーザ管理</li> <li>設定</li> </ul>													
• Nuclias Conne T	etic po												

図 10-19 Nuclias Connect について - モデルリスト

「オンライン更新」をクリックすると、アクセスポイントのリストを更新できます。新しくアクセスポイント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-2610、DAP-2680 のみです。(「Nuclias Connect 対応機器(p.9)」を参照)

# 【付録】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 DAP 製品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。Nuclias Connect アプリの機能を説明する追加情報も含まれています。

## 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。

< nuclias	Default							🔕 🔀 јр 🗸
(ib) ダッシュボード	全てのサイト >	合計1ネットワーク 合計1/1 >	トンラインAP イ	ት計 <mark>0</mark> クライブ:	ント		1	ネットワークを追加
<u>出意</u> モニタ >	サイト名 ▲	✓ ネットワーク名 ▲   >	合計デバイ	オンライン:	クライアンご	プロファイ.::	検出	アクション
🗙 設定 🗸 👻	site1	Network1	1	1	0	e d	Q	e î
<ul> <li>プロファイルを作成</li> <li>プロファイル設定</li> <li>ファームウェアアップグレード</li> <li>SSL証明時</li> <li>決済代行システム</li> </ul>								
「」 レポート 、								
ت n // >								
, ATRY 0								
	1 - 15 of 1 トータルアイテム	:1		~	< 1	/1 > >	15 v	ページごとのアイテム

図 11-20 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。

一般 接続 SMTP バック	マテップ REST API シングルサインオン (SSO)
接統設定	
<i>デバ</i> イスブクセスアドレス	その他 ~
	192.168.0.60
デバイスアクセスボート	8443 ポートを変更するには、"CAProgram Files (x86\) Nuclias connect/Core\config\appconfig.ison" へ発動し、必要に応じてポート要素を編集してく
	231.
コブサーバアクセスボート	8443

図 11-21 設定 - 接続タブ

# 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 DAP 製品を 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 DAP 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 DAP 製品を Nuclias Connect コントローラ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 DAP の設定を変更し、複数の DAP にデプロイする設定プロファイルを保存できます。

#### クイックセットアップ

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



図 11-22 Nuclias Connect アプリ(iOS)

次の手順を参照し、AP プロビジョンプロファイルを選択して DAP デバイスにプッシュ送信します。

- Step1:プロビジョニングプロファイルの選択
- ・ Step2:アクセスポイント検出範囲の定義
- Step3:アクセスポイントへのプロファイル適用

#### Step 1: プロビジョニングプロファイルの選択

- 1. 「Quick Setup」をタップすると、「Step 1」画面が表示されます。
- 2. 「Provision File」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、プロファイルをダウンロードする手順を示すポップアップページが表示されます。
- 3. Nuclias Connect コントローラへの接続を指定するには、「プロファイルのダウンロード」を選択します。



図 11-23 Step 1 - プロファイルのダウンロード

- 4. Nuclias Connect コントローラの接続が確立されると、「Provision File」フィールドの横に表示されます。
- 5. 「Provision File」をタップして、ローカル AP プロビジョンプロファイルを選択します。次の図では、エントリ Nuclias\_test\_Network1 を使用できます。

副中華電信 4G	9:27 AM 🛛 6	4% 💶 🖓
<	Quick Setup	
•	0	0
STEP 1:		
Please select an A Access Points.	P Provision Profile to push to suitable	В
Provision File		132 >
iteps there to get	a suitable AP Provision profile.	

図 11-24 Step 1 - プロビジョンプロファイルの選択

6. ポップアップ画面が表示されます。ローカルストレージから利用可能なプロビジョニングファイルを選択し、「Done」をタップして続行します。



図 11-25 Step 1 - プロビジョンプロファイルの選択

### ■ Step 2:アクセスポイント検出範囲の定義

処理が続行され、アプリは前の画面に戻ります。「Step 1」の画面で「Next」をタップして続行します。「Step 2」画面が表示されます。この画面から、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 DAP を検出することができます。

- 1. L2 フィールドのボタンをタップして、L2 ネットワークで検出を有効にします。また、L3 フィールドのボタンをタップして、L3 ネットワーク で検出を有効にします。
- 2. 「From」および「To」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. 「IP range」フィールドで、開始 IP アドレスと終了 IP アドレスを指定します。範囲を定義した後、「Next」をタップして検出プロセスを開始します。

■中華電信 4	G 9:2	8 AM	o 64% 💻
<	Quick	Setup	
-			0
STEP 2:			
Discover sta wireless net	indalone Access F works	Points in L2/L3	
L2			
_3			
_3	192.168.1.50	to 192.16	8.1.200

図 11-26 アクセスポイント検出範囲の定義

#### ■ Step 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、「Step3」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. DAP の横にあるラジオボタンをタップして選択します。Step 1 で選択したローカルのプロビジョニングファイルが、選択した DAP にプッシュ されます。
- 3. 「Push Provision File」をタップして続行します。

中華電信 🗢	9:49 AM	0 61% 💻
<	Quick Setup	G
•	•	-
STEP 3:		
heck the settings he Access Points y	for each Access Point be ou want to push the prov	law then select ision file to.
liscovered AP List		۵ ک
DAP-2662	15	2.168.1.166
V1.00	00:aa:	ca:cc:99:10

図 11-27 アクセスポイントの選択

**4.** DAP ログインのポップアップウィンドウが表示されます。リストされた IP アドレスと MAC アドレスがウィンドウの上部に表示されます。選択 内容を確認し、選択した DAP へのアクセスを許可するユーザ名とパスワードを入力します。



図 11-28 アクセスポイントへのログイン

5. 「Apply(適用)」をタップして、ログインプロセスを続行します。「Modify IP Information」画面が表示されます。リストされている情報はすべて変更できます。詳細については、次の表を参照してください。

項目	説明
キャンセル	タップして変更を破棄し、処理を続行します。
完了	タップして変更を承認し、処理を続行します。
型名	表示されている DAP デバイスのモデル名が表示されます。
MAC	リストされている DAP デバイスの MAC アドレスを表示します。
DHCPモード	タップして、DHCP モード機能を有効または無効にします。有効にすると、DAP は許可されたクライアント接続で動
	的 IP アドレス設定を確立します。
IPアドレス	タップして IP ゲートウェイ設定を指定します。
サブネットマスク	タップしてサブネットマスクを指定します。
デフォルトゲートウェイ	タップしてデフォルトゲートウェイ設定を指定します。
DNS	タップして、DNS 設定を指定します。

- 6. 「Apply(適用)」または「Cancel(キャンセル)」をタップして、処理を続行します。プロビジョニングファイルは、選択した DAP デバイス(複数可)にプッシュされます。Step3の画面に戻り、プッシュ機能のステータスが表示されます。検出された DAP には、プッシュ機能の状態が 正常または失敗のいずれかの状態で表示されます。以下の図を参照してください。
- 7. 「Finish (終了)」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、「Push Provision」をタップしてプッシュ機能を再試行します。



図 11-29 プロファイルの適用

## Nuclias Connect サーバへの接続

Nuclias Connect は、サイトとネットワークを管理できるワイヤレスアクセスポイント管理ツールです。

1. 「Nuclias Connect」を選択して Nuclias Connect サーバに接続します。



図 11-30 Nuclias Connect アプリ - トップ画面

Welcome 画面が表示されます。過去にペアリングされた 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ように求められます。追加(+) ボタンをタップして、処理を開始します。



3. 指定した Nuclias Connect サーバにログインするために必要な項目を以下に示します。各フィールドに必要な情報を入力します。

項目	説明
Specify NucliasConnect	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。
URL/IP Address	
Specify a reference name	ペアになる Nuclias Connect サーバを簡単に識別するための名前を入力します。
User name	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。
Password	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。
Login	「ログイン」をタップして、ログイン処理を開始します。

4. 「Login」をタップして、ログイン処理を開始します。



図 11-32 新規サーバへのログイン画面

5. ログインが成功すると、ペアリングがリストに追加され、今後のログイン選択に使用できるようになります。



図 11-33 Nuclias Connect サーバのリスト

- 6. 一覧から Nuclias Connect サーバを選択します。
- 7. ログイン画面が表示されます。選択した Nuclias Connect サーバにアクセスするための権限を持つユーザ名とパスワードを入力します。「Login」 をタップして、ログイン処理を開始します。

atl 4G	3	36 PM	100%
<	Nuclia	s Connect	
		nuclias	connect
-		61.216.155.	11:30001
te	ist		
			-
			•
		ogin	

図 11-34 ログイン画面

8. ログイン認証が完了すると、ダッシュボードが表示されます。Nuclias Connect 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、クライアントが表示されます。



これで、Nuclias Connect アプリが Nuclias Connect サーバにペアリングされました。アプリを使用して、プロファイルをローカルデバイスにダウン ロードし、その後、サポートされている DAP にプッシュすることができます。

### スタンドアロンアクセスポイントの検出と設定

#### ■ DAPの検出

Discover DAP 機能を使用すると、L2/L3 ワイヤレスネットワーク内の DAP デバイスを検出することができます。

1. 「Standalone Access Point」をタップします。



図 11-36 Nuclias Connect アプリ - トップ画面

- 2. L2 フィールドのボタンをタップして、L2 ネットワークで検出を有効にします。また、L3 フィールドのボタンをタップして、L2 ネットワーク で検出を有効にします。
- 3. 次に、「From」および「To」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。

	18 4G		9:39 AM		<b>e</b> 63% 🗖	D
<		Discov	er Access	s Point		
Discov	er stan s netw	idalone Acci orks	ess Points i	n L2/L3		
.2						)
.3						)
> Fr	m	192.168.1.	50 to	192.168.1.2	00	
		(+) Ad	d an IP Ra	ange		
			Discover			
		<u></u>	Discover			

- 4. 検出範囲を定義した後、「Discover」をタップして検出プロセスを開始します。または、ページの下部にある「Configure Access Point Profiles」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。詳細は「プロファイル設定(p.31)」を参照してください。
- 5. ネットワーク範囲のスキャンが終了すると、Step3の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。

6. DAP デバイスの横にあるラジオボタンをタップして選択します。選択済みのローカルプロビジョニングファイルが、選択したデバイスにプッシュ されます。「Push Provision」をタップして続行します。



7. DAP デバイスへのログインポップアップウィンドウが表示されます。画面上部に IP アドレスと MAC アドレスが表示されます。選択内容を確認 し、選択した DAP へのアクセスが許可されているユーザ名とパスワードを入力します。「Apply」をタップして続行します。



図 11-39 アクセスポイントへのログイン

8. ログインが成功すると、DAP インタフェースメニューが表示されます。「IP Info」「Wireless」「Client」タブが上部に表示されます。

項目	記明
キャンセル	タップして変更を破棄し、処理を続行します。
型名	表示されている DAP デバイスのモデル名が表示されます。
MAC	リストされている DAP デバイスの MAC アドレスを表示します。
DHCPモード	タップして、DHCP モード機能を有効または無効にします。有効にすると、DAP は許可されたクライアント接続で動
	的 IP アドレス設定を確立します。
IPアドレス	タップして IP ゲートウェイ設定を指定します。
サブネットマスク	タップしてサブネットマスクを指定します。
デフォルトゲートウェイ	タップしてデフォルトゲートウェイ設定を指定します。
DNS	タップして、DNS 設定を指定します。

「IP Info」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。



図 11-40 IP 情報の設定

「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
キャンセル	タップして変更を破棄し、処理を続行します。
DAP	AP デバイスのモデル名と IP アドレスが表示されます。
	2.4G SSID
SSID-#	スライドボタンをタップして、SSID を有効または無効にします。# の文字は、SSID の識別番号を示します。
SSID 名	タップして、SSID の現在の名前を変更します。
セキュリティ	タップして、特定のセキュリティプロトコルを選択します。
	・ 選択肢:「Open System(初期値)」「WPA-Personal」「WPA-Enterprise」
	5G SSID
SSID-#	スライドボタンをタップして、SSID を有効または無効にします。# の文字は、SSID の識別番号を示します。
SSID 名	タップして、SSID の現在の名前を変更します。
セキュリティ	タップして、特定のセキュリティプロトコルを選択します。
	・ 選択肢:「Open System(初期値)」「WPA-Personal」「WPA-Enterprise」
	ワイヤレス情報
無線帯域	タップして、特定の無線帯域を選択します。
	・選択肢:「Off」「2.4G」「5G」「2.4G/5G」
無線 2.4G モード	タップして、特定の 2.4G 無線モードを選択します。
	・ 選択肢:「Mixed 802.11n」「80211g and 802.11b」「Mixed 802.11g」「802.11b」「802.11n Only」
無線 5G モード	タップして、特定の 5G 無線モードを選択します。
	・ 選択肢:「Mixed 802.11n」「80211a」「802.11a Only」「802.11n」「Mixed 802.11ac」
国コード	DAP に割り当てられている国名を表示します。
設定の適用	タップして、検出された代替 DAP デバイスを選択し、現在の設定をプッシュします。
設定の保存	タップして、現在の構成プロファイルに名前を付けてアーカイブ保存します。

4	4:27 PM	99%
Cancel	DAP-2680	
IP Info	Wireless	Client
DAP-2680		<b>192.168.1.166</b> 40:9b:cd:0c:66:20
2.4G SSID		
SSID-1		
SSID Name		dlink
Security		Open System
SSID-2		0
SSID-3		0
5G SSID		
SSID-1		
SSID Name		dlinkiii
Security		Open System
SSID-2		
100000		-

\$	4:27 PM	99%
Cancel	DAP-2680	
IP Info	Wireless	Client
SSID-1		
SSID Name		dlinki
Security		Open Systen
SSID-2		0
SSID-3		0
Wireless Information	1	
Radio Band		2.4G 50
Radio 2.4G Mod	e Mixed 802.11n,	802.11g and 8
Radio 5G Mode		Mixed 802.11a
Country Code		United States
Copy & Save Config	uration	
Apply Configura	tion	
Save Configurat	ion	

図 11-41 ワイヤレス設定

# ネットワークプロファイルの削除

プロファイルを削除するには、以下の手順を実行します。

1. 左上のメニューをタップします。



2. 「AP Provision Profile」を選択します。



図 11-43 Nuclias Connect アプリ - メニュー項目

3. 対象のプロファイルを選択して削除します。



図 11-44 Nuclias Connect アプリ - プロファイル選択