Contended

ユーザマニュアル



● 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/product-assurance-provision

- 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

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

: 本マニュアルの対象者	
表記規則について	
第1章 製品概要	6
Nuclias Connect(DNC-100)について	6
サポート機能	6
推奨システム要件 Nuclias Connect 対応機器	7 7
	,
弗 2 卓 ソフトウェアのセットアップ	<u> </u>
Windows への Nuclias Connect インストール	
アットウェア のインベート かいいい Nuclias Connect サーバの実行	
Linux への Nuclias Connect インストール (リリース予定)	
ソフトウェアのインストール データベーフプロファイルの歌字	
テーダペースフロファイルの設定	
Nuclias Connect オンライン登録への初回ログイン	
アカウントの登録	
Nuclias Connect ハウロクイノアクティベーション	
Nuclias Connect アプリのセットアップ	
ネットワークプロファイルのエクスポート	
Nuclias Connect パフリケーションを使用した AP の検出と設定	
キッティック シンロシット (2005)が	
ファームウェアのアップロード	
<u>第3章 Nuclias Connect の管理インタフェース</u>	38
Nuclias Connect への接続	
ウィザード	
ユーザプロファイル	
個人情報 ヤキュリティ	
管理インタフェースからのログアウト	
第4章 ダッシュボード	43
第5章 モニター	44
アクセスポイント	
アクセスボイント - デバイス詳細	
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	
アクセスポイント - 隣接 AP	
ヘイッテ	
基本タブ	
ポートタブ	
IP インタフェースタフ	
電源タブ	
ツールタブ	61
スイッチ - スイッチクライアント	
用り草 トホロン	68
<u>第7章 フロア計画</u>	
第8章 設定	73
プロファイルの作成	
ネットワークの追加 プロファイル設定	74 74
アクセスポイント - SSID	
ネットワークの追加 プロファイル設定アクセスポイント - SSID	

եը

Je,

1	
・ アクセスポイント - VLAN	
アクセスポイント - 帯域幅の最適化	
アクセスポイント - RF 最適化	91
アクセスポイント - スケジュール	
アクセスポイント - デバイス設定	
アクセスポイント - パフォーマンス設定	
アクセスポイント - WLAN パーティション	
アクセスポイント - ワイヤレスリソース	
スイッチ - 一般 - RADIUS サーバ	
スイッチ - 一般 - 時間プロファイル	
スイッチ - 基本	
スイッチ - IPv4 ACL	
スイッチ - アクセスポリシー	
スイッチ - ポート設定	
スイッチ - SNTP 設定	
ファームウェアの更新	
SSL 証明書	
決済代行システム ※本項目は日本ではサポート対象外となります。	
	115
第9章 レホート	115
アクセスポイントのレポート	
ピークネットワークアクティビティ	
時間別ネットワークアクティビティ	
日別ネットワークアクティビティ	
最もアクティブな AP	
スイッチのレポート	
時間別ネットワークアクティビティ	
日別ネットワークアクティビティ	
トップランキング	
<u>第10章 ログ</u>	122
デバイスシスログ	122
システムイベントログ	123
デバイスログ	124
アン・コン・コン・コン・コン・コン・コン・コン・コン・コン・コン・コン・コン・コン	125
	125
	120
<u> 弗 草 ジステム官埋</u>	127
デバイス管理	
ユーザ管理	
ユーザステータス	
ユーザ権限	
設定	
一般	
接続	
SMTP	
バックアップ&リストア	
REST API	
シングルサインオン(SSO)	
アラート	138
FOTA	139
リソース	139
Nuclias Connect について	
【11」「球】 「	141

"Lpi

rБ

cŀ

本マニュアルの対象者

本マニュアルは、本サービスの管理についての情報を記載しています。また、ネットワーク管理の概念や用語に十分な知識を持っているネットワー ク管理者を対象としています。

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。



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。

第1章 製品概要

- 「Nuclias Connect (DNC-100) について」
- 「サポート機能」
- 「推奨システム要件」
- 「Nuclias Connect 対応機器」

Nuclias Connect (DNC-100) について

Nuclias Connect は、D-Link Nuclias Connect 対応アクセスポイントを管理するための、フリーの Wi-Fi 集中管理ツールです。本製品は、Web ベース の中央 AP 管理ユーティリティであり、管理者が無線ネットワークを容易かつ効率的に管理および監視するために、キャプティブポータル、自動 RF 管理、および帯域幅最適化などをサポートします。

サポート機能

- Windows、Linux^{*1}のサポート
- 最大 1500AP 管理 / サーバ
- ・ https エージェントを使用した NAT パススルー (NAT デバイスの後方にある複数の AP を管理可能)
- AP と Nuclias Connect 間のすべてのトラフィックを暗号化
- ・ 日本語 GUI のサポート
- ・ コンフィグレーション / ログのバックアップと復元
- ・スケジューリングによるプロファイル/ファームウェア更新
- Web による管理(HTTPS)
- ・ Syslog サーバ^{** 2}
- ・ 外部 Syslog サーバ^{** 3}
- 同一ネットワーク上の AP 検出
- ・ セットアップウィザード
- Nuclias Connect モニタ対応アプリ
- AP/ クライアントの上位使用状況表示
- ・ レポート

※ 1 Linux は対応予定

※2本機が管理しているデバイスから送信されるログを受信する Syslog サーバとしての機能となります。

※3キャプティブポータルログのみ対応

ビジネス Wi-Fi 機能

- ・ キャプティブポータル:AP では内部データベース、リモート RADIUS、POP3、パスコード認証をサポートします。
- キャプティブポータルページのカスタマイズ
- ・ ホットスポットプリンティング
- ・ キャプティブポータル
- ・ マルチ SSID
- ・ SSID ごとの VLAN
- ・ スケジューリングによる無線のオン / オフ
- ・ 5GHz 優先(バンドステアリング)
- エアタイムフェアネス
- 自動 RF 管理
- 帯域幅の最適化
- クライアントのアクセスコントロール

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

推奨システム要件

D-Link Nuclias Connect は、管理者がネットワーク全体のワイヤレスデバイスを中央から管理するための、汎用性のある便利なソフトウェアソリューションです。

項目	大規模環境	小規模環境
最大管理アクセスポイント数	1500 台	100 台
推奨 CPU	8 世代 Intel® Core ™ i7 プロセッサ以上	Intel® Core™i5 プロセッサ 3.2 GHz 以上
推奨 RAM	24G DDR3 以上	8G DDR3 以上
推奨ストレージ容量	4TB 以上	2TB 以上
イーサネット NIC	ギガビットイーサネットカード	ギガビットイーサネットカード
モニタ解像度	1080p	1080p
プラットフォーム (Windows)	Windows 10 Professional または Windows Server 2016 (64-bit)	Windows 10 Professional (64-bit)
プラットフォーム (Linux*)	Ubuntu、CentOS 7	Ubuntu、CentOS 7
Nuclias Connect 管理用ブラウザ	Edge、Chrome、Safari	Edge、Chrome、Safari
推奨アップリンク帯域幅	20Mbps以上	10Mbps 以上

※ 対応予定。Linux プラットフォームでのインストールには、Docker および Docker Compose ツールセットが必要です。

Nuclias Connect 対応機器

Nuclias Connect では以下の機器をサポートしています。

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

※ Nuclias Connect に対応したファームウェアバージョンにおいて CWM は利用できません。

第2章 ソフトウェアのセットアップ

- 「Windows への Nuclias Connect インストール」
- 「Linux への Nuclias Connect インストール (リリース予定)」
- 「Nuclias Connect オンライン登録への初回ログイン」
- 「Nuclias Connect アプリのセットアップ」

本章では、Nuclias Connect アプリケーションを正常に実行するためにインストールする必要があるソフトウェアについて説明します。

次のソフトウェア・アプリケーションは、以下の順序でインストールする必要があります。

- Nuclias Connect サーバアプリケーション: 無線ネットワークの日常的な管理・保守タスクを担当するメイン・アプリケーションです。詳細 については、「Windows への Nuclias Connect インストール (p.8)」、「Linux への Nuclias Connect インストール (リリース予定) (p.16)」 および「第3章 Nuclias Connect の管理インタフェース (p.38)」を参照してください。
- Nuclias Connect アプリケーション:スタンドアロンの D-Link AP 製品への簡単な設定および展開、また、複数のサイトやネットワークの管理を可能にする無線アクセスポイント管理ツールです。詳細については、「Nuclias Connect アプリのセットアップ(p.26)」を参照してください。

Windows への Nuclias Connect インストール

ソフトウェアのインストール

以下の手順を参照して Nuclias Connect ソフトウェアをインストールします。

注意 この作業を始める前に、D-Link Japan のサイトから最新の Nuclias Connect を入手してください。

注意 ソフトウェアを再インストールする場合、NC、Mongo DB、および WinPcap の全てを アンインストールし、新規に Nuclias Connect をイ ンストールする手順を推奨します。

Npcap のインストール

Nuclias Connect ソフトウェアをインストールする前に、Npcap をインストールする必要があります。

1. 以下のサイトから NPcap v1.70 をインストールします。 https://nmap.org/npcap/dist/npcap-1.70.exe

注意

Npcap のバージョンは v1.70 をインストールしてください。

2. 使用許諾に同意します。

Npcap 1.70 Setup	~	⊐ ×
NMAP. ORG	License Agreement Please review the license terms before installing Npcap	1.70.
Press Page Down to see t	he rest of the agreement.	
NPCAP COPYRIGHT / EN	D USER LICENSE AGREEMENT	^
Npcap (https://npcap.co library and is copyright (e Project"). All rights reser Even though Npcap sour not open source softwar	m) is a Windows packet sniffing driver and c) 2013-2022 by Nmap Software LLC ("The Nmap rved. ce code is publidy available for review, it is e and may not be redistributed or used in other participant from the Nmap Project The	
standard (free) version is	s usually limited to installation on five	~
If you accept the terms o agreement to install Npca	f the agreement, dick I Agree to continue. You must accep p 1.70.	t the
	I Agree	Cancel

図 2-1 Npcap - 使用許諾

3. デフォルトオプションのまま「Install」をクリックします。

😚 Npcap 1.70 Setup	- 🗆 🗙
MMAP. ORG	Installation Options Please review the following options before installing Npcap 1.70
Restrict Npcap drive	's access to Administrators only
Support raw 802.11	raffic (and monitor mode) for wireless adapters
🗹 Install Npcap in Winl	cap API-compatible Mode
Nullsoft Install System V3.07	
	< Back Install Cancel
図 2-2 Npcap - イン	

4. 「Next」をクリックします。

🍞 Npcap 1.70 Setup				
MMAP, ORG	Installation Complete Setup was completed successfully.			
Completed				
Show details				
Nullsoft Install System v3.07 -				
	< Back	lext >	Can	cel

図 2-3 Npcap - インストール完了

5. 「Finish」をクリックしてウィザードを終了します

😚 Npcap 1.70 Setup			_		\times
MMAP, ORG	Finished Thank you for installing Npca	ap			
Npcap has been install	ed on your computer.				
Click Finish to close thi	s wizard.				
Nullsoft Install System v3.07					
realized in scale system (19,07	< Back	Finish		Cance	3
図 2-4 Npcap - ウィ	ザード完了				

Nuclias Connect のインストール

- 6. Nuclias Connect パッケージのファイルを実行してインストールプロセスを開始します。
- 7. 「Welcome」画面が表示されるので、「Next>」ボタンを選択して続行します。インストールを中止して終了するには、「Cancel」ボタンをクリックします。

Nuclias connect 1.2.0.9b1 S	Setup — 🗆 🗙
P-Link	Welcome to the Nuclias connect 1.2.0.9b1 Setup Wizard This wizard will guide you through the installation of Nuclias connect 1.2.0.9b1. It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer. Click Next to continue.
	Next > Cancel

図 2-5 Nuclias Connect - セットアップウィザード

8. 「License Agreement (使用許諾)」画面が表示されます。インストールする前に、ライセンス条項を確認してください。同意後に「I Agree (同意する)」ボタンをクリックして続行します。



9. 「Choose Destination Location」 画面が表示されます。別のフォルダまたは別のドライブに Nuclias Connect をインストールするには、「Browse…」 ボタンをクリックしてフォルダを指定します。

「Next>」ボタンをクリックして次の手順に進みます。前の画面に戻る場合は「<Back」ボタンをクリック、インストールを中止して終了するに は、「Cancel」ボタンをクリックします。

Nuclias connect 1.2.0.9b1 Setup	—		×
Choose Install Location Choose the folder in which to install Nuclias connect 1.2.0.9b1.			<n< td=""></n<>
Setup will install Nuclias connect 1.2.0.9b1 in the following folder. To ir folder, click Browse and select another folder. Click Next to continue.	nstall in a	<mark>different</mark>	
Destination Folder C:¥Program Files (x86)¥Nuclias connect	Bro	wse	
Space required: 256.0MB Space available: 116.4GB			
< Back Nex	kt >	Can	icel

図 2-7 Nuclias Connect - インストールフォルダの指定

10. 以下の画面では、必要に応じて「Web Port(初期値:30001)」と「CoreServer Port(初期値:8443)」を入力します。アクセスポイント接続に 使用されます。初期値のポートが利用可能である場合は、そのまま初期設定を使用します。

「Next>」ボタンをクリックして次の手順に進みます。前の画面に戻る場合は「<Back」ボタンをクリック、インストールを中止して終了するには、「Cancel」ボタンをクリックします。

Nuclias connect will Listening Port, Click	listen the following	port. To liste	en to a differ	ent port, r	modify the	
Listering Forth Circle						
Port Settings						
Web Port:	30001					
Care Carrier Darts	0.440					
Coreserver Port:	8443					
Port check pass!					Check	

図 2-8 Nuclias Connect - ポート設定

11.「Database Service Environment Check」画面が表示されます。ここでは、必要な MongoDB データベースサービスのシステムチェックが実行されます。「MongoDB status summary」セクションにレポートが表示され、サービスがインストールされている場合は、MongoDB のバージョンとステータスが表示されます。

Nuclias Connect が正しく機能するには、データベースサービスが必要です。サーバ上またはリモートで既存の MongoDB を利用する場合は、「Use an existing MongoDB」、新規のサービスをインストールする場合は「Install a new MongoDB」を選択します。

「Next>」ボタンをクリックして次の手順に進みます。前の画面に戻る場合は「<Back」ボタンをクリック、インストールを中止して終了するに は、「Cancel」ボタンをクリックします。

ecking MongoDB database service requin	ed by the Nuclias connect.
MongoDB status summary	
A Service named " MongoDB ":	Not installed
MongoDB service running status:	Not running
The running MongoDB version:	4.0.18
Nuclias requires a database service provi a new MongoDB 4.0.17, the installation as a MongoDB service on the server. If y you can let Nuclias to connect a remote N Install a new MongoDB 4.0.17	ded by MongoDB 4.0.17. So if you choose 'Inst will try to install MongoDB 4.0.17 and register it ou choose 'Use an existing MongoDB 4.0.17', MongoDB service. Use an existing MongoDB 4.0.17

12.「MongoDB Database Configuration」画面が表示されます。この画面で、本アプリケーションに関連付けられる MongoDB リスニングポート(デフォルト:27010)、ユーザ名、およびパスワードを指定します。

「Next>」ボタンをクリックして次の手順に進みます。前の画面に戻る場合は「<Back」ボタンをクリック、インストールを中止して終了するに は、「Cancel」ボタンをクリックします。

Specify the database	listening port, username and password
MongoDB Port:	27010
User name:	
Password:	

図 2-10 Nuclias Connect - MongoDB データベース設定 インストールボタンでは?新規インストールで再確認

補足

コンピュータのファイアウォールによって Apache HTTP Server アプリケーションがブロックされる場合があります。サーバが Windows ファ イアウォールを使用している場合は、セキュリティ警告メッセージが表示されます。「アクセスを許可する」をクリックして、アプリケーショ ンがネットワークと通信できるようにします。

福足「Windows セキュリティの重要な警告」画面に、サーバーサイド JavaScript などの特定の機能のインストールがブロックされていることを示す警告が表示される場合があります。ポップアップ画面が表示された場合は、ファイアウォールアクセスに最適なネットワーク(「プライベート ネットワーク」)を選択し、「アクセスを許可する」をクリックします。それ以外の場合は、「Cancel」をクリックしてインストールプロセスを中止します。

 Nuclias Connect サービスがインストールされると、「Installation Complete」画面が表示されます。「Next>」ボタンをクリックして次の画面に 進みます。

Nuclias connect 1.2.0.9	b1 Setup				
stallation Complete					
etup was completed suc	cessfully.				S
Completed					
(NO	T_STOPPABLE, NOT	T_PAUSABLE, IGNOF	ES_SHUTDOWN	()	^
WIN32_EXIT_COD	E :0 (0x0)				
SERVICE_EXIT_CO	DE : 0 (0x0)				
CHECKPOINT	: 0x0				
WAIT_HINT :	0x7d0				
PID : 249	04				
FLAGS :	anten en				
Start Nuclias connect W	eb server successfi	ully.			
Create shortcut: C:¥Pro	gramData¥Microsof	ft¥Windows¥Start M	enu¥Programs¥l	Nuclia	

図 2-11 Nuclias Connect - インストール完了

14. Nuclias Connect セットアップウィザードの完了画面が表示されます。「Finish」をクリックします。



15. 既定のブラウザで Nuclias Connect に接続されます。

この接続ではプライバシーが保護されません localhost では、悪意のあるユーザーによって、パスワード、メッセージ、クレジット ードなどの情報が盗まれる可能性があります。詳細 NET-ERR_CERT_AUTHORITY_INVALID Chrome の最高レベルのセキュリティで保護するには、保護強化機能を有効に してください。	この接続ではプライバシーが保護されません localhost では、悪意のあるユーザーによって、パスワード、メッセージ、クレジット、 ードなどの情報が盗まれる可能性があります。詳細 NET-ERR_CERT_AUTHORITY_INVALID Chromeの最高レベルのセキュリティで保護するには、 <u>保護強化機能を有効に してください</u> 。	A	
Iocalhost では、悪意のあるユーザーによって、パスワード、メッセージ、クレジット ードなどの情報が盗まれる可能性があります。詳細 NET-ERR_CERT_AUTHORITY_INVALID	Iocalhost では、悪意のあるユーザーによって、パスワード、メッセージ、クレジット ードなどの情報が盗まれる可能性があります。詳細 NET-ERR_CERT_AUTHORITY_INVALID	この	接続ではプライバシーが保護されません
NET:ERR.CERT_AUTHORITY_INVALID Chrome の最高レベルのセキュリティで保護するには、保護強化機能を有効に してください。	NET-ERR_CERT_AUTHORITY_INVALID Chrome の最高レベルのセキュリティで保護するには、 <u>保護強化機能を有効に してください</u> 。 詳細設定 詳細設定	localho ードな	st では、悪意のあるユーザーによって、パスワード、メッセージ、クレジット: どの情報が盗まれる可能性があります。 <u>詳細</u>
Chromeの最高レベルのセキュリティで保護するには、保護強化機能を有効にしてください。	 Chrome の最高レベルのセキュリティで保護するには、保護強化機能を有効に してください。 詳細設定 	NET::ERR	_CERT_AUTHORITY_INVALID
	詳細設定	Ō	Chrome の最高レベルのセキュリティで保護するには、 <mark>保護強化機能を有効に</mark> してください。
詳細設定 セキュリティで保護されたページに戻		詳細調	セキュリティで保護されたページに戻る

図 2-13 Nuclias Connect への接続



参照 ソフトウェアインストール後の Nuclias Connect セットアップやログイン手順については、「Nuclias Connect オンライン登録への初回ログ イン (p.20)」を参照してください。

をクリックして

<n Nuclias connect Service Configurator

Nuclias Connect サーバの実行

インストールが完了すると、プログラム一覧にアプリケーションが表示されます。



図 2-14 Windows ショートカットメニュー

注意

以下の手順は、Windows10オペレーティングシステムに基づいて記載されています。画面や手順などは、お使いのオペレーティングシステムによって異なる場合があります。

デスクトップから、スタート > すべてのプログラム > Nuclias Connect の順に移動し、

Nuclias Conr	nect	
1.2.0.9b1		sn
Restart Services	Stop Services	
Launch a Browser t	o Manage the Network	
Copyright(C)2018-2022	? D-Link. All Rights Reser	rved.

⊠ 2-15 Nuclias connect Setup

■ サービスの有効化 / 無効化

Nuclias Connect を管理するには、最初にサービスを有効にする必要があります。「Restart Services」ボタンをクリックして Nuclias サーバのサービスを有効化、または「Stop Services」ボタンをクリックしてサービスを無効化します。

■ 管理インタフェースへの接続

Nuclias Connectの管理インタフェースには、ブラウザ画面からアクセスできます。「Launch a Browser to Manage the Network」をクリックしてデフォルトのブラウザを開きます。

Linux への Nuclias Connect インストール (リリース予定)

ソフトウェアのインストール

以下の手順を参照して Nuclias Connect ソフトウェアをインストールします。

- 注意 この作業を始める前に、D-Link Japan のサイトから最新の Nuclias Connect を入手してください。(リリース予定)

注意 ソフトウェアを再インストールする場合、NC、Mongo DB、および WinPcap の全てを アンインストールし、新規に新しい Nuclias Connect をインストールする手順を推奨します。

注意 この例では、tar パッケージ(nuclias-connect.tar.gz)がアーカイブ形式(GZ)でデスクトップにダウンロードされているものとします。

■ Nuclias Connect パッケージの展開

- デスクトップから Ctrl+Alt+T を押してターミナルウィンドウを起動します。ターミナルウィンドウから、ダウンロードした tar パッケージの場 1. 所に移動します。この例では、パッケージはデスクトップにあります。
- ディレクトリを変更するコマンドを入力します。 2.

\$ cd Desktop

3. 正しいディレクトリに移動したら、ls コマンドを使用して、ディレクトリ内の使用可能なファイルのリストを表示します。パッケージを展開す るには、次のコマンドを入力します。

:~/Desktop\$sudo tar xvzf nuclias-connect.tar.gz

このコマンドは、パッケージの内容を展開します。以下の結果が表示されます。 4

```
Nuclias_connect/
Nuclias connect/docker-compose.yml
Nuclias_connect/config/
Nuclias connect/config/key/
Nuclias connect/config/key/ca-cert.pem
Nuclias_connect/config/key/openssl.cnf
Nuclias connect/appconfig.json
Nuclias_connect/images
Nuclias connect/images/mongo.tar
Nuclias_connect/images/core.tar
Nuclias_connect/images/web.tar
Nuclias_connect/entrypoint-initdb.sh
```

5. これで、Nuclias Connect パッケージが展開され、インストールの準備が整いました。init.sh ファイルを含むディレクトリに移動します。次の コマンドを入力して、Nuclias Connect パッケージを初期化します。必要に応じてユーザ名とパスワードを入力します。

\$ cd Desktop ~/Desktop\$ cd nuclias connect ~/Desktop/nuclias_connect\$ sudo ./init.sh 6. バイナリが実行され、次の結果が表示されます。

########## Welcome to Nuclias Connect ####################################
- $(1/(11))$ about our duator time
SYSTEM: Linux Ubuntu
-e check system finished
-e (2/11) check docker
Docker version 18.09.6, build 481bc77
-e docker installed
-e (3/11) check docker-compose
docker-compose version 1.23.1, build b02f1306
-e docker-compose installed
-e (4/11) check docker status
-e docker sevice is running
-e (5/11) check core image
message: 2
-e core image is existed
-e (6/11) check web image
message: 2
-e web image is existed
message 2
-e mongo image is existed
-e (8/11) check web port
message: 0
-e web_port is free
-e (9/11) check core_port
message: 0
-e core_port 1s free
-e (11/11) check file and directory
-e check file finished
-e all check_job finished
-e Now initial set the database administrator account for Nuclias Connect, please
confirm is the first time set administrator account? $[y/n]$

Nuclias Connect の初期化が行われると、データベース管理者アカウントの設定を要求するプロンプトが表示されます。データベースを初めて使用 する場合は、アカウントのデータベース管理者を設定する必要があります。

データベースプロファイルの設定

1. 初めて使用する場合は、最初にデータベース管理者を設定する必要があります。Nuclias Connect の初期化では、次のような画面が表示されます。

-e Now initial set the database administrator account for Nuclias Connect, please confirm is the first time set administrator account? [y/n]

2. 「Y(はい)」を入力して、管理者アカウントとパスワードを設定します。プロンプトで、管理者ユーザ名とパスワードを入力します。次の例では、 変数 admin が両方のインスタンスに使用されています。

3. Mongo DB、Core、および Web コンテナの設定が完了し、Web ブラウザを使用して Nuclias Connect を起動できるようになります。

サーバ IP アドレスの検索

Nuclias Connect に接続するには、以下の手順に従います。

- 1. デスクトップから Ctrl+Alt+T を押してターミナルウィンドウを起動します。
- コンソールで、Nuclias Connect パッケージを含むディレクトリに移動します。次の例では、nuclias_connect フォルダがソフトウェアの場所を 示しています。

\$ cd Desktop ~/Desktop\$ cd nuclias_connect

3. 次のコマンドを入力して、Nuclias Connect インスタンスの定義済み IP アドレスを取得します。

~/Desktop/nuclias_connect\$ ip addr

4. 結果が次のように表示されます。Web ブラウザで使用する IP アドレスは以下のメッセージ内で確認できます。この例では、インスタンスのアドレスは 172.17.5.47 です。

1: lo: <LOOPBACK, UP, LOWER UP> mtu 65536 qdisc noqueue state UNKNOWN group t glen 1000 Link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00 Inet 127.0.0.1/8 scope host lo Valid_lft forever preferred_lft forever Inet6 ::1/128 scope host Valid lft forever preferred lft forever 2: enp3s0f2: <BROADCAST, MULTICAT, UP,LOWER_UP> mtu 1500 qdisc fq_codel state up group default qlen 1000 link/ether 30:65:ec:25:be:3b brd ff:ff:ff:ff:ff inet 172.17.5.47/24 brd 172.17.5.255 scope global dynamic noprefixroute ip3 sof2 valid_lft 22085sec preferred_lft 22085sec inet6 fe80::c3a8:bcbd:6cda:4dc3/64 scope link noprefixroute valid lft forever preferred lft forever 3: wlp2s0: <NO-CARRIER, BROADCAST, MULITCAST, UP> mtu 1500 qdisc noqueu state DOWN group default qlen 1000 link/ether a4:db:30:cb:36:0e brd ff:ff:ff:ff:ff 4: docker0: <NO-CARRIER, BROADCAST, MULITCAST, UP> mtu 1500 qdisc noqueu state DOWN group default glen 1000 link/ether 02:42:11:ff:39:9f brd ff:ff:ff:ff:ff:ff inet 172.18.0.1/16 brd 172.18.255.255 scope global docker0 valid lft forever preferred lft forever

上記のインタフェースセッションでは、Nuclias Connect の IP アドレス(172.17.5.47)を確認することができます。これは、Web ブラウザを介して Nuclias Connect インタフェースにアクセスするために使用する IP アドレスです。

これで、Linux 環境への Nuclias Connect インストール処理が完了しました。Web ブラウザを介して Nuclias Connect にアクセスするためのコアコ ンテナが用意されました。Nuclias Connect インタフェースを開始するには、「Nuclias Connect サーバへの接続(p.31)」を参照してください。

コアコンテナと MongoDB プロファイルが設定されている場合は、Web ブラウザから Nuclias Connect にアクセスすることができます。 Web ブラウザを使用して Nuclias Connect にアクセスするために定義された IP アドレスを取得するには、「サーバ IP アドレスの検索(p.19)」を 参照してください。

Nuclias Connect オンライン登録への初回ログイン

Nuclias Connect では、30 日間のトライアル期間を提供しています。register.nuclias.com で Nuclias アカウントを登録すると、継続して本ソフトウェ アを使用することができます。アカウント登録画面には、Nuclias Connect 管理インタフェース右上の**クリックしてアクティベート > アカウント登** 録から遷移することもできます。

< nuclias connect
Nuclias Connect is offered as a 30-days trial. If you want to continue using Nuclias Connect beyond this period, simply register your details using the link below to activate Nuclias Connect
Your E-mail
Your password
No account? Register now Back Next
© 2019 D-Link Corporation English 🧹
図 2-16 Nuclias Connect 初回ログイン

アカウントの登録

登録プロセスが初期化されると、新しいブラウザ画面が開き、サーバ登録ページが表示されます。以下の手順を参照し、登録を行います。

1. 地域を「Asia」、国を「Japan」に設定し、「次」をクリックします。

•	-0-	(
ステップ1 サーバの地域、[国を選択してください。	
	4 mu alian	
		k
新しいアカウ: されます。カ; す。	ントと組織は、選択した地域内 スタマーサービスは選択された	回のサーバーに作成 E国に転送されま
サーバの地	域	
Asia		
国		
Japan		•
	次	
既に	アカウントをお持ちですか?	ログイン
0.47		



すでにアカウントをお持ちの場合は、そのアカウントを使用してログインすることができます。新しいアカウントを作成する必要はありま せん。 2. アカウント情報(ユーザ、組織、住所など)の入力画面が表示されます。必要な情報を入力し、利用規約およびプライバシーポリシーに同意し ます。アカウント作成ボタンが有効になります。

	S
ЕХ-Л	
フルネーム	
パスワード	0
新しいパスワードの確認	0
組織名	
Japan	
Asia/Tokyo(UTC+09:00, DST)	•
住所	
 ○ 私はこれらを全て読み、同意します。 プライバシー □ p-Link製品のアップデートやオファー せします。 	: <u>利用規約</u> 並びに をメールでお知ら
私は人間です	hCaptcha ブライバシー。各項

- 3. 入力後、CAPTCHA 認証を行い、「アカウントの作成」をクリックします。
- **4.** アカウント作成後、登録したメールアドレスへ Nuclias(verify@nuclias.com)から認証メールが送信されます。メール内に記載されたアクティ ベーション用の URL をクリックし、Nuclias アカウントのアクティベーションを行ってください。
- 5. 認証完了後、ログインページにリダイレクトされます。Nuclias Cloud 対応デバイスがない場合は、本手順を省略できます。

D-Link
0
/
アカウントの作成

Nuclias Connect へのログイン

Nuclias Connect には複数のログイン方法が用意されており、ローカルコンピュータにインストールされた Nuclias Connect ソフトウェアを利用する 方法と、リモートコンピュータからブラウザ(Edge または Chrome 推奨)を利用する方法があります。

ブラウザから直接接続する方法(Windows/Linux)

ブラウザを開き、Nuclias サーバを実行しているホストコンピュータの IP アドレスまたはドメイン名(https://172.17.5.47:30001 や https://domainname.com など)を入力します。



Nuclias Connect サーバへの接続を確立すると、プライバシーエラーメッセージが表示される場合があります。この場合、「172.17.5.47 に アクセスする(安全ではありません)」を選択して Nuclias Connect ポータルを開きます。

ソフトウェアから接続する方法(Windows)

ローカルにインストールされたソフトウェアの場合は、Nuclias Service Configurator または Nuclias Connect のショートカットを使用して、ブラウ ザでインタフェースを起動することができます。

- 1. デスクトップから、スタート > すべてのプログラム > Nuclias Connect の順に選択し、 いuclias connect Service Configurator をクリックして Nuclias Connect Setup 画面を起動します。
- 2. 「Nuclias Connect」画面で、「Launch a Browser to Manage the Network」をクリックすると、既定のブラウザが起動し、Nuclias Connect イン タフェースが表示されます。

🚇 Nuclias connect Setup	– 🗆 X
Nuclias Connect	
1.2.0.9b1	<u>sn</u>
Restart Services Stop Services	
Launch a Browser to Manage the Network	
Copyright(C)2018–2022 D–Link. All Rights Reserve	d.
図 2-20 Nuclias Connect Setup 画面	

または、次の方法でインタフェースに直接アクセスすることも可能です。

 デスクトップから、スタート>すべてのプログラム> Nuclias Connect の順に選択し、 い Nuclias connect をクリックしてデフォルトの Web ブラウザを開きます。

http://1/2.1/.	,4/130001	
	<nuclias< th=""><th></th></nuclias<>	
	ログインアカウント 11本語 -	
	あたたのユーザーネーム	
	キャプチャを入力してください 5 279 パスワードを忘れた場合	
	₽ <i>₫</i> 4.У	
	© 2018-2022 D-Link Corporation. All rights reserved. Terms of Service Privacy Policy	

図 2-21 Nuclias Connect ログイン画面

3. ログイン画面で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。

< nuclias connect	
ログインアカウント	□本語 ~
あなたのユーザーネーム	
ペスワード	
キャプチャを入力してください 5 279	パスワードを忘れた場合
₽ <i>9</i> 4.9	
© 2018-2022 D-Link Corporation. All ri Terms of Service Privacy Policy	ghts reserved.

補足

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

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

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

最初にログイン 要があります	した後、パスワードを変更する必
メルーの ク み ラ 。	は、小文字と大文字のアルファベット文字と数字を含む8
30文字である必要があり	ます。
Old password	
New password	
Confirm personal	
Commin pissword	

図 2-23 パスワードの変更

注意 一般的な単語や名前は使用しないでください。

現在のパスワードを「old password」フィールドに入力し、「new password」フィールドに新しいパスワードを入力します。 「confirm password」フィールドに同じパスワードを入力して、入力内容を確認します。「変更」をクリックして処理を完了します。 5. 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。デバイスアクセスアドレスまたはポートを変更 した場合は、Nuclias Connect Core サーバを再起動する必要があります。

デバイスアクセスアドレス	その他・・
デバイスアクセスポート	8443
Jaj	Afghanistan
タイムゾーン	(GMT-12:00) International Date Line West $\qquad \lor$



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。

アクティベーション

Nuclias Connect は 30 日間の試用期間で提供されています。引き続き使用するには、以下の手順にてアクティベーションを行う必要があります。

1. 画面右上の「試用 (x 日)、クリックしてアクティベート」をクリックします。

∢nuclias	Default 説明 (6日)、クリックレズアクティベート 🔍 💉 JP
(k) ダッシュボード	
100 H = 2 A	15-30 15-45 16-00 16-15 16-30 16-30 16-30 16-30 16-30 16-30
ト ポロジ	\$\u03c9 \u03c9
● フロア計画	
🗙 設定 🔷	チャネル利用数
□ レポート →	2.4 GHz $\neq \star \div \star \odot \Delta P$
- - - - - - - - - - - - - - - - - - -	20
50 VX74 >	
図 2-25 アク	ティベート

2. 以下の画面が表示されます。アカウント情報を入力して、「次へ」をクリックします。

🖹 アクティベーション				×
Nuclias Com この期間を責 は、以下の! Connect を有	uect は、30日間の えてNuclias Com ンクを使用して言 効にしてください	試用版として提 nect を引き続き(羊細情報を登録し [^] 。	供されています。 更用したい場合 て、Nuclias	
メールア	¢νд			
パス	7 — F			
	アカウントがあり)ませんか? すぐに	登録	
			次~	終了

図 2-26 アカウント情報の入力

3. アクティベーションのために必要な情報を入力して、「適用」をクリックします。

>
D情報を入力してくだ
利用 🔿 お客様用
Pick one v
Pick one ~
適用 終了

図 2-27 管理情報の入力

項目	説明
どのように Nuclias Connect	Nuclias Connect の用途を選択します。
を使用しますか?	・ 選択肢:[個人利用][お客様用]
何人で使用しますか?	部署内の人数を指定します。
	・選択肢:<10, 10-50, 50-100, >100
何台の AP を管理する予	管理対象のアクセスポイント数を指定します。
定ですか?	・選択肢:<20, 20-50, 50-100, 100-500, >500
いくつのサイトを管理	管理するサイト数を入力します。
する予定ですか?	

以上でアクティベーションは完了です。「OK」をクリックして画面を閉じてください。

🖹 アクティベーション	×
Nuclias Connect は14/Jan/2020 18:12:39にアクティベートされました。	_
	ОК

図 2-28 アクティベーションの完了

Nuclias Connect アプリのセットアップ

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

このセクションでは、接続されたアクセスポイントを管理するために必要なネットワークプロファイルを Nuclias サーバからエクスポートする方法 について説明します。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(サーバ)の認証キーと IP アドレスが含まれます。

参照 Nuclias Connect 管理インタフェースから同一セグメント内のデバイスを検出する場合、本手順は不要です。ネットワークおよびデバイスの検出手順については、「ネットワークの追加(p.74)」を参照してください。

- 1. 設定 > プロファイルを作成の順にクリックします。
- 「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< th=""><th>Default</th><th></th><th></th><th></th><th></th><th></th><th>10:36:23</th><th>2023-03-08</th><th>😍 🔀 JP ~</th></nuclias<>	Default						10:36:23	2023-03-08	😍 🔀 JP ~
ダッシュポード	全てのサイト・、		7 合計2ネットワーク	クセスポイント:合計	1/1オンライン スイ	ッチ:合計1/1オン	ノライン		ネットワークを追加
1417 €=Ø →				9472F:374FU		472 Fister 2 3	5		
	サイト名 🔺	▼ ネットワーク名 ▲	× ネットワークID×	合計デバイス >	オンラインデバマ	クライアント	✓ プロファイル	検出	アクション
	Site1	Network1		0	0	0	e o e	9,	Ľ ū
A 10 10 10 10	Site2	Network2		2	2	23	e o e	9	2 ô
🗙 ikiz 🔹 🗸									
 プロファイルを作成 									
 プロファイル設定 									
• ファームウェアの更新									
 SSL证明書 									
 決済代行システム 									
レポート >									
⊑ ¤% →									
50 >X74 >									

図 2-29 設定 - 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。

<nuclias< th=""><th>Default 12:55:42 2023-03-08 🤌 🔍 JP 🗸</th></nuclias<>	Default 12:55:42 2023-03-08 🤌 🔍 JP 🗸
ダッシュポード	一般 接続 SMTP パックアップ&リストア RESTAPI シングルサインオン(SSO) アラート FOTA
100 E=9 >	
▶ ポロジ	REAL
◎ フロア計画	デバイスアクセスアドレス 172.16.150 V このアドレスを変更する場合、必要に応じてデバイスを手動で提出して管理して
🗙 設定 🔹 >	(20).
	デバイスアクセスポート 8443 このボートを変更する場合、でくiProgram Files (366)/Xudias connect(Core)confly/appconfly/json*~も移動してポート番号を変更し、サーバを得起 動してください、その後、必要にはじて手動でデバイスを再移出し、常用してください。
5 E / >	コブサーバアクセスポート 8443
 デバイス管理 	Webアクセスポート 30001 ブラクザからアクセスできる有効なポートであることを確認してください。
 ユーザ管理 設定 	與 作
 リソース Nuclias Connectについて 	SSLā(4)]. [7.4-12] fr
	証明能をアップロービー ブラウザ
	キーをアップロード ブラウザ
	α <i>θ</i>

図 2-30 システム - 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、スタンドアロンのアクセスポイントを Nuclias Connect にすばやくデプロイしたり、 D-Link アクセスポイントを検索したり、アクセスポイントの個別設定を行ったりすることができます。

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

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

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

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

クイックセットアップ

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

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



図 2-31 Nuclias Connect アプリ(iOS)

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

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

ステップ1:プロビジョニングプロファイルの選択

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

1475 10 64 (49)		· · · · · · · · · · · · · · · · · · ·	
	クイックセットアップ		
•	0		
	-	~	
eスポイントにプッシュする APプ	ロビジョニングファイルを選択してください。		
ヨニングファイル		QU >	
L I - 200/- Blitte AD -FOLK21-	- V/Con ZI & Bolt Z > Lator to VBA _ Nuclear Connect FRMI _ 1	ENI-M- TROUGHER	
PU-PHCENKAPJUC98		PRINCIE D CRAW CE N. 9 5	-
			プロビジョニングファイルは、このデバイス
			で見つかりませんでした。
			プロファイルをダウンロード
			キャンセル
	*^		

図 2-32 ステップ1-プロファイルのダウンロード

- **4.** (+) 「+」アイコンをクリックし、Nuclias Connect サーバへの接続情報を入力してログインします。接続に必要な入力項目については、31 ページの「Nuclias Connect サーバへの接続」を参照してください。
- 5. サイトとネットワークを選択し、「ダウンロード」をタップしてプロファイルをダウンロードします。
- 6. 「ダウンロードを続ける」または「戻る」をタップし、「ステップ1」の画面に戻ります。
- 7. プロビジョニングプロファイルが選択されている状態で「次へ」をタップします。

1:41 12月15日(木)	Nuclias Connect	* *** $\ominus \oplus$
Nuclias Connectへようこそ		
接続先の Nuclias Connect サーバーをi	択してください。 ここに表示されていない、または表示されていない場合は、新しい	いものを登録できます。
dhc test admin		30001 2022/12/15 11:40:57

図 2-33 ステップ1-プロビジョンプロファイルの選択

■ ステップ2:アクセスポイント検出範囲の定義

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

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



図 2-34 アクセスポイント検出範囲の定義

■ ステップ3:アクセスポイントへのプロファイル適用

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



図 2-35 アクセスポイントの選択

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



図 2-36 アクセスポイントへのログイン

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



図 2-37 プロファイルの適用

Nuclias Connect サーバへの接続

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

1. 「Nuclias Connect」をタップします。

11:16 12月15日(木)		🗢 100% 🚥
=	Nuclias Connect	
品		ि
クイックセットアップ	Nuclias Connect	スタンドアロンアクセスポイント
アクセスポイントを Nuclias Connect に すばやく簡単に展開します。	Nuclias Connect 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	個々のアクセスポイントの設定を変更し、 複数のアクセスポイントに展開する設定プ
	クセスホイント管理ワールです。	ロフアイルを保存できます。
	~	~

図 2-38 Nuclias Connect アプリ - トップ画面

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

12:21 12月15日(木)		🗢 93% 💼)
<	Nuclias Connect	
	Nuclias Connectへようこそ	
	Nucles Connect サーバーが見つかりませんでした。 「+」をタップして新しいものを追加してください。	
	\bigcirc	
	(\pm)	

図 2-39 Nuclias Connect へようこそ画面

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

15日(木)	
	Nuclias Connect
	新しいNuclias Connect サーバーの追加
	Nuclas Connect URL / P アドレスを入力する;
	Https://
	このNuclias Connect サーバの名前を作成する
	Nuclias Connect 9-X-A
	2-1/-2
	パスワード 👁
	ПØ4>

図 2-40 新規サーバへのログイン画面

以下の項目が表示されます。

項目	項目				
	Nuclias Connect URL/IP アドレスを入力する				
Https:// アプリとペアリングする Nuclias Connect サーバのセキュアな URL/IP アドレスを入力します。					
この Nuclias Connect サーバの名前を作成する					
Nuclias Connect サーバー名	ペアになる Nuclias Connect サーバを識別するための名前を入力します。				

項目	説明
ユーザー名	Nuclias Connect サーバにアクセスする権限を持つユーザ名を入力します。
パスワード	Nuclias Connect サーバにアクセスする権限を持つユーザのパスワードを入力します。

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

12:28 12月15日(木)	ダッシュボード	* *2% ■ *
	2 サイト	2 ネットワーク
	2/2 アクセスポイント	<mark>1</mark> クライアント
50	0/0 スイッチ	0 クライアント
アクセスポイント	スイッチ	
直近1時間の情報		Q
直近1時間のクライアント数と3	過去7日間のクライアント数 4 4 4 4	
図 2-41 ダッ	シュボード	

ペアリング済みサーバは、「Nuclias Connect」>「Nuclias Connect へようこそ」画面に一覧表示されます。

アプリを使用して、プロファイルをローカルデバイスにダウンロードし、サポートされているアクセスポイントにプッシュすることができます。

12:19 12月15日(木)		중 94% 🖿
<	Nuclias Connect	\ominus \oplus
Nuclias Connectへようこそ		
接続先のNuclias Connectサーバーを選択してください。	、ここに表示されていない、または表示されていない場合は、新しい	ものを登録できます。
disc test		122 10 1 50 30001
admin		2022/10/15 12 04/54

図 2-42 Nuclias Connect サーバのリスト

スタンドアロンアクセスポイントの検出と設定

■ アクセスポイントの検出

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

1. 「アクセスポイントの検出」をタップします。



図 2-43 Nuclias Connect アプリ - トップ画面

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



図 2-44 アクセスポイントの検出範囲

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

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

3:41 12月15日(木)		
<	アクセスポイント設定をプッシュ	53
	All 👻	
検出された AP リスト		۲ 😒
OAP-2680 v2.00		102.W1488 4070bcst0c64.s0
DAP-3666 v1.10		172 18138 DNC 172 191908443
	設定をプッシュ	

図 2-45 プロファイルの配信

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

	アクセスポイント設定をプッシュ	3
	All 🕶	
検出されたAPリスト		Ø 💿
DAP-2680 v2.00	アクセスポイントログイン	172.%/183. 4070/cst.0cd4.40
DAP-3666		172.181.38 DNC/172.161.190.8443
	2-17-26	
	バスワード 💿	
	通訳したすべてのアクセスホイントに適用	
	キャンセル	
	1042 5 - T + 2	

10. 「選択したすべてのアクセスポイントに適用」をタップして続行します。

図 2-46 アクセスポイントへのログイン

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

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

「IP 情報」タブには以下の項目が表示されます。

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

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

項目	説明		
DAP-xxxx	アクセスポイントの IP アドレスと MAC アドレスが表示されます。		
	SSID 設定		
2.4G/5G	項目をタップして、SSID 設定を表示します。 上部の「SSID-#」をタップして各 SSID の設定を確認することができます。(#の文字は、SSID の識別番号) ・「SSID を有効化:SSID のステータス(有効/無効)が表示されます。 ・「SSID 名」:SSID 名が表示されます。 ・「セキュリティ」:SSID で使用されるセキュリティプロトコルが表示されます。		
	ワイヤレス情報		
周波数帯	無線帯域が表示されます。		
周波数帯 2.4G/5G モード	2.4G/5G の無線モードが表示されます。		
国コード	アクセスポイントに割り当てられている国名が表示されます。		
設定をコピーして保存			
設定を適用	検出された別のアクセスポイントを選択し、この設定をプッシュします。		
設定を保存	プロファイルに名前を付けてローカルの設定プロファイルリストに保存します。		

13:58 12月15日(木)			
キャンセル		DAP-3666	
	IP 情報	ワイヤレス	クライアント
モデル名			DAP-3666
MAC			60.68-46.8117-30
DHCPモード			
Pアドレス			172.161.08
サブネットマスク			255.255.255.0
デフォルトゲートウェイ			1010610
DNS			1721015
Nuclias Connect 情報			
Nuclias Connect			171 151 150 8443

図 2-47 IP 情報の設定

13:59 12月15日(木)				? 85% 🗖
		DAP-3666		
	IP情報	ワイヤレス	クライアント	
DAP-3666				0150130 903036-01730
SSID 設定				
2.4G				>
5G 1				>
ワイヤレス情報				
周波数带				2.4G、5G1
周波数帯2.4Gモード			802.11n, 802	.11g、802.11b混在
周波数帯 5G 1モード				802.11ac混在
国コード				Japan
設定をコピーして保存				
設定を適用				>
設定を保存				>

図 2-48 ワイヤレス設定

ネットワークプロファイルの削除

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

1. 左上のメニューをタップします。



図 2-49 Nuclias Connect アプリ - トップ画面

2. 「AP プロビジョニングプロファイル」を選択します。



図 2-50 Nuclias Connect アプリ - メニュー項目

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

<	プロビジョニングプロファイル	完了
コーカル AP プロビジョニングプロファイルを以	下に示します。ここで、プロファイルを追加したり、剤除したりできます。	
ゆプロビジョニングプロファイル		
Site1_Network1 dnc test		2022/12/15 12:05:0
23 12月15日(木) く	ブロビジョニングブロファイル	❤ s1%. 完了
23 12月15日(本) 〈	プロビジョニングプロファイル	♥ 81%(完]
23 12月15日(本) く コーカルAP プロビジョニングプロファイルを3 D プリビジョニングプロファイルを3	プロビジョニングプロファイル 下と良します。ここで、プロファイルを追加したり、制限したりできます。	♥81%i 第7
23 12/31388(1) く コーカルルデロビジョニングブロファイルをは かプロビジョニングブロファイル	プロビジョニングプロファイル 下と良します。ここで、プロファイルを追加したり、制限したりできます。	♥ 81%1 第7 17590 18930445

図 2-51 Nuclias Connect アプリ - プロファイル選択
管理対象アクセスポイントの確認

アクセスポイント接続を確認するには、以下の手順を実行します。

- 1. Nuclias Connect 管理インタフェースから、モニタ > アクセスポイント > アクセスポイントに移動します。
- 2. ドロップダウンメニューをクリックして、サイトとネットワークを選択します。管理対象のアクセスポイントが一覧表示されます。

「ステータス」列には、現在の AP ステータスとそのオンライン(●)およびオフライン(●)状態が表示されます。 「ローカル IP アドレス」、「MAC アドレス」、「モデルタイプ」、「ネットワーク」などの情報も確認することができます。

connect	Default	09:46:23 2023-03-08 🖉 🕓 🗎	*
🎧 ダッシュボード			
101 x - 4	金でのサイト ◆ ◆ てのネットワーク ◇ ◆ ☆ でのネットワーク ◇ ◆ ☆ ☆ ☆		
	介語 ダウンロード:o Byte 介語 アップロード:o Byte		
• アクセスポイント			
アクセスポイント	MB	● ダウンロード(MB) ● ブッブロード(MB) ● 合計((MB)
ワイヤレスクライブ	(72)		
隣接AP			
スイッチ	>		
 スイッチ トポロペ 			
スイッチ トポロジ		ف ف ف ف ف ف ف ف	00
 スイッチ トポロジ フロア計画 	> 0000 10000 10000 1000 1000 1000 1000 1	و هوري قوري قوري قوري قوري قوري قوري قوري ق	08:00
 スイッチ トポロジ フロア計画 ζ 設定 	2 0000 0000 0000 0000 0000 0000 0000 00	ම සැපම සාපම සංසම සාපම සාපම සංසම සංසම ස	08:00
スイッチ a トボロジ フロア計画 。 設定 1 レポート	* ***********************************	¹⁰ から ¹⁰⁰ の ¹⁰⁰ 0 ¹⁰⁰	08:00
スイッチ a トポロジ フロア計画 2 成定] レポート	** **	 あった。のであ、のであ、のであ、のであ、のであ、のであ、のであ、のであ、のであ、のであ、	08:00
 スイッチ トポロジ フロブ出版 () (次定) □ レポート □ ログ 		¹⁰ かっ ⁵⁰ かっ ⁵⁰ 検索方法 ローカル 1 27 F レスマ	00 ^{8:00}
 スイッチ トボロジ フロブ出側 (設定) レポート) ログ 2 ×274 	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$	 あった⁰ のった⁰ のった⁰ 検索/法 (P − カル[P7 F レスマ) キーフーF を脱去 * キットワーク[D₂マ クライイエ 2,4G + キネル * 5G + キネル1 * 0 H 60 	08:00

図 2-52 モニタ - アクセスポイント - アクセスポイント

ファームウェアのアップロード

Nuclias Connect インタフェースを使用し、個別または複数の AP モデルを管理することができます。管理機能には、ファームウェアのアップグレードも含まれます。ファームウェアファイルを選択してすぐに適用するか、更新時間をスケジュールして適用することができます。

- 1. 設定>ファームウェアの更新の順に移動し、サイトとネットワークを選択して使用可能な AP モデルを表示します。
- 2. 「ファームウェアの手動更新」タブをクリックします。
- 3. 「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を選択します。

<nuclias< th=""><th>Default</th><th></th><th>10:2</th><th>16:59 2023-03-08</th><th>R</th><th>2</th><th>×</th><th>JP ~</th></nuclias<>	Default		10:2	16:59 2023-03-08	R	2	×	JP ~
(i) ダッシュポード								
122 ÷= 2 >	♥ ファームウェアの更新	ファームウェアの更新 > Site1 > Network1						_
-10	Sites	オンラインチェックアップデートファームウェア	ファームウェアの手動更新					
-F # # 2	© Network1							
◎ フロア計画	30.02	各モデルのファームウェアファイルをアッ	ブロード		アップデ	ートを確認	E.	
🗙 #z 🗸		- モデル番号 / ハードウェアパージョッ	現在のファームウェアバージョン(m× 新しいファームウェm× リリ		ームウェアフ	アイル		
 プロファイルを作成 								
 プロファイル設定 								
• ファームウェアの更新								

図 2-53 設定 - ファームウェアの更新 - ファームウェアの手動更新

4. 以下のいずれかの手順でファームウェアを適用します。

即時適用:

- (1) 「開始時間」フィールドで「即時」を選択します。
- (2) 「適用」をクリックして、ネットワーク上の選択したアクセスポイントにファームウェアをすぐに適用します。

指定日時に適用:

- (1) 「開始時間」フィールドで「時間を選択」オプションを選択して、ファームウェアをアップロードする時間を定義します。
- (2) 「適用」をクリックしてアップグレードのスケジュールを保存します。

第3章 Nuclias Connect の管理インタフェース

- 「Nuclias Connect への接続」
- 「ウィザード」
- 「ユーザプロファイル」
- 「管理インタフェースからのログアウト」

Nuclias Connect への接続

ここでは、Nuclias Connect クライアントアプリケーションについて説明します。

 ソフトウェアのインストールが完了すると、以下のアプリケーションが使用可能になります。 Windowsのメニューから「Nuclias Connect」を選択し、クライアントアプリケーションを開きます。



Nuclias Connect は、セキュアな HTTPS 接続を使用して Nuclias Connect コントローラに接続します。 初期値では、アプリケーションにより既定の Web ブラウザが起動され、コンピュータ自身の IP アドレスを意味する「localhost」に接続します。

または、リモートコンピュータから、コントローラ(サーバ)アプリケーションがインストールされているコンピュータの IP アドレスを Web ブラウザに入力して、Nuclias Connect サーバに接続することもできます。リモートコンピュータの Web ブラウザ(Edge、Chrome、Safari 推奨) を開き、Web ブラウザのアドレスバーにホストコンピュータの IP アドレスまたはドメイン名を入力し、Enter キーを押して Nuclias Connect 管 理インタフェースを開きます。

- 2. サーバへの接続が確立されると、Nuclias ログイン画面が表示されます。
- 3. ログインユーザ名、パスワード、CAPTCHA コードを入力し、「ログイン」をクリックして Nuclias Connect にログインします。

< nuclias connect	
ログインアカウント	□本語 ~
あなたのユーザーネーム	
$\sim z \overline{z} - k$	
キャプチャを入力してください 5 279	バスワードを忘れた場合
ログイン	
© 2018-2022 D-Link Corporation. All r Terms of Service Privacy Polic	ights reserved. Y

図 3-2 Nuclias Connect へのログイン

注意 デフォルトでは、ユーザ名とパスワードは admin です。サポートされる言語は、英語(デフォルト)、繁体字中国語、簡体字中国語、韓国 語、日本語、フランス語、スペイン語、ドイツ語、ロシア語、イタリア語、トルコ語です。

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。

1. 画面右上の 💘 をクリックして、ウィザードを開始します。

「システム情報を設定し、「保存して次へ」をクリックします。ウィザードを中止するには「キャンセル」をクリックします。

			>
で更する場合、Nuclias Cor	nnectコアサーバの再起動	りが必要となります。	
172.16.159	~		
8443			
Japan	~		
(GMT+09:00) Osaka,	Sapporo, Tokyo	~	
		保存して次へ	キャンセル
	変更する場合、Nuclias Cor	更する場合、Nuclias Connectコアサーバの再起動 「こここ」 8443 Japan ~ (GMT+09:00) Osaka, Sapporo, Tokyo	変する場合、Nuclias Connectコアサーバの再起動が必要となります。 8443 Japan ~ (GMT+09:00) Osaka, Sapporo, Tokyo ~

図 3-3 ウィザード-システム設定

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	Network1	
ネットワークID		
	ネットワークIDはREST APIに使用されます。	
		戻る 次へ キャンセル
		and the second

図 3-4 ウィザード - ネットワークを追加

- 3. 「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。
- **4.** 「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、「次へ」をクリックします。前の画面に戻るには「戻る」をクリック、ウィザードを中止するには「キャンセル」をクリックします。

第3章 Nuclias Connectの管理インタフェース

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

福足 スイッチ製品は未サポートです。

一般設定		
国	Japan v	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸 🗸	
デバイスタイプ	アクセスポイント スイッチ ネットワーク内で管理されるデバイスタイプを選択してください。	
アクセスボイント		,
スイッチ		,

図 3-5 ウィザード - ネットワークの設定

般設定		^
国	Japan	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸 🗸	
デバイスタイプ	✓ アクセスポイント スイッチ ネットワーク内で管理されるデバイスタイプを選択してください。	
アクセスポイント		-
管理者		
ユーザ名	admin	
パスワード*	20	
SSID名	dlink	
セキュリティ	WPA- ν - γ + ν \vee	
SSIDパスワード*	Ś	
SSID設定		
ゲストSSID名	クストSSIDを追加(オフション)	
スイッチ		

図 3-6 ウィザード - ネットワークの設定(アクセスポイント)

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

「次へ」をクリックして続行します。設定プロセスを中止するには「キャンセル」をクリックします。

Ҟ ネットワーク設定を検出	Х
✓ レイヤ2	
レイヤ3(IP)	
- つ選択 ~	+
	戻る 次~ キャンセル

図 3-7 ウィザード - ネットワーク設定を検出

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

設定可能	管理									
	7	バイスタイプ	アクセス	ポイント ×			М	ACアドレ:	ス (キーワード'を	検索 C
x	デート	∨ IPアドレス	~	MACプドレス	~ モデル番号	~	結果をイン	/ ポート	 NMS URL 	~ ネット
🖌 僧	1理	711-261		dordenstrailer:	7 DAP-3666				111011_10:8 4	43 NetworkA
			7							
× ► 7 - 7 :	ブロファイバ	~をインボート:	admin		•••• ;	R	{ ∧3{ - } +			

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

9. 右上の「×」ボタンをクリックして画面を閉じます。

ユーザプロファイル

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。

ユーザプロファイル			
\bigcirc	個人情報 セキュリ	<i>₸ 1</i>	
	情報		
	ユーザ名*	admin	
admin	設置場所		
システム管理者	電話番号		
A メールノドレス指数なし	說明		
		更新	
			終了
			4C 1

図 3-9 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。

ユーザプロファイル		×
	個人指限 セキュリティ	
	パスワードを変更	
admin	新しいパスワード*	
システム管理者 ▲ メールアドレス情報なし	バスワード確認*	
		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 3-10 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4章 ダッシュボード

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

補足 スイッチは未サポートです。



図 4-1 ダッシュボード

画面上部の統計情報には以下の項目が表示されます。

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

「アクセスポイント」タブには以下の項目が表示されます。

項目	説明
直近1時間の情報	以下の履歴情報を表示します。表示するサイト / ネットワークおよび期間を指定することができます。
	 ・ 直近1時間のクライアント数と過去7日間のクライアント数
	• 直近1時間のトラフィック使用量と過去7日間のトラフィック使用量(MB)
	• 直近1時間のダウンリンク/アップリンクトラフィック使用量(MB)
	・ 直近 1 時間の SSID ごとのトラフィック使用量(MB)
チャネル利用数	2.4GHz 帯域 /5GHz 帯域のチャネルごとのアクセスポイントの台数を表示します。
直近のイベント	最新イベントの簡易的なログを表示します。
	表示するサイト / ネットワークを指定することができます。

「スイッチ」タブには以下の項目が表示されます。

項目	説明
直近1時間の情報	以下の履歴情報を表示します。表示するサイト / ネットワークおよび期間を指定することができます。
	• 直近 1 時間の Tx/Rx トラフィック使用量(MB)
	• 直近 1 時間の PoE 使用量(W)
PoE 利用率	PoE 利用率ごとのスイッチの台数を表示します。
	表示するサイト / ネットワークを指定することができます。
直近のイベント	最新イベントの簡易的なログを表示します。
	表示するサイト / ネットワークを指定することができます。

第5章 モニタ

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

補足 スイッチ製品は未サポートです。

アクセスポイント

< nuclias 09:46:23 2023-03-08 🖉 🕓 💘 JP 🤇 Default () ダッシュボー 全くのサイト 金式のネットワーク >
 ②
 合計: 1/1 アクセスポイント 🖳 == 9 合計 ダウンロード: o Byte 合計 アップロード: o Byte ● ダウンロード (MB) 🛛 ◆ アップロード (MB) 🔹 合計 (MB) 防接AP - H-11 - 2 ◎ 707計画 アクセスポイント N 1258 検索方法「ローカルIPアドレスッ」「キーワードを検索 Q 園 レポート No.... ステータエ アクション ローカルIPアドレ...× MACアドレス × モデル番号 × ネットワーク × ネットワークID...× クライアエ 2.4Gチャネル × 5Gチャネル1 : ----1 🕒 () 🔓 💬 mala and and and DAP-2680 Networks 2023 5 システム

図 5-1 モニタ - アクセスポイント - アクセスポイント

■ 対象範囲の指定 / デバイスの検索

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

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

■ レポート項目

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

- ステータス
- ・ ローカル IP アドレス
- ・ ローカル IPv6 アドレス
- ・ MAC アドレス
- モデル番号
- ファームウェアバージョン
- 名前
- 設置場所
- ・サイト
- ・ ネットワーク
- ネットワーク ID
- クライアント
- 44 2.4G チャネル

- 5G チャネル1
- 5G チャネル2(トライバンド)
- 2.4G 出力
- 5G出力1
- 5G 出力2(トライバンド)
- ・ ダウンロード
- アップロード
- トラフィック使用量
- ・ トラフィック使用率(%)
- CPU 使用率(%)
- メモリ使用率(%)
- 最終更新情報
- 稼働時間

タスを表示します。

左側のパネルからモニタ>アクセスポイント>アクセスポイントをクリックし、トラフィック使用量の時間毎の推移と各アクセスポイントのステー

アクセスポイント - デバイス詳細

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

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

∢nuclias connect	Default				09:46:382	023-03-08	۰ 😮	JI
<i>係 ダッシュ</i> ポード								
₩ * *	デバイス情報							
• アクセスポイント	ステータス 🛑	オンライン	ローカルIPブ ドレス	cutot	MACブドレス	seal-ploch-pla		
アクセスポイント	モデル番号 DA	P-2680	ハードウェアバージョン	2A1G	ファームウェアバージョン	v2.00B08r051		
ワイヤレスクライアント	ネットワーク Net	works	アップロード		ダウンロード			
陸接AP	メモリ使用本(96) 27		CPU使用率 (%)	6	称他时间	5d 20h 17m 33s		
• スイッチ >								
►#¤\$	デバイス設定							
● フロブ計画								
🗙 設定 >	2.4Gチャネル 11	~	2.4G[][]]	100% ~	名前	dap2680		
レポート >	5Gチャネル1 60	~	5GHUJ1	100% ~	設置場所			
ヨ ログ >	5Gチャネル2(トライ 該当 バンド)	なし 5	GHIJ12(トライバン ド)	該当なし				
· AFRY Or						1	保存	
	使用量							
					● ダウンロード (MB)	🔶 ブッブロード (MB)	◆ 合計(MB)	
	1							
	0.00.00.00.00	no. 00. 00. 00.	00 00 0		90 90 90	00 00 00	0000	

図 5-2 モニタ - アクセスポイント - アクセスポイント - デバイス詳細

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

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

アクセスポイント - ワイヤレスクライアント

接続しているクライアント

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

∢nuclias connect	Default 09:46:46 2022-02-08 🖉 🚨 💘 JP 🗸
(b) ダッシュポード	18月1-11はスクライデント ダルークネルトクライデント
€=9 *	
 アクセスポイント 	
アクセスポイント	
ワイヤレスクライアント	
陳接AP	
• • • •	
000 F#FFF	
◎ フロア計画	
🗙 ikiz 🔹 🔸	
「」 レポート >	
5 ¤7 >	
50 VXFA >	クライアントがまだ接続されていませ ん。

図 5-3 モニタ - アクセスポイント - ワイヤレスクライアント(接続しているクライアント)

■ 対象範囲の指定 / デバイスの検索

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

■ レポート項目

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

- ・サイト
- ネットワーク
- ・IPアドレス
- ・ IPv6 アドレス
- ・ MAC アドレス
- ホスト名
- 認証タイプ
- ユーザ名
- OS
- アップロード
- ・ダウンロード

- ・ チャネル
- RSSI (dBm)
- SNR (dB)
- 周波数帯
- SSID
- ・ AP MAC アドレス
- トラフィック使用量
- ・ トラフィック使用率(%)
- 最終更新情報
- 稼働時間

ブロックされたクライアント

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

<nuclias< th=""><th>Defau</th><th>ult</th><th></th><th></th><th></th><th></th><th>16:44:30 2022-12-19 🖉 🚨</th><th>🔀 JP</th></nuclias<>	Defau	ult					16:44:30 2022-12-19 🖉 🚨	🔀 JP
$(\underbrace{\mathbf{k}}_{\mathbf{k}}) \mathcal{J} = \mathcal{J} = \mathbf{k} - \mathbf{k}$								
- e=+	0.0	CT06274721	2 B 9 9 8 M 2 9 7 4 7 9 8					
 72+3×4×1 	会計	370998nt:	アナイアント				全てのサイト ッ 全てのネットワーク	~ (R
アクセスポイント	No). アクショ	i A ≥ F 9 − 2	 MAC7 FLA + 	~ 周续载带	✓ SSID	< 認証タイプ	2
ワイヤレスクライアン	1	5	Networks	100 million (100 million)	2.4GHz	dlinknctest	$\mathfrak{A}=\mathfrak{Y}^{\prime}\mathfrak{E}/\mathscr{A}\mathfrak{I}\mathfrak{I}=\mathfrak{I}^{\prime}$	
總證AP	2	5	Networks	ALC: NO. 10. 10. 10.	gGHz 1	dlinknctest	ユーザ名/パスワード	
• スイッナ	3	5	Networks	10000	93H2 2 (F 🤊 イ / ' ' / '')	dlinknctest	$x = \theta' \in / < x : 7 = V$	
tens								
Ø 7 = 7 計画								
× RE ,								
レポート ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・								
a 7 5								
50 2×74 0								

図 5-4 モニタ - アクセスポイント - ワイヤレスクライアント(ブロックされたクライアント)

■ 対象範囲の指定

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

■ レポート項目

ブロックされた各無線クライアントについて、以下の項目が表示されます。

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

アクセスポイント - 隣接 AP

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th></th><th></th><th>16:4</th><th>4:22 2022-12-19</th><th>😤 😩 🤾 јр 🗸</th></nuclias<>	Default							16:4	4:22 2022-12-19	😤 😩 🤾 јр 🗸
$ (\widehat{\mathcal{T}}) = \mathcal{T} = \mathcal{T} = \mathcal{T} $										
∰ e=2 ×								被索方法 により	秋出 ~ +	7-17を検索
 アクセスポイント 	No.	BSSID 🔺 👻	により秋出 エー・イ	77-97 v	SSID ×	*******	RSSI(dBm) ~	BW (MHz) ~	≠ + \$ μ ×	**-+\$\$\$\$\$#
アクセスポイント	1		Constant of the	未知	DAP-X1900	WPA2-PSK(AES)	-56	20	4	B ₄ G ₃ N
ワイヤレスクライアント	2	1000	· · · · · · · ·	未知	DAP-X1900	WPA2-PSK(AES)	-44	80	128	A,N,AC
純投AP	3			未知	DWC-2000	WPA2-PSK(AES)	-95	20	4	$B_{g}G_{g}N$
• X497 3	4			未知	100.000	WPA3-PSK(AES)	-95	20	2	B ₁ G ₁ N
teres	5	a second so planta	1	未知	DAP-X2810	WPA2-PSK(AES/TKL	-62	20	3	B,G,N
○ 7 □ 7 計画	6		100.000	未知	DAP-X2810	WPA2-PSK(AES/TRL.	-52	80	120	A,N,AC
20.000	7	1.000		未回	100	WPA2-PSK(AES)	-57	20	1	B,G,N
X RE >	8	0.0000000000000000000000000000000000000		未知	ALC: 1	WPA2-EAP(AES)	-57	20	1	B ₄ G ₄ N
1 v#-> >	9	1.000		未知		WPA2-PSK(AES/TKL	-95	20	1	B,G,N
E =/ >	10	1.000 Barris		未知		WPA2-PSK(AES/TKL	-95	20	1	B ₄ G ₃ N
Lo 2274 >	11	1.000		未知		WPA2-PSK(AES/TKL	-95	20	1	B,G,N
	12	0.000		未知	Married Street	WPA2-PSK(AES/THL	-46	20	1	B ₄ G ₃ N
	13	1.000		未知	10000	WPA2-PSK(AES/TKL	-45	20	1	B ₁ G ₁ N
	14	0.000		未回	10000	WPA2-PSK(AES/TKL	-95	20	1	B ₄ G ₃ N
	15	1.000		未知	2000	WPA2-PSK(AES/TKL	-60	20	1	B,G,N
	16	and the factor of the	for the second second	未知	10000	WPA2-PSK(AES/TKL	-57	20	1	B ₄ G ₄ N
	17	0.0000000000000000000000000000000000000		未知	10000	WPA2-PSK(AES/TKL	-59	20	1	B ₈ G ₈ N
	1 - 20 of 268 P -	タルアイテム: 268						« < <u>1</u>	/14 > > 2	0 シーベニとのブイテム

図 5-5 モニタ - アクセスポイント - 隣接 AP

■ デバイスの検索

以下の項目が表示されます。表示項目を変更するには、 をクリックします。

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



「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」をご確認ください。

スイッチ

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

補足 スイッチ製品は未サポートです。



図 5-6 モニタ-スイッチ-スイッチ

■ 対象範囲の指定 / デバイスの検索

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

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

■ レポート項目

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

- ・ステータス
- ・ ローカル IP アドレス
- ・ MAC アドレス
- モデル番号
- ・ ファームウェアバージョン
- ・ ハードウェアバージョン
- シリアル番号
- ・名前
- 設置場所
- ・サイト
- ・ ネットワーク

主要な項目の説明は以下の通りです。

 項目
 説明

 名前
 ユーザ定義のスイッチの名前を表示します。名前が指定されていない場合は何も表示されません。 列をクリックして、名前を設定または変更します。最大 63 文字で入力します。

 設置場所
 スイッチの位置を表示します。 列をクリックして、場所の名前を設定または変更します。最大 32 文字で入力します。

 クライアント
 スイッチに接続しているクライアントの総数を表示します。 クライアントの数をクリックすると、「スイッチクライアント」画面に遷移します。

 ポート
 スイッチのポートの総数を表示します。 ポートをクリックすると、「スイッチポート」画面に遷移します。

- ・ ネットワーク ID
- ・ クライアント
- 配信された電力
- ・ パワーバジェット
- CPU 使用率(%)
- メモリ使用率(%)
- ・ポート
- 設定を使用
- 最終更新情報
- 稼働時間

項目	説明
設定を使用	設定モード(プロファイル/スタンドアロン)を表示します。
	・ プロファイル:プロファイルモードのデバイスは、プロファイル内の同じ設定を共有します。
	 スタンドアロン:デバイス個別の設定があり、プロファイルの影響を受けることはありません。
最終更新情報	スイッチが最後に接続された時刻を表示します。
稼働時間	スイッチが再起動してから経過した起動時間を表示します。

スイッチ - デバイス詳細

左側のパネルからモニタ>スイッチ>スイッチをクリックし、スイッチの一覧を表示します。 アクション欄の 💬 (デバイス詳細ページへのリンク)をクリックすると、デバイスの詳細画面が表示されます。

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

基本タブ

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



補足 スイッチ製品は未サポートです。

<nuclias< th=""><th>Default</th><th>10:09:06 2023-03-08</th><th>😍 🔀 JP 🗸</th></nuclias<>	Default	10:09:06 2023-03-08	😍 🔀 JP 🗸
$\begin{array}{c} \overbrace{(k)}^{\infty} & \mathcal{I} \neq \mathcal{I} = \exists l - l \end{array}$	基本 ポート IPインタフェース ルーティング フール		
• アクセスポイント >	デバイス結果		
• スイッチ	ステータス 🕒 オンライン MACアドレス MACアドレス	モデル番号 DGS-1210-20	
スイッチクライアント	$\gamma - F \phi = T \gamma - \varphi = F $ $T \gamma - L \phi = T \gamma - \varphi$ v6.30.bo22	シリアル番号 QBDES12105200	
スイッチボート	DDP 有効化 RSTPルート RSTPは無効化されています。 ネットワーク Networks メモリ使用率(%) 20	LBD 無効化 CPU使用率 (%) 97	
	ローカル発格結晶 ユーデ名: admin タイムゾーン (GMT+og.co.0) Osaka, Sapporo, Toky	稼働時間 2m 335	
◎ フロア計画	21×17 - F :		
🗙 iki 🔹 🔹	形は大穀産		
	設定を使用 ● プロファイル ○ スタンドプロン		
i 77 >	クロメ属性		
50 VXFA >	VLAN設定		
	VLAN ID*		
	2-4094		
	12(H)		
	X1.311 クリア		
	VLANリスト VLAN ID キーワードを除意		

図 5-7 モニタ - スイッチ - スイッチ - デバイス詳細 - 基本タブ

デバイス情報

「デバイス情報」セクションには、以下の項目が表示されます。

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

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

デバイス設定

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

■ VLAN 設定

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

VLAN ID*				
	2-4094			
說明				
	追加 クリ	7		
VLANリスト	テーブル内のエント	リの最大数は 256 です。.	VLAN ID キーワード'を検索 残り255	ß
	VLAN ID	説明	アクション	

図 5-8 VLAN 設定

VLAN を作成する場合、以下の手順を実行します。

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

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

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

■ IGMP スヌーピング

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

IGMPスヌーピング設定	
IGMPスヌービング	○ 有効化 ● 無効化
VLAN	1-4004 例: 1-4.7もしくはall

図 5-9 IGMP スヌーピング設定

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

■ アンクロス属性

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

アンクロス属性		
名前		
設置場所		
STPブリッジプライオリティ	32768	~

図 5-10 アンクロス属性

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

■ 設定の適用

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

IP 接続

「IP 接続」セクションでは、プライマリ接続を設定できます。

217	DHCP A # 7 4 % 7 IP		
ローカルIPブドレス*			
VLAN*	1	20 現在このVLANに属しているメンバボート	
ネットマスク*	255.255.255.0		
$\dot{\gamma} = \mathbb{E} \neq \pm A^{\star}$	172.16.1.1		
DNS	172.16.1.5		
			適用

図 5-11 IP 接続

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

CPU 使用率

「CPU 使用率」セクションには、CPU 使用率のグラフが表示されます。



図 5-12 CPU 使用率

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

ポートタブ

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

補足 スイッチ製品は未サポートです。



図 5-13 デバイス詳細 - ポートタブ

概要

ポートの色とアイコンが示すステータスは以下の通りです。

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

ポートトラフィック利用量

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



図 5-14 ポートトラフィック利用量

ポート情報

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

					検索方法	VLAN ~	ポートタイプ	全てのタイプ い	・ キーワード'を検索	
									Ľ	
η(−)- "λ	アグリゲート.x	リンクー・	TXバイト数 ~	RXバイト数 ~	合計バイト数.x	使用許電力 ~	ポートタイプム	VLAN ~	許可されたVLAN.x	ポートステ
1	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		行効化
2	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		有効化
3	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化
4	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		有効化
5	-	自動/リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	-	アクセス	1		有効化
6	-	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		有効化
7	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		有効化
8	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		行効化
9		自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		宿効化
10	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)	2	アクセス	1		行効化
11	2	自動 / リンクダウン	0.00 (MB)	0.00 (MB)	0.00 (MB)		アクセス	1		有効化

図 5-15 ポート情報

テーブルには以下の項目が表示されます。

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

■ ポートの検索

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

■ ポートの変更

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

- 1. 変更するポートの横にあるチェックボックスにチェックを入れます。
- 2. 2 をクリックして編集を行います。下にスクロールして、当該ポートのポート設定を編集してください。

ポート設定					
設定を使用	スタンドプロン				
スイッチボート	/7,/13				
	Update 2 ports				
リンク(RJ45)	自動	~	DDP	有効化	~
$\mathscr{X} = \{ \prec \overline{\tau} = \}$	有効化	×	ポートシャットダウンスケジュー ル	Unscheduled	v
ポートタイプ	アクセス	~	LBD	無効化	~
RSTP	有効化	~	$\operatorname{STP} \vec{n} = \vec{r}$	無効化	
VLAN	1	~			
アクセスポリシー	無効	v			
					適用キャンセル

図 5-16 ポート設定

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

11日11日11日11日11日11日11日11日11日11日11日11日11日	
ポートタイプ	
	 ・「トランク」: トランクポートでは、選択したポートが 802.1Q のタグ付きトラフィックを受け入れ / パスすること ができます
	- 「ネイティブ VLAN」:すべてのアンタグトラフィックがこの VLAN に配置されます。1-4094の範囲で指定します。 - 「許可された VLAN」:選択された VLAN のみがこのリンクを通過できます。all(すべて)または 1-4094 の範 皿で指定します
	 ・「アクセス」:アクセスポートは、すべてのトラフィックを定義された VLAN に配置します。 ・「VLAN」:すべてのトラフィックがこの VLAN に配置されます。1-4094 の範囲で指定します。 -「アクセスポリシー」:このポートに制限ポリシーを適用します。
	- 「無効」: すべてのデバイスがこのポートにアクセスできます。 - 「スタティック MAC ホワイトリスト」: このリストで指定された MAC アドレスを持つデバイスのみがこの
	ホートにアクセスできます。 -「ポートセキュリティ delete-on-time モード」:エントリがエージアウトした場合、またはユーザがこれら のエントリを手動で削除した場合に、学習されたすべての MAC アドレスが消去されます。「ダイナミッ クホワイトリストサイズ制限」の設定により、動的に学習されたエントリの数を制限できます。「ダイナ ミックホワイトリスト MAC」の総数が「ダイナミックホワイトリストサイズ制限」の値を超えると、後
	続のすべての MAC アドレスがこのポートへのアクセスを拒否されます。 - 「ユーザ定義のアクセスポリシー」:「アクセスポリシー」画面で定義したポリシー名を適用します。

3. 設定を変更後、「適用」をクリックしてスイッチに設定を適用します。

アグリゲート管理

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

ポートチャネルID	2	~		
アグリゲートタイプ	 ● LACP ○ スタディック 			
ポートリスト	Unselected:	Sele	ted:	
	Port3			
	Port4			
	Port5			
	Port6			
	Port7			
	Port8			
	Port9			
	2~8個のボートを組み合わせてリンク	アグリゲーショングループを形成し	\$ <i>†</i> ,	
				31 /1 / 2 / 2
Latur 1 1.11 7 L				
ブル内のボートチャネルの最	大数は8です。,残り7			
ポートチャネルID	アグリゲートタイプ	dt - F	ブクション	

図 5-17 アグリゲート管理

■ アグリゲーショングループの作成

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

■ ポートチャネルリスト

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

■ アグリゲーショングループの編集・削除

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

「適用」をクリックして設定をスイッチに適用します。

ミラー管理

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

送信先ボート F	Port3 aselected:	~				
送信元ポートリスト UT	aselected:					
			Selected:			
	Porta					
	Port2					
	Port4					
	Port5					
	Port6					
	Port7					
	Port8					
						_
					30.)	1 <i>/ 1 T</i>
ドートミラーリスト テーブル内のボートミラーの最大数は1*	です。、残り〇					
送信先ボート	送信元ポート (Tx)	送信元ポート(R	(z	送信元ポート(両方)	アクション	
3				4	e î	

図 5-18 ミラー管理

■ ミラーリングの作成

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

■ ポートミラーリスト

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

■ ミラーリングの編集・削除

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

「適用」をクリックして設定をスイッチに適用します。

クライアント情報

「クライアント情報」セクションに、クライアント情報の概要が表示されます。

				検索方法	Client MAC	Address 🗸	e.g. 3c:1e: 04:16:53:20
No. v	クライアントMACアドレス	クライアントIPv4アドレス	$\exists^t - \vdash$	VLAN	LLDP	製造	最終更新情報
1	mentapoya angle	a.	15	1	2	2	2023/03/08 10:09
2	second and and	4	15	1	2	-	2023/03/08 10:09
3	server a difference		15	1	2	2	2023/03/08 10:09
4	serve public da		15	1	2	-	2023/03/08 10:09
5	selloperation	-	15	1	2	-	2023/03/08 10:09
6	yeahayangan	1	15	1	2	-	2023/03/08 10:09
7	well-supervise.	<u>a</u>	15	1	3		2023/03/08 10:00

図 5-19 クライアント情報

■ クライアント情報の表示・検索

「検索方法」のドロップダウンメニューで検索項目の属性を選択した後、キーワードを入力し、
 したのでのであった。

以下の項目が表示可能です。表示項目を変更するには、 * をクリックします。

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

- 「ポート」では、クライアントが接続されているスイッチのポート番号を表示します。ポート番号をクリックすると、ポート詳細画面が開きます。

- 「LLDP」では、隣接機器の LLDP 情報を表示します。
- 「製造」では、LLDP 経由のリモートデバイスの製造名を表示します。
- 「最終更新情報」では、ネットワーク上でクライアントが最後に検出された時刻を表示します。

IP インタフェースタブ

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

補足 スイッチ製品は未サポートです。

de de l	IPA 2971-X	ルーティング ツール			
IPv4インタフョ	- 7				
	VLAN ID	1			
	ステート	無効化・・			
	₽7ドレス*				
	ネットマスク*				
		通加 クリア IP接続がDHCPモードであり、I	Pインタフェースを追加できません。		
IPv4インタフ	ェーステーブルのエント	・リの最大数は4です。,残り3			
VLAN ID	ステート	IPアドレス	リンクステータ	アクション	
	Tithey	/ 255 255 255 0	Up		

図 5-20 デバイス詳細 - IP インタフェースタブ

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

■ IPv4 インタフェーステーブル

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

■ インタフェースの編集・削除

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

「適用」をクリックして、設定をスイッチに適用します。

ルーティングタブ

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

補足 スイッチ製品は未サポートです。

IPv4スタティック/デフォルトルート	設定									
IPアドレス*	0.0.0			? 1	Default					
ネットマスク*	0.0.0.0									
	e.g. 255.255.255.2	54								
ゲートウェイ*	e.g. 172.18.192.1									
□スト (1-65535) *	1									
バックアップステート	プライマリ		v							
テーブル内のエントリの最大数は 16 ・	Akon 9 5									
No IPアドレス/ネットマスク	~ 4-	トウェイ	✓ = スト	~	プロトコル	× バックアップ	~	ステータス・	アクション	

図 5-21 デバイス詳細 - ルーティングタブ

■ IPv4 スタティック / デフォルトルート設定

- 1. 「IP アドレス」「ネットマスク」を入力、または「Default」にチェックを入れます。
- 2. 「ゲートウェイ」「コスト」を入力し、「バックアップステート(プライマリ/バックアップ)」を選択します。
- 「追加」をクリックして、ルート設定を保存します。
 設定をキャンセルするには、「クリア」をクリックします。
- 4. 「適用」をクリックして、設定をスイッチに適用します。

■ スタティックルートテーブルの表示

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

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

■ スタティックルートの編集・削除

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

「適用」をクリックして、設定をスイッチに適用します。

■ IPv4 ルートテーブル

IPv4 ルートテーブルには、スイッチのルート情報が格納されます。以下の項目が表示されます。 ・「IP アドレス」「ネットマスク」「ゲートウェイ」「インタフェース名」「コスト」「プロトコル」

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

電源タブ

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

補足 スイッチ製品は未サポートです。



図 5-22 デバイス詳細 - 電源タブ

■ システム消費電力

「システム消費電力」のグラフには、スイッチの電力使用量(W)が時間単位で表示されます。 また、合計 / 現在の消費量 / 最大消費量 / 最小消費量 も確認することができます。

■ PoE ポートステート

「PoE ポートステート」の一覧には、以下の項目が表示されます。

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

ツールタブ

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

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

デバイスがオフラインの場合、ツールは無効になります。



補足 スイッチ製品は未サポートです。

Ping

Ping ツールを使用すると、デバイスへの接続可否を判断できます。

Ping	
IPアドレス/FQDN	
e.g. 172.18.192.10, Google.com	Ping
Ping結果	

図 5-23 Ping

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

MAC 転送テーブル

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

実行				
		MAC	キーワード'を検索	
No. MAC	VLAN	,∜.— ŀ	タイプ	
		5		
	データが見つかり	ませんでした		

図 5-24 MAC 転送テーブル

「実行」クリックして処理を開始します。

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

ケーブルテスト

ケーブルテストでは、1つまたは複数のポートの接続をテストできます。

205-	・でケー	-ブルテストを	実行		
⊀— ŀ				Ŧ	71
	e.g. 1	1-5,7,11,20-23			
警告: この	テスト	は、デバイス・	への通信を中断します。		
ケーブル・	テスト編	1.			
차	ŀ	タイプ	リンクステー	テスト結果	ケーブル長(M)
			G	2	
			データが見つかり	ませんでした	

図 5-25 ケーブルテスト

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

注意 ケーブルテストにより、デバイスへのトラフィックが中断されます。

サイクル PoE

サイクル PoE 機能を使用すると、特定のポートで PoE を無効化してから再度有効化することができます。 このツールは、PoE が有効な場合にのみ実行できます。スイッチが PoE をサポートしていない場合、このセクションは無効になります。

PoEを無	効化して、再度有効化			
ポート		テス	F	
	e.g. 1-5,7,11,20-23 PoEはスイッチでサポートされていません。			
警告: Pol	2受電デバイスは一時的にパワーダウンします。			
サイクル	PoEテスト結果			

図 5-26 サイクル PoE

デバイスの検索

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

デバイスの検索	開始	停止			
デバイスの検索結果	e.				

図 5-27 デバイスの検索

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

他のデバイスに設定をコピー

本機能を使用すると、以下の設定をネットワーク内の他のデバイスにコピーできます。 ・ ユーザ設定モード、VLAN 設定、IGMP スヌーピング設定、ポート設定、アグリゲート管理、ミラー管理

C	-	
	- 12	= [
	-	- T- T- T-
	•	1

コピー元とコピー先の2つのデバイスは同じモデルである必要があります。

このネットワーク内の同じモデルのデバイン	2	
Inselected:	Selected:	
	*	
没定をコピー		
改定をコピー 		
設定をコピー コピー 以下の設定がコピーされます・		
設定をコピー コピー 以下の設定がコピーされます: ・ユーザ設定モード		
 設定をコピー コピー 以下の設定がコピーされます: ・ユーザ設定モード ・VLAN設定 		
 設定をコビー コビー 以下の設定がコビーされます: ューザ設定モード VLAN設定 IGMPススービング設定 		
 設定をコビー コビー 以下の設定がコビーされます: ューザ設定モード VLAN設定 IGMPススービング設定 ボート設定 		

図 5-28 他のデバイスに設定をコピー

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

第5章 モニタ

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

スイッチ-スイッチクライアント

左側のパネルからモニタ>スイッチ>スイッチクライアントをクリックします。

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



補足 スイッチ製品は未サポートです。

connect	Default								10:14:48	2023-03-08	ß	٩	×	
	余ての	11 v Aco	k≠ k7 k7 - 2 ∨ 🕞 A	計: 25 接続しているクライア	2 F									
2 6 -9 ×						(A.5.4	のスイッチ	√ 検索方:	Client MAC Add	ress v	8.E. 3018	04:16:53:20		ß
アクセスポイント >	Nox	ABITYLMACTE V	クライアント IDes アドレン	7 (- 4MACT 11 - 7	71.49		P=1 V	VI AN X	LIDR	0425		LA DE LA		
2199	140.11	77477719L3071	2247211147124	AN TARCTURA -	A1774		40 1	V LOUX	LLDI	34741		Acre Lee le 0		l
スイッチ	1	NEXTRACTOR NAMES	<i>.</i>	REPORTE HOLDER HE			15	1	-			2023/03/08	.0:09:35	5
スイッチポート	2	Nectories	-	REPORT FOR AND	-		15	1	-			2023/03/08 :	.0:09:35	5
	3	seconded/fight	С ¹	Reformer and a second	0		15	1	0	-		2023/03/08 :	0:12:41	
Fat D S	4	sourceshdow		Record Course	~		15	1	~			2023/03/08	10:09:35	5
フロア計画	5	searce should	<i></i>	Recorder of Commencements			15	1	đ	-		2023/03/08	10:09:35	5
設定 >	6	10 Table and	e.	RECORDER COVER			15	1	-			2023/03/08 :	10:09:35	5
Link to the	7	etib-crocove.					15	1		-		2023/03/08	10:09:35	5
	8	will-constal	~	NHOW DE VOID AND			15	1	~			2023/03/08	10:09:35	5
¤ <i>7</i> >	9	and the second second		HERONO COLORING			15	1	0	-		2023/03/08 :	10:11:13	
システム	10	schoeldos		CHOUDE HEROENE	~		15	1				2023/03/08	10:09:35	5
	11	-control activity	12064-6	Record Control of The			15	1	-	-		2023/03/08	10:09:35	5
	12	ablaboritzy	-	HARDARD COLOURS			15	1		-		2023/03/08 :	10:09:35	5
	13	whendow		HADADE HER CALLER			15	1				2023/03/08	10:09:35	5
	14	the second second	~	(HONDERGOWNE)			15	1	-			2023/03/08 :	10:09:35	5
	15	soutcate		HARVER DOWN			15	1	-	-		2023/03/08 :	10:14:15	

図 5-29 モニタ-スイッチ-スイッチクライアント

■ 対象範囲の指定 / クライアントの検索

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

■ レポート項目

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

をクリックします。

・サイト

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

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

スイッチ - スイッチポート

左側のパネルからモニタ>スイッチ>スイッチポートをクリックします。

補足 スイッチ製品は未サポートです。

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

uclias connect	Default								1	0:14:54 2023-	03-08	×
$\mathscr{I} = \mathscr{V} = \mathscr{K} = \mathbb{F}$												
€=\$ v	全てのち	HAR V	全てのネットワー	-2 ~ R {	合計: 20 スイッチ:	K - F						
アクセスポイント >				全ての	0ポートグルーマ	全てのスイッチ	· · · · · · · · · · · · · · · · · · ·	部方法 VLAN	✓ ポートタイ	ア「全てのタイプ	✓ # - 7 - F'≤	検索
スイッチ	No.	SWITCH/PO	アクション	アグリゲートぶ	リンク・	ポートタイプス	VLAN ~	許可されたVLAM	$\#- \models \rtimes \not = - \dots \lor$	PoE ~	4(−) ×	RSTP
(イッチ	1	/1		1	自動/リンク	アクセス	1		有効化	無効化	20	有効化
(イッチクライアント	2	/ 2			自動/リンク	アクセス	1		有効化	無効化	20	有効化
イッチボート	3	/ 3		1	自動/リンク	アクセス	1	6	有効化	無効化	20	有効化
トポロジ	4	/ 4			自動/リンク	アクセス	1		有効化	無効化	20	石勋化
フロブ計画	5	/ 5		-	自動/リンク	アクセス	1	-	有効化	無効化	20	有効化
改定 >	6	/6			自動/リング	アクセス	1	α	有効化	無効化	20	有効化
	7	/7		1	自動/リンク	アクセス	1	-	有効化	無効化	20	有効化
- 4- F	8	/ 8		-	自動/リング	アクセス	1		有効化	無効化	20	有効化
n7 >	9	/9		1	自動/リンク	アクセス	1	-	有効化	無効化	20	有効化
9X74 >	10	/ 10			自動/リンク	アクセス	1		有効化	無効化	20	石刻化
	11	/ 11		-	自動/リンク	アクセス	1	-	有効化	無効化	20	有夠化
	12	/ 12			自動/リング	アクセス	1		有効化	無効化	20	有効化
	13	/ 13	-	1	自動/リング	アクセス	1	-	有効化	無効化	20	有効化
	14	/ 14		e.	自動/リング	アクセス	1	a.	有効化	無効化	20	有夠化
	15	/ 15		1	自動 / 1Gbps	アクセス	1	1	有効化	無効化	20	有効化
	16	/ 16	\odot		自動/リンク	アクセス	1		有効化	無効化	20	有效化

図 5-30 モニタ-スイッチ-スイッチポート

■ 対象範囲の指定 / ポートの検索

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

■ レポート項目

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

SWITCH/PORT

ポートタイプ

許可された VLAN

ポートステート

• アクセスポリシー

アグリゲートリンク

• VLAN

PoE

• LBD

• DDP

ポート

- ミラー
 LLDP
 ポート名
 - 小 1 1
 - Rx ブロードキャストパケット
 Tx ブロードキャストパケット

 - ・ Rx マルチキャストパケット
 - ・ Tx マルチキャストパケット
 - Rx バイト数
 Tx バイト数

- RSTP
- Rxパケット数
 Txパケット数
- ・ 合計バイト数
- ポートシャットダウンスケジュール
- PoE 供給スケジュール

- 「SWITCH/PORT」では、スイッチ名とポート番号を表示します。

- 「アグリゲート」では、ポートチャネルグループのリンクアグリゲーションタイプ(Static/LACP/-)を表示します。
- 「リンク」では、ポートのリンク設定とリンク状態を表示します。

第5章 モニタ

■ 特定ポートの詳細

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

ポートの詳細画面では、以下の情報が表示されます。

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

Overview Port15					
iGbps 📒 10/100Mpbs	Disconnected Disabled	Mirror 🗧 Error 📪 PoE+3	firror		
1 3 5 7 9 2 4 6 8 10	11 13 15 17 19 12 14 16 18 20 17 18 19 Combo	20			
ペートトラフィック利用率					
MB				Rx (MB)	📕 Tx (MB) 📲 合計 (MB)
1					
0 17:00 18:00 19:00	20:00 21:00 22:00 23:00 00:00 01:0	00 02:00 03:00 04:00 05:00	06:00 07:00 08:00	09:00 10:00 11:00 12:0	10 13:00 14:00 15:00
現在の設定					
設定を使用	スタンドプロン				
クロス属性					
スイッチポート	test / 1				
	Update a ports				
リンク(RuJ45)	自動 ~	DDP	有効化	~	
ポートステート	有効化 ~	ボートシャットダウンスケジュー ル	unscheduled	~	
ポートタイプ	ブクセス	LBD	無効化		
RSTP	有効化	STP H - F	無効化	~]	
VI. 6 N	 T				
	* * *				
アクセスポリシー	無効				
アンクロス属性					
<i>*</i> /一十名		リンクアグリゲーショングループ	-		
: 7-					
				適	1
					3
$\overline{\tau} - g \times$					
	- 111日本 - 1111		4-1-5-	Walk a h a) ナ	
4 ⁻	RSTP -		T - F A T - F	POE ではない	
	LBD -		リンクネゴシエーション	1Gbps全二重	
リンクアグリゲーション	イグループ -				
	說明 Access Port using Access VLAN 1				



				タイムフレーム Last 15 Minuty
	合計	Rx	Tx	$ u = + (R_X, T_X) $
Total Traffic	2904	2683	221	
Broadcast	1954	1954	0	
Multicast	581	581	0	
CRC Error	0	0		-
Discard	1347	1347	0	
Fragment	0	D		2
Collision	0		o	
Error	0	0	0	

				検索	S方法 Client MAC Address 〜	e.g. 30:10: 04:16:53:20
No.	クライブントMACアドレス	クライブントIPマ4ブドレス	VLAN	LLDP	製造	最終更新情報
1	00:00:29:25:44:3b		1	-	-	2022/11/17 11:27:5
2	oo:1c:fo:1ftae:bf		1			2022/11/17 11:27:5
3	00000:40:68:0b:4e		1			2022/11/17 11:27:5
4	6c:19:8f:1b:87:8b		1			2022/11/17 11:27:5
5	6c:19:8f:1b:87:89		1		-	2022/11/17 11:27:5
6	90:d6:43:0a:34:01		1		-	2022/11/17 11:27:5
7	90:d6:43:0a:35:13		1		-	2022/11/17 11:27:5

第6章 トポロジ

トポロジ画面では、ネットワーク内のデバイス間のトポロジ関係を表示します。

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



図 6-1 トポロジ

■ 詳細情報の確認

デバイスのアイコンをダブルクリックすると、右側にデバイスの情報が表示されます。 デバイス情報の ・ をクリックすると、デバイスの詳細画面が開きます。 リンクをダブルクリックすると、リンク情報が表示されます。

■ トポロジの表示の調整

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

デバイス情報

デバイス情報には以下の項目が表示されます。





項目	説明
	アクセスポイント
名前	サーバ上でアクセスポイントを識別するための名前を表示します。 ─ をクリックすると、デバイス詳細画面に遷移
	します。 AP 名はサイトに対して一意である必要があります。
ステータス	AP の接続ステータス(オンライン、オフライン)が表示されます。
	緑色はオンライン、赤色はオフラインを示します。
ローカル IP アドレス	IP アドレスを表示します。
MAC アドレス	アクセスポイントのシステム MAC アドレスを表示します。
モデル番号	アクセスポイントの型番を表示します。
ハードウェアバージョン	アクセスポイントのハードウェアバージョンを表示します。
ファームウェアバージョン	ファームウェアバージョンを表示します。
CPU 使用率(%)	アクセスポイントの CPU 使用率を表示します。
メモリ使用率(%)	アクセスポイントのメモリ使用率を表示します。
アップロード	アクセスポイントのアップロードトラフィックを表示します。
ダウンロード	アクセスポイントのダウンロードトラフィックを表示します。
稼働時間	前回の起動または再起動後からの AP の稼働時間を表示します。
設置場所	デバイスの設置場所を表示します。
	スイッチ
名前	サーバ上でスイッチを識別するための名前を表示します。 ── をクリックすると、デバイス詳細画面に遷移します。
	スイッチ名はサイトに対して一意である必要があります。
ステータス	スイッチの接続状態(オンラインまたはオフライン)を表示します。
	緑色はオンラインを示し、赤色はオフラインを示します。
ローカル IP アドレス	IP アドレスを表示します。
MAC アドレス	スイッチのシステム MAC アドレスを表示します。
モデル番号	スイッチの型番を表示します。
シリアル番号	スイッチのシリアル番号を表示します。
IGMP スヌーピング	IGMP スヌーピングのステータス(有効化 / 無効化)を表示します。
ハードウェアバージョン	スイッチのハードウェアバージョンを表示します。
ファームウェアバージョン	スイッチのファームウェアバージョンを表示します。
CPU 使用率(%)	スイッチの CPU 使用率を表示します。
タイムゾーン	デバイスが属するタイムゾーンを表示します。
RSTP ルート	ルートブリッジとそのスパニングツリープライオリティを表示します。表示形式は以下の通りです。
	・「ルートは [X]/ ルートブリッジプライオリティ:Y」- [X] はルートスイッチのデバイス名(システム名)を表します。
	[Y] はルートスイッチのブリッジプライオリティを表します。
	・「RSTP は無効化されています。」- スイッチで RSTP が有効になっていません。RSTP は、ポートではなくスイッチ
	でのみ有効になります。
	・「-」- スイッチがオフライン、または情報を中継しないことを意味します。
LBD	スイッチの LBD 設定のステータス(有効化 / 無効化)を表示します。
DDP	スイッチの DDP 設定のステータス(有効化 / 無効化)を表示します。
稼働時間	前回の起動または再起動後からのスイッチの稼働時間を表示します。
設置場所	スイッチの設置場所を表示します。

リンクの作成

デバイス間のリンクを手動で定義することができます。

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



3. リンクが作成されると、リンク設定画面が表示されます。

リンクメ	タイプ 💿 一般的	約なリンク	○ LACPリンク			
リンクディ	イス 172.16.1	.47 17	2.16.1.36			
リンクボ	- F Port 1	~	リンク先	Port 1	~	
クリスト						
No 9	リンクポート	リン	2 先	検出	直近の更新	
			Ø			
		データが	見つかりません	でした		
					OT	A 11 12

図 6-4 リンク設定

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

トポロジ情報の設定と表示

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

各アイコンの説明は以下の通	Ŋ	で	す	•
---------------	---	---	---	---

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

第7章 フロア計画

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

1. "ここ"をクリックします。

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

<nuclias< th=""><th>Default</th><th>10:34:26 2023-03-08</th><th>ß</th><th>2</th><th>*</th><th>JP ~</th></nuclias<>	Default	10:34:26 2023-03-08	ß	2	*	JP ~
$\textcircled{\mathscr{G}} \mathscr{I} \mathscr{I} \mathscr{I} \mathscr{I} = \exists^{\mathcal{I}} = I^{\mathcal{I}}$						
<u>107</u> ≈ = Ø →						
Ø 2 □ 7 計画						
🗙 💥 🔹 🔹 👌						
₩ ¤ % >						
50 vata >						
	フロアブランのマップが存在しません。最初にフロアブランのマップを追 加してください。 マップファイルを追加できます、ここ					

図 7-1 フロア計画

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

〔❷ フロア計画のマップ	でを作成		×
名前*	例: 3Fマップ		
サイト*	Site1	~	
ネットワーク*	Networkı	v	
画像をアップロード *			
	uni Ma es	ドラッグ&ドロップ	
	hele z -	こい (ワリカル)かんは、ついば、うりない しくけ ちょういん ちしくは クリック 両像を選択	
			保存 キャンセル

図 7-2 フロア計画のマップを作成

第7章 フロア計画

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



5. 「保存」をクリックします。

デバイスアイコンは、接続ステータスの色(オンライン:緑、オフライン:赤)で表示されます。 デバイスアイコンの上にマウスオーバーすると、デバイス情報(名前、モデル番号、IP アドレスなど)を確認することができます。
第8章 設定

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

プロファイルの作成

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

<nuclias connect</nuclias 	Default						10:36:23	2023-03-08	JP
(K) ダッシュボード	全てのサイト レ	全てのネットワーク ッ 良合語	アー ト2ネットワーク カー	クセスポイント:合計 ライアント:合計 0	1/1オンライン スイ クラ	ッチ:合計 1/1 オンワー イアント・会計 22	í >		ネットワークを追加
100 H=- 9 >									
トポロジ	サイト名 🔺	> ネットワーク名 ▲ >	ネットワークID×	合計デバイス >	オンラインデバ…~	クライアント マ	プロファイル	校出	ブクション
○ フロブ計画	Site1	Networkı		0	o	0	r d e	9	e t
	Site2	Network2		2	2	23	C D B	Q	2 1
🗙 ike 🔹 🔪									
 プロファイルを作成 									
 プロファイル設定 									
 ・ アデームサエアの更新 SSL語明書 									
• 決済代行システム									
「」 レポート ・									
50 VX74 >									

図 8-1 プロファイルを作成

既存のネットワークに対しては、以下の操作を実行することができます。

項目	説明
プロファイルを編集 🗹	選択したサイトのプロファイル設定画面を開きます。セキュリティ、アクセスコントロール、ユーザ認証などの設定を
	編集できます。
このネットワークにプ	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(*.dat)をローカルディレクトリにエクスポートします。
イルをエクスポート 📑	
検出2	「ネットワーク設定を検出」画面を開きます。この画面から、L2 プロトコル層に配置されているデバイス、または特定の
	IP アドレス / プレフィックスサブネット IP を検索できます。
	 (1) 条件を定義し、「次へ」をクリックします。
	(2) 「桸出開始」をクリック」て、デバイスを検出します(「設定可能」「管理」々ブ)
ラットロークも毎年に	「ネットワークを編集」両両を開きます。この両面から、ネットワーク設定を編集したり、新しいサイトまたけ既友のサ
「イツトワークを編集」	「ホノーノーノを補未」面面を用さます。この面面から、ホノーノーノ政定を補未したり、新しいサイトまたは成件のケーイトに移行した日本ステレビできます
ネットワークを削除 💼	選択したネットワーク設定を削除します。

第8章 設定

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。

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th></th><th>10:36:23</th><th>3 2023-03-08</th><th>ß</th><th>2</th><th>🗙 JP 🗸</th></nuclias<>	Default						10:36:23	3 2023-03-08	ß	2	🗙 JP 🗸
$(\overbrace{k}) \ \ \ \ \ \ \ \ \ \ \ \ \$	全てのサイト ッ 全て	のネットワーク > 日本	7 計2ネットワーク 。	クセスポイント:合計	L/1オンライン スイ	ッチ:合計 1/1 オンライ				ネットワ	ークを追加
100 €= % >				7472F:mir0	25	(472)):()計23					
	サイト名 ▲ ~	ネットワーク名 🔺 👻	ネットワークID×	合計デバイス >	オンラインデバ…>	クライアント マ	プロファイル	校出	7	クション	
Q 707780	Site1	Networkı		0	0	0	RDB	Q	[Z ū	
	Site2	Network2		2	2	23	C D B	Q.	[2 1	
🗙 ike 🗸 🗸											

図 8-1 プロファイルを作成

2. 「ネットワークを追加」画面で、以下の項目を設定します。

「次へ」をクリックして次に進みます。前のページに戻るには「戻る」をクリックします。

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

newSite v	
Networkı	
ネットワークIDはREST APIに使用されます。	オー キャンセル
	newSite マ Network1 ネットワークIDはREST APIに使用されます。

図 8-2 ネットワークを追加

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

一般設定		1
国	Japan	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo \checkmark	
デバイスタイプ	アクセスポイント スイッチ ネットワーク内で管理されるデバイスタイプを選択してください。	
アクセスボイント		,
スイッチ		

図 8-3 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。

「次へ」をクリックして続行します。設定プロセスを中止するには「キャンセル」をクリックします。

🗙 ネットワーク設定を検出	×
レイヤ2	
レイヤ3(IP)	
ーう選択 ・	+
	戻る 次へ キャンセル

図 8-4 ネットワーク設定を検出

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

秋田開	治 管理							
		デバイスタイプ	アクセスポイント ×			MACT ドレス	キーワード'を検索	ه
	ステート	✓ IPアドレス	✓ MACアドレス	∨ モデル番号	~ 結果	をインポート	 NMS URL 	~ ネット
	管理	2012/014	a óciósweta.a	7 DAP-3666			1110 ⁴ L 10:8443	NetworkA
						_		
ネットワー	- <i>7 7</i> ¤ 7 7 <i>A</i>	ルをインポート:	admin	····· &	· / ンポ	•		
*>+7-	-970774	ルをインボート:	admin	••••• &	174	-	戻る 適 用と網	ار به

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

7. 右上の「×」ボタンをクリックして画面を閉じます。

プロファイル設定

プロファイル設定機能では、既存のネットワークを管理することができます。

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

< nuclias	Default						10:3	7:06 2023-03-08	2		×	
(i) ダッシュポード												
B += 4	C 707712		プロファイル > Site2 > Network2									
20	Site1		設定をアップロード									
	Site2		Bednine A. L.T	Part of the state								
O THE PARTY	Ø Network2		開始時間	BRY ~								
3 2 0 7 mm	アクセスポイント											
2 RE -	スイッチ								這川	29	τ	
 プロファイルを作成 												
 プロファイル設定 			実行ステータス									
• ファームウェアの更新												
 SSL证明書 			追用ステータス	1/2								
 決済代行システム 			44.00									
<u> ネート ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・</u>		<	新采	実行時間 マニー・	名前	✓ IPブドレス	Y MAC7ドレス	× モデル番号	* 結果	~		
				2023-03-08 10:26:26	dap2680	custa-4	-coalcoloc3	DAP-2680	成功			
- vx74 ->												

図 8-6 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。

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

「クリア」をクリックして、定義済みの設定を削除します。

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

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

■ ネットワークの各種設定

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

- アクセスポイント
- 「アクセスポイント SSID」
- 「アクセスポイント VLAN」
- 「アクセスポイント 帯域幅の最適化」
- 「アクセスポイント RF 最適化」
- 「アクセスポイント スケジュール」
- 「アクセスポイント デバイス設定」
- 「アクセスポイント パフォーマンス設定」
- 「アクセスポイント WLAN パーティション」
- 「アクセスポイント ワイヤレスリソース」
- スイッチ ※スイッチ製品は未サポートです。
- 「スイッチ 一般 RADIUS サーバ」
- 「スイッチ 一般 時間プロファイル」
- 「スイッチ 基本」
- 「スイッチ IPv4 ACL」
- 「スイッチ アクセスポリシー」
- 「スイッチ ポート設定」
- 「スイッチ SNTP 設定」

アクセスポイント - SSID

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

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th>10:3</th><th>7:19 2023-03-08</th><th>\$ 2</th><th>×</th></nuclias<>	Default					10:3	7:19 2023-03-08	\$ 2	×
ダッシュポード									
€=.9 >	CP Jujyin	プロファイル > Site2 > Netwo	ork2 > アクセスポイント	> SSID					
	Sitez	インデックス ▲ ~	周波数带 ▲ ~	SSID	> セキュリティ 、	デクセスコントロー	× ユーザ認証	ブクション.	
00 F##99	③ Network2	721-21	0 4GHz	dlinknetast	WDA.c.y+w	445 (2)h (1)-	ter toh fir	2	
● フロブ計画	アクセスポイント		2.4042	uninkiietest	WPAD - 7 7 10	無効化	THE NUTLE	2	
¥ 設定 →	SSID	プライマリ	5GHz 1	dlinknctest	WPA-パーソナル	無効化	無効化	2	
 プロファイルを作成 プロファイル設定 ファームウェアの更新 	VLAN 帯域編載適化 RF試道化 スケジュール								
 SSL証明書 決済代行システム 	デバイス設定 パフォーマンス								
レポート >	WLAN $r^2 = \vec{\tau} + \vec{v} = \vec{v}$	くセキュリティ							^
🗐 ¤ // 🔹 >	×4.97	ワイヤレス設定							
50 VXF4 ->		140 aug	股带 2.4GHz	~		インデックス	SSID 1 \sim		
		SS	ID *		SSID	ブロードキャスト	有効化 マ		
		セキュリ	ティープンシス	~ 47	WMM	(Wi-Fiマルナメデ イブ)			
		$\beta_{ij} = 0$	シグ 無効化 、	× この機能はWiFi4E	日でのみ利用可能です。				
		セキュリティ設定							
		10	8化 無効化 、			キーサイズ			
		4-9.	IT HEY						

図 8-7 プロファイル設定 - アクセスポイント - SSID

セキュリティ

A 477 1 4 47 11 10 10 10			
1 T V ARKE			
周波数带	2.4GHz V	インデックス	SSID 1 V
SSID *		SSIDブロードキャスト	有効化 🗸
セキュリティ	オープンシステム 🗸	WMM (Wi-Fiマルチメデ イブ)	有効化 🗸
高速ローミング	無効化 マ この機能はWiFl4EUで	のみ利用可能です。	
キュリティ設定			
暗号化	無効化 🗸	キーサイズ	64ビット V
	HEX		
キータイプ			

図 8-8 SSID - セキュリティ

「セキュリティ」セクションでは、以下の設定項目が表示されます。

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

項目	説明
セキュリティ	ドロップダウンメニューをクリックして、ワイヤレスセキュリティプロトコルを選択します。
	・ 選択肢:「オープンシステム」(事前共有キー不要)
	[Enhanced Open]
	Enhanced Open + Open J
	「WPA-パーソナル」
	「WPA- エンタープライズ」(RADIUS サーバが必要)
	「802.1X」
WMM	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。
(Wi-Fi マルチメディア)	「ワイヤレスモード」が「802.11g/b 混在」または「802.11a のみ」に設定されている場合に指定可能です。
高速ローミング	高速ローミング機能を有効または無効にします。
	注意 802.11k/r のみサポートしています。802.11v はサポートしていません。
	注意 日本語のメッセージ(「この機能は WiFi4EU でのみ利用可能です。」)は誤りですので、無視してください。

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

■ 新規 SSID の追加

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

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の C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。

設定を中断する場合は、「キャンセル」をクリックします。

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

補足 「高速ローミング」、「Enhanced Open」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」をご確認ください。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」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

暗号化	有効化 ~		キーサイズ	64ビット マ
キータイプ	HEX 🗸			
> 1418		2-		

図 8-9 SSID - セキュリティ (オープンシステム)

項目	説明
	セキュリティ設定
暗号化	ドロップダウンメニューをクリックして、WEP オープンシステムの暗号化を有効または無効にします。
キーサイズ	ドロップダウンメニューをクリックして、WEP キーのサイズを選択します。
	・ 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「WPA- パーソナル」に設定した場合

$WPA- \in - \Vdash$	自動 (WPAもしくはWPA〜	暗号化タイプ	自動 ~
パスフレーズ*	66	グループキー更新問題	2600

図 8-10 SSID - セキュリティ(WPA- パーソナル)

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

補足 「WPA3」は、製品によりサポート可否が異なります。詳細は「【付録】 機能別サポート製品 / バージョンについて (p.141) 」をご確認ください。

■「セキュリティ」項目を「WPA-エンタープライズ」に設定した場合

$\mathrm{WPA}{=}-\mathbb{K}$	自動 (WPAもしくはWPA〜			
暗号化タイプ	「山助」	グループキー更新問題	3600	
ネットワークアクセス保 護	無効化 ~			
プライマリRADIUSサーバ設	定			
RADIUSサーバ*		RADIUSポート*	1812	
RADIUSシークレット*	Ø			
バックアップRADIUSサーハ	設定(オブション)			
RADIUS #		RADIUSポ−ト	1812	
RADIUSシークレット	95			
プライマリアカウンティング	"サーバ設定			
アカウンティングモード	無効化 ~			
アカウンティングサーバ		アカウンティングポート	1813	
アカウンティングシーク レット	Ŕ			
バックアップアカウンティン	/グサーバ設定(オプション)			
アカウンティングサーバ		アカウンティングポート	1813	

図 8-11 SSID - セキュリティ (WPA- エンタープライズ)

項目	説明
	セキュリティ設定
WPA モード	ドロップダウンメニューをクリックして、WPA モードを選択します。 ・ 選択肢:「自動 (WPA もしくは WPA2)」「WPA2 のみ」「WPA3 のみ」
	注意 DAP-3666 は WPA3-エンターフライスは未サホートです。
暗号化タイプ	ドロップダウンメニューをクリックして、暗号化タイプを選択します。 ・ 選択肢:「自動」(「自動 (WPA もしくは WPA2)」を指定した場合) ・ 選択肢:「AES」(「WPA2 のみ」「WPA3 のみ」を指定した場合)
グループキー更新間隔	WPA グループキーの更新間隔の値を入力します。
ネットワークアクセス保護	ネットワークアクセス保護機能を有効または無効にします。

項目	
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。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットを入力します。
プライマリア	7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を入力します。



補足

補足 Radius Request は AP から送信されます。

「ネットワークアクセス保護」、「WPA3」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョ ンについて (p.141)」をご確認ください。

■「セキュリティ」項目を「802.1X」に設定した場合

:キュリティ設定					
キー更新間隔	300				
ライマリRADIUSサーバ副	定				
RADIUS ⊕ − ×*			RADIUSポート*	1812	
RADIUSシークレット*		N.			
ックアップRADIUSサーィ	*設定(オブション)				
RADIUS + − ×			$\operatorname{RADIUS} \vartheta^{t} = \Bbbk$	1812	
RADIUSシークレット		do D			
"ライマリアカウンティング	ブサーバ設定				
アカウンティングモード	無効化 ~				
アカウンティングサーバ			アカウンティングポート	1813	
アカウンティングシーク レット		Ø			
『ックアップアカウンティン	ノグサーバ設定(オブシ	∃ <i>∨</i>)			
アカウンティングサーバ			アカウンティングポート	1813	

図 8-12 SSID - セキュリティ (802.1X)

項目	説明
	セキュリティ設定
キー更新間隔	キーの更新間隔の値を入力します。
· · · · · · · · · · · · · · · · · · ·	プライマリ RADIUS サーバ設定 / バックアップ 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。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットパスフレーズを入力します。
プライマリ	アカウン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

CL		
アクション	無効化 ~	
MACアドレス	XX:XX:XX:XX:XX 説明 最大長32 (オプション) 追加	
MACアドレスリストをア ップロード	ブラウザ ブラブロード ダウンロード	
	2.4GH2帯のMACアドレスリストの最大数は512です.残り512	
	No. MACアドレス * 説明 * アクション	
	データが見つかりませんでした	
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 道加	
	IPフィルタの最大エントリ数は64です。,残り64	
	10-7 (1, 7 ,	

図 8-13 SSID - アクセスコントロール

「アクセスコントロール」セクションでは、以下の設定項目が表示されます。

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

■ 新規 SSID の追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの m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。



第8章 設定

ユーザ認証

認証タイプ	Webリダイレクトのみ マ	アイドルタイムアウト (2~1440)	60 分	
IPインタフェース設定				
IPインタフェース設定は、VLAN	>IPインタフェースリスト内で設定される必要が	ぶあります。		
IPIFステータス	無効化 >			
VLAN ID (VID)	1			
IPアドレスの取得	スタティックIPアドレス(手動) 🗸 🗸			
IPプドレス		サブネットマスク		
ゲートウェイ		DNS		
✓ Webリダイレクショ:	X			
Web++ ().*	http://			

図 8-14 SSID - ユーザ認証

「ユーザ認証」セクションでは、以下の設定項目が表示されます。

項目	
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」「クリックスルー」「ソーシャルログイン」
アイドルタイムアウト	クライアントがアクセスポイントから切断され、指定した時間が経過すると再認証が必要となります。本値は、経過
(2~1440)	後に STA を切断する時間ではなく、再接続に際して再認証が必要となる時間を設定します。
	注意 Nuclias Connect の「アイドルタイムアウト」(本項目)が、DAP-2680/DAP-3666 の WebUI における「Session
	Timeout」に該当します。
同時ログインを有効化	同時ログインを有効または無効に設定します。
	「ユーザ名 / パスワード」「リモート RADIUS」「LDAP」「POP3」を選択した場合に設定します。
セッションタイムアウト	ログイン後、指定時間が経過すると再認証が必要になります。
(2~1440)	「ユーザ名 / パスワード」「リモート RADIUS」「LDAP」「POP3」「クリックスルー」を選択した場合に設定します。
許可 (1~720)	ワイヤレスクライアントが1日に再ログインできる回数を定義します。開始時刻は 0:00 です。
	「セッションタイムアウト」を有効化した場合に設定します。
間隔 (0~720)	セッションタイムアウトの制限回数を超えた後、無線クライアントがログインできるようになるまでの期間を定義します。
	「セッションタイムアウト」を有効化した場合に設定します。
	ホワイトリストを有効化(認証タイプが「Web リダイレクトのみ」以外の場合)
ホワイトリストを有効化	チェックを入れると、ホワイトリスト機能が有効になります。
MAC アドレス	ホワイトリストに登録するネットワークデバイスの MAC アドレスを入力し、「追加」をクリックしてアドレスをホワ
	イトリストテーブルに追加します。
ホワイトリストファイルを	「ブラウザ」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。
アップロード	「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードす
	るには、「ダウンロード」をクリックします。
	IP インタフェース設定
IRIF ステータス	IP インタフェース設定は、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタ
	フェースリスト内で設定される必要があります。
VLAN ID (VID)	IP インタフェース設定は、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタ
	フェースリスト内で設定される必要があります。
IP アドレスの取得	IP インタフェース設定は、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタ
	フェースリスト内で設定される必要があります。
IP アドレス	P インタフェース設定は、設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタ
	フェースリスト内で設定される必要があります。
サブネットマスク	IP インタフェース設定は、 設定 > ブロファイル設定 > サイト > ネットワーク > アクセスボイント > VLAN > IP インタ
	フェースリスト内で設定される必要があります。
ケートウェイ	IPインタノェース設定は、 設定>フロファイル設定>サイト>ネットワーク>アクセスボイント> VLAN> IPインタ
	ノエースリスト内で設定される必要かあります。
DN2	ビインダノエース設定は、 設定>フロノアイル設定>サイト>ネットワーク> パクセスホイント> VLAN > I P インタ
	ノェームリムト内 () 設定される必要かめります。

項目	説明
	ユーザ名 / パスワード(認証タイプが「ユーザ名 / パスワード」の場合)
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力します。
	ユーザ名とパスワードを入力した後、「追加」をクリックします。入力値をリセットする場合は「Clear」をクリック
	します。
ユーリ名/ハスワートノア イルをアップロード	「ノブワリ …」をクリックして、ローカルコノヒューダに保存されにユーリ治ノハスワートリストのノアイルを迭折し ます 「アップロード」をクリック」てユーザリストを再新します。田在のユーザリストをダウンロードするには「ダ
	「より、「ケノノロー」「」をクリックしてエーテラス」を定称しより、現在のユーテラス」をクリックロードするには、ケーウンロード」をクリックします。
	リモート RADIUS(認証タイプが「リモート RADIUS」「MAC アドレス」の場合)
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットを入力します。
リモート RADIUS タイプ	RADIUS サーバのタイプを選択します。
	・ 選択肢:「SPAP」「MS-CHAPv2」
NAS ID	NAS ID を有効または無効にします。有効にした場合、NAS ID を入力します。
	NASID 設定は「リモート RADIUS」選択時のみ設定可能です。3 台の RADIUS サーバで共通の設定となります。
	アカリノティンクモートを有効または無効にします。「リモート KADIUS」 選択時のみ設定可能です。
	アカウノティングサーバのIPアドレスを入力します。「リモート KADIUS」 選択時のみ設定可能です。
	アカウノティングリーハの小一下番号を入力します。「リモート RADIOS」 迭状時のみ設定可能です。
	「ノガサンノインソリーハロシークレッドを入力しより。」リヒードINADIOS」 医抗時のの設定可能です。
	LDAP(「認証タイプが「LDAP」の場合
サーバ	LDAP サーバの IP アドレスを入力します。
ポート	LDAP サーバのポート番号を入力します。
認証モード	ドロップダウンメニューをクリックして、認証モードを選択します。
	・ 選択肢:「シンプル」「TLS」
ユーザ名	LDAP データベースにアクセスして検索できる管理者のユーザ名を入力します。
パスワード	LDAP データベースにアクセスして検索できる管理者のバスワードを入力します。
	LDAP テーダベースのベースドメイン名を入力します。
アカワント周任	アカワノトの属性を入力します。
	「官哇省の名前を入力します。」日勤コビー」にチェックを入れると、入力済みの他のハウメータの値が反映されます。
++/\\	
<u> ポート</u>	$POP3 \pm -i \int \sigma x^2 - b = \pi + 2 \int \sigma x^2 - b = $
 接続タイプ	ドロップダウンメニューをクリックして、接続タイプを選択します。
	 ・選択肢:「なし」「SSL/TLS」
	· パスコードリスト(認証タイプが「パスコード」の場合)
パスコードリスト	このネットワークに割り当てられたフロントデスクユーザによって生成されたパスコードを表示します。
	外部キャプティブポータル(認証タイプが「外部キャプティブポータル」の場合)
サーバアドレス	ドロップダウンメニューから「http://」または「https://」を選択し、キャプティブポータルの URL を入力します。
	Web リダイレクション(認証タイプが「MAC アドレス」以外の場合)
Web リダイレクション	チェックを入れると、Web サイトのリダイレクト機能が有効になります。
Webサイト	ドロップダウンメニューから「http://」または「https://」を選択し、リダイレクト先 URL を入力します。
	ウォールガーデンを有効化(認証タイプが「Web リダイレクトのみ」以外の場合)
ウォールガーデンを有効化	チェックを入れると、ウォールガーデン機能が有効になります。
ウォールガーデン範囲	ウォールガーデンの範囲を IP アドレス、IP アドレス / サブネットもしくはドメイン名を入力します。
ウォールカーテンノアイル キマップロード	-フラワザ…」をクリックして、ローカルコンビュータに保存されたワオールカーテン範囲リストのノアイルを選択し ます、「アップロード」をクリックしていてんを再新します。現在のリフトをダウンロードするには、「ダウンロード」
	より。「アックロート」をクリックしてリストを更新しまり。現任のリストをダリンロートするには、「ダリンロート」 をクリック ます。
	<u></u>
Facebook	ソーシャルログインの資格情報として Facebook を使用します。
Google	ソーシャルログインの資格情報として Google を使用します。
スプラッシュページカス	、 タマイズ(「認証タイプが「Web リダイレクトのみ」「外部キャプティブポータル」「MAC アドレス」以外の場合)
認証タイプ	認証タイプを選択します。

項目	説明
テンプレートを選択	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。
	・「エディタ」をクリックして、スプラッシュページを編集します。
	・「ログインファイルをアップロード」をクリックして、新しいスタイルをアップロードします。
	・ 💼をクリックして、選択したスタイルを削除します。
	・ 🔃 をクリックして、スタイルテンプレートをダウンロードします。

■ 新規 SSID の追加

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

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の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。

設定を中断する場合は、「キャンセル」をクリックします。

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



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

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



注意

ド (p.76)」を参照してください。

認証設定の一部機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」 をご確認ください。

ホットスポット

ホットスポット2.0			^
この機能は、互換性のある型番と ホットスポット ⑦	:特定のファームウェアバージ	「ヨンでのみ使用できます。この機能をサポートしていない場合	?、APはSSIDを作成しません。
ホットスポット2.0	無効化 ~	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	無夠化 🗸
L2TIF	無効化 ~		
インターワーキング			
インターワーキング	有効化 ~	アクセスネットワークタ イプ	プライベートネットワーク
インターネット	石効化 ~	ASRA	無効化 ~
ESR	無効化 ~	UESA	無効化 ~
$\operatorname{Venue} \mathcal{I} \mathcal{N} - \mathcal{I}^{\bigstar}$	0	Venue $\ensuremath{\ensuremath{\mathcal{I}}}\xspace \ensuremath{\mathcal{I}}\xspace $	0
Venue 名	英語 🗸	:	
HESSID	XX:XX:XX:XX:XX		
WANメトリック			
WANリンクステータス	リンクアップ 〜	WAN対称リンク	الله (oxo1) ب
WAN带城	いいえ(0x00) ~	WANメトリックダウンロ	0

図 8-15 SSID - ホットスポット 2.0

「ホットスポット 2.0」セクションでは、以下の設定項目が表示されます。

項目	説明			
ホットスポット				
ホットスポット 2.0	ドロップダウンメニューをクリックして、ホットスポット 2.0 機能を有効または無効にします。			
OSEN	ドロップダウンメニューをクリックして、OSEN(OSU Server-Only Authenticated L2 Encryption Network)のセキュ			
	リティ認証を有効または無効にします。			
クロス接続を許可	ドロップダウンメニューをクリックして、クライアントのクロス接続を有効または無効にします。			
P2P を管理	ドロップダウンメニューをクリックして、P2P 管理を有効または無効にします。			
DGAF	ドロップダウンメニューをクリックして、DGAF(Downstream Group-Addressed Forwarding)を有効または無効に			
	します。有効にすると、AP はダウンストリームのグループアドレスフレームを転送することができます。			
プロキシ ARP	ドロップダウンメニューをクリックして、プロキシ ARP を有効または無効にします。			
L2TIF	ドロップダウンメニューをクリックして、L2TIF(Layer 2 Traffic Inspection and Filtering)を有効または無効にします。			
	インターワーキング			
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タイ	アクセスネットワークのタイプを選択します。			
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	この接続を介したインターネットの利用を有効または無効にします。			
ASRA	ドロップダウンメニューをクリックして、ASRA(Additional Steps required for Access)を有効または無効にします。			
ESR	ドロップダウンメニューをクリックして、ESR(Emergency services reachable)を有効または無効にします。			
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。			
	 ・ 設定可能範囲:0-255 			
Venue タイプ	Venue タイプの値を入力します。			
	 ・ 設定可能範囲:0-255 			
Venue 名	言語を選択し、Venue 名を入力します。			
HESSID	Homogenous Extended Service Set (ESS) ID を入力します。サービスプロバイダネットワークを識別するために使用			
	されます。			

百日	≣ĞAB
	・ 選択時 ・「リンクアップ」「リンクダウン」「テストステートでのリンク」
L WAN 対称リンク	WAN 対称リンクのステータスを「はい」「いいえ」から選択します。「はい」の場合、アップロード/ダウンロードは
	同じ速度になります。
WAN 帯域	WAN 帯域のステータスを「はい」「いいえ」から選択します。アクセスポイントやネットワークがキャパシティの上
	限に達している場合、「はい」を選択します。
WAN メトリックダウン	WAN 接続のダウンロードスピードを kbps 単位で入力します。ダウンロードスピードが不明な場合は 0 を指定します。
ロードスピード (kbps)	
WAN メトリックアップリ	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。
ンクスピード(kbps)	
	リスト
ネットワーク認証タイプ	接続タイプを選択します。
	 ・ 選択肢: 「利用規約への同意」「オンライン登録をサポート」「http/https リタイレクション」」DNS リタイレクション」
利田司代たりフドレフタイ	「http/https リタイレクション」「UNS リタイレクション」の場合は、URL を人力する必要かめります。 利用可能を ID スドレスタイプを発行します。 ういしロークへの認証後、 キャレスポットのすぶし、 クやエバイルデ
利用り能な IP アドレスタイ プ	利用可能な IP アドレスタイノを迭折します。 イットワークへの認証後、 ホットスホットのオペレータやモバイルナ
	/ / / 人によつしこの/ トレスダイフが使用されより。 - 選切時・「アドレフタイプけ利田できません」「利田可能たグローバル IP アドレフ」「利田可能たポート制限され」
	・ 医小瓜・ファレスタイフは利用できるとい。」「利用可能なフローブル」「アレス」「利用可能なホート可服され」 た IPv/4 アドレス」「利田可能たシングル NAT さわたプライベート IPv/4 アドレス」「利田可能たダブル NAT さわた
	プライベート IPv4 アドレス 「利用可能なポート制限された IPv4 アドレスとシングル NAT された IPv4 アドレス
	「利用可能なポート制限された IPv4 アドレスとダブル NAT された IPv4 アドレス」「アドレスタイプの IPv4 可用性
	は不明です。」「利用可能な IPv6 アドレスタイプ」「アドレスタイプの IPv6 可用性は不明です。」
	ドメイン名リスト
ドメイン名	アクセスポイントの実行エンティティのドメイン名を入力し、「追加」をクリックします。
	ローミングコンソーシアム
ローミングコンソーシアム	サービスプロバイダや、ローミングパートナーのグループを入力し、「追加」をクリックします。ネットワークに接
	続する際に、それらのセキュリティ認証が使用されます。
	・ 入力可能な値:6 桁または 10 桁の 16 進数
	NAI レルムリスト
NAI LILL	■ をクリックして NAI レルムを入力します。BSS で利用可能な全ての NAL レルムを設定します。入力した NAI レル
	ムを削除する場合は、「■をソリックします。
EAP 方式	以下の手順でEAP 方式を設定します。
	1. EAP 方式を選択します。
	2. 🛨 をクリックして、認証 ID とパラメータタイプを指定します。認証 ID/ パラメータタイプを削除する場合は、
	<mark>-</mark> をクリックします。
	■ C / J / J / C C / C AP 古式のエントリを追加します
	BFC 4282 への進拠を「はい」「いいえ」から選択します。「追加」をクリックして、上記 NAI レルムの入力情報とと
	もにエントリとして追加します。
	3GPP セルラーネットワーク
MCC/MNC	アクセスポイントで利用可能な 3GPP セルラーネットワークを指定します。MCC とMNC の値を入力し、「追加」をクリッ
	クします。
	・ 設定可能範囲:000-999(「MCC」)、00-999(「MNC」)
	接続機能
IP プロトコル	IP プロトコルを選択します。
	・ 選択肢:「ICMP」「TCP」「UDP」
ポート番号	ポート番号を入力します。
ステータス	IP プロトコルのステータスを選択します。
	・ 選択肢:「閉じる」「オープン」「不明」
オペレータフレンドリー名	言語を選択し、オペレータフレンドリー名を入力します。Hotspot Venue オペレータの識別名です。
	OSU (Online Sign-Up)
OSU SSID	OSU SSID を入力します。本機能を使用すると、モバイルクライアントで利用可能なオンラインサービスを選択してオ
	ンラインサービスにサインインすることができます。
OSU サーバ URI	OSU サーバ URI を入力します。
	OSU 方式リスト
OSU 方式	言語を選択し、OSU 方式を入力します。「追加」をクリックして、OSU 方式を追加します。
OSU コンフィグ	OSU コンフィグ選択します。
	 ・ 選択肢:「コンフィグ1」「コンフィグ2」
IOSU 言語コード	IOSU言語コードを選択します。

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

■ 新規 SSID の追加

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

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の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。 設定を中断する場合は、「キャンセル」をクリックします。

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



注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.76)」を参照してください。

補足 「Hotspot2.0」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」を ご確認ください。

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

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

アクセスポイント - VLAN

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

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

nuclias	Default	10:39:31 2023-03-08	 Sector Sector
🎧 ダッシュボード			
	CP プロファイル	プロファイル > Site2 > Network2 > アクセスボイント > VLAN	
101 €=\$ >	Sites		
Land A	Site2	VLANステー	
	Metwork2 Metwork2	χ. χ	
🗿 7 0 7 tha	アクセスポイント		
V 21.2 -	SSID	VLANリスト ポートリスト VLANを追加/編集 PVID設定 IPインタフェースリスト IPインタフェースを追加/編集	
• プロファイルを作成	VLAN 2556615320 P	$ \text{VLAN VID} \bullet \lor \forall \text{VLAN } \$ \lor \forall \mathcal{I} \forall \forall \text{VLAN } \$ = \flat \lor \forall \mathcal{I} \lor \vartheta \forall \forall \text{VLAN } \$ = \flat \lor \forall \text{VLAN } \bullet = \flat \lor \lor \forall \text{VLAN } \bullet = \flat \lor \forall \text{VLAN } \bullet = \flat \lor \lor \forall \text{VLAN } \bullet = \flat \lor \lor \forall \text{VLAN } \bullet = \flat \lor \lor \lor \lor \lor \lor \lor \lor \lor $	77232
 プロファイル設定 	PELLAN	1 default 管理, LAN1, LAN2, LAN3, ブライマリ (2.4G), SSID1 (Ľ
 ファームウェアの更新 SSL証明書 決済代行システム 	スケジュール デバイス設定 パフォーマンス		
<u> レポート</u>	$\mathrm{WLAN}^{_{\mathcal{F}^{\mathcal{F}}}}=\bar{\mathcal{T}}^{_{\mathcal{F}^{\mathcal{F}}}}\neq \underline{\mathbb{P}}^{_{\mathcal{F}^{\mathcal{F}}}}$	x	
1 u / >	×4×+×3 ×4×+		
1 AFR 02			

図 8-16 プロファイル設定 - アクセスポイント - VLAN

「VLAN」画面には、以下の項目が表示されます。

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

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

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。

☑をクリックして、既存の VLAN を変更します。

■をクリックして、既存の VLAN を削除します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

ポートリスト

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

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

VLAN を追加 / 編集

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



PVID 設定

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



注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.76)」を参照してください。

IP インタフェースリスト

「IP インタフェースリスト」タブでは、IP インタフェース概要を表示できます。以下の情報が表示されます。 ・「VLAN VID」「VLAN 名」「IP アドレスの取得」「IP アドレス」

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

IP インタフェースを追加 / 編集

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

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

「保存」をクリックして、変更を保存します。

アクセスポイント - 帯域幅の最適化

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

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

<nuclias< th=""><th>Default</th><th></th><th>10:</th><th>39:42 2023-03-08</th><th>ß</th><th>×</th><th>JP v</th></nuclias<>	Default		10:	39:42 2023-03-08	ß	×	JP v
$\textcircled{(k)} \ \ \forall \ \forall \ \forall \ \ = \exists \ \ \forall - \forall$	19 JUTTAN	プロファイル > Site2 > Network2 > アクセス:	イント - 帯域幅設造化				
105 €= Ø >	Site1						
Pares	Site2	带域相最適化を有効化	無効化 >				
	Network2						
○ 2 □ 7 計画	アクセスポイント	ダウンリンク 帯域幅	80 Mbps				
🗙 ikiz — -	SSID VLAN	アップリンク 帯域幅	80 Mbps				
 プロファイルを作成 プロファイル設定 	带域标识道化	帯域幅最適化ルールを追加					
 ファームウェアの更新 COT SOULD 	スケジュール	ルールタイプ					
 35LR/File 決許代行システム 	デバイス設定 パフォーマンス	周波数带					
$\boxed{1} \lor d! - b \longrightarrow$	WLAN × · · · · · · · · · · · · ·	< \$\$\$104 × 7' = 7 ×					
国 ログ >	X4 y #	ダウンリンク スピード	80 Mbps v				
50 VXF4 >		<i>フップリンクスピード</i>	80 Mbps ~				
			ХШ Ф.У.Т.				
		周波数帯.× SSID × × タイプ	▼ ダウンリンクスピード ▼ ブッ	プリンクスピード × フ	「クション		

図 8-17 プロファイル設定 - アクセスポイント - 帯域幅設定

以下の設定項目が表示されます。

項目	説明
帯域幅最適化を有効化	ドロップダウンメニューをクリックして、帯域幅最適化機能を有効または無効にします。
ダウンリンク帯域幅	ネットワーク内のアクセスポイントのダウンリンク帯域幅の合計速度を入力します。
アップリンク帯域幅	ネットワーク内のアクセスポイントのアップリンク帯域幅の合計速度を入力します。
	帯域幅最適化ルールを追加
ルールタイプ	 ドロップダウンメニューをクリックして、ルールタイプを選択します。 ・「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% ドロップダウンメニューをクリックトアールールを適用する無線周波数帯域を選択します
	・ 選択肢:「2.4GHz」「5GHz 1」「5GHz 2(トライバンド)」
SSID インデックス	ドロップダウンメニューをクリックして、ルールを適用する SSID を選択します。
ダウンリンク スピード	各ステーションまたは指定された SSID に割り当てるダウンリンク スピードを入力します。
アップリンク スピード	各ステーションまたは指定された SSID に割り当てるアップリンク スピードを入力します。

■ 新規ルールの追加

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

■ 既存ルールの変更

ルールを変更する場合は、対象ルールの をクリックします。設定完了後、「保存」をクリックしてルールを保存します。 ルールを削除する場合は、対象ルールの をクリックします。 設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。



アクセスポイント - RF 最適化

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

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

<nuclias< th=""><th>Default</th><th></th><th>10:39:48 2023-03-08</th><th>Q</th><th>火 JP s</th></nuclias<>	Default		10:39:48 2023-03-08	Q	火 JP s
$(\mathbf{k}) \neq \forall \mathbf{x} \neq \mathbf{k} = \mathbf{k}$					
₩ +=9 >	CP プロファイル	ブロファイル > Silte2 > Network2 > アクセスポイント > RF最適化			
 Target 	Site2	RF hlight			
000 P 40 M 2	Ø Network2	2007/07/07			
◎ フロア計画	アクセスボイント	104-52-06-091 0 マンパート 0 マンパート 101 101 101 101 101 101 101 10			
🗙 ittie 🔹 👻	SSID	自動チャネル調整			
• プロファイルを作成	VLAN 带城幅最適化				
 プロファイル設定 	RF标道化				
 ファームウェアの更新 SSL証明書 決済代行システム 	スケジュール デバイス設定 バフォーマンス				WH.
	WLAN $r^2 \rightarrow \overline{r} \prec r > \pi > r$	< c			
₩ ¤% →	×1++				
10 VX74 >					

図 8-18 プロファイル設定 - アクセスポイント - RF 設定

以下の設定項目が表示されます。

項目	説明
調整周期	ドロップダウンメニューをクリックして、RF 周波数を調整する周期を 1 時間単位で設定します。
自動チャネル調整	チェックボックスにチェックを入れて、RF 干渉を回避するためにクライアントのチャ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。チェックボックスにチェックを入れて、干渉が存在する場合にカバ
	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.76)」を参照してください。

「RF 最適化」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」を ご確認ください。

アクセスポイント - スケジュール

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

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

<pre><nuclias connect<="" pre=""></nuclias></pre>	Default			10:39:54 2023-03-08	&	×	JP -
$\bigoplus \mathscr{I} = \mathcal{I} = \mathbb{P}$	10 -1-7-7 14	Tra Tra (d. s. Sites - Mature					
±=β ≥=β	Sites	2 0 2 7 H /F 2 Sile2 2 Network	A // X A OF A Y A Y A Y A Y A				
A 1400	Site2	ワイヤレススケジュー	1000 P				
~	③ Network2	R.					
Ø 7□7計刷	アクセスポイント	スケジュールルールを	鱼加				
🗙 ike 🔹 👻	SSID VLAN	名前					
 プロファイルを作成 プロファイル設定 	带域転最適化 RF最適化	インデックス					
• ファームウェアの史新	スケジュール	SSID	dlinknctest				
 SSL証明書 決済代行システム 	デバイス設定 パフォーマンス	曜日	 1期間中 〒を選択 				
「」 レポート ・	WLANパーティション ワイヤレスリソース	4	日曜日 月曜日 大曜日 木曜日 本曜日 金曜日 土曜日				
国 ログ →	スイッチ	時間	 1日中 時間を選択 				
50 2X74		開始時間	10:40 AM				
		終了時間	10:41 AM				
			i(1,前) クリア				
		ステータス … 名前 🔺	◇ SSIDインデックス ◇ □	× 81272-2 × 71+	レスニア アクショ	r×	

図 8-19 プロファイル設定 - アクセスポイント - スケジュール

以下の設定項目が表示されます。

項目	説明
ワイヤレススケジュール	ドロップダウンメニューをクリックして、ワイヤレススケジュール機能を有効または無効にします。
	スケジュールルールを追加
名前	スケジュールルールの名前を入力します。
インデックス	ドロップダウンメニューをクリックして、スケジュール設定が適用される SSID を選択します。
SSID	SSID名が表示されます。
曜日	ラジオボタンをクリックして、スケジュールで無線をアクティブとする曜日を設定します。
	・「1週間中」:1週間の全ての曜日でルールを有効にします。
	 ・「曜日を選択」:ルールを有効にする曜日を指定します。
時間	ラジオボタンをクリックして、スケジュールで無線をアクティブとする時間を選択します。
	・「1日中」:終日ルールを有効にします。
	 「時間を選択」:ルールの開始時刻と終了時刻を指定します。
開始時間	開始時間を設定します。この機能は、「時間」が「時間を選択」の場合にのみ使用できます。
終了時間	終了時間を設定します。この機能は、「時間」が「時間を選択」の場合にのみ使用できます。
夜間	チェックボックスをオンにすると、夜間のアクティビティが有効になります。
	「12:00 AM」をまたぐ場合は、本オプションにチェックを入れる必要があります。

■ 新規ルールの追加

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

■ 既存ルールの変更

ルールを変更する場合は、対象ルールの をクリックします。設定完了後、「保存」をクリックしてルールを保存します。 ルールを削除する場合は、対象ルールの をクリックします。 定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

アクセスポイント - デバイス設定

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

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th>10:40:00 2023-03-08</th><th>\$ 2</th><th>×</th><th>JP ∽</th></nuclias<>	Default				10:40:00 2023-03-08	\$ 2	×	JP ∽
$\bigoplus_{i \in \mathcal{V}} \mathscr{I} : \forall \forall i \neq j \neq i \neq j \neq j$								
€=\$ >	Q4 7 0 7 7 4 74		70774 ~> Site2 > Network	2 > アクセスポイント > アハイス設定				
	Sites		管理者					
666 F#FF9	Network2		PERCENT OF A					
○ フロブ計画	アクセスポイント		ユーデ名	admin				
A# 1942	SSID		$r^2 \ge 7 - F$	······				
 ブロファイルを作成 ブロファイル設定 ファームウェアの実新 	VLAN 帯域転録適化 RF最適化 スケビュール		コンソール設定 コンソールプロトコル	 ✓ 15%用化 ● Telaet ○ \$5\$H 				
• SSL证明]的	デバイス設定		411705	20				
• 決済代行システム	パフォーマンス		21A77E	3/1				
jii v#−F →	WLANパーティション ワイヤレスリソース	¢	LED設定 ステータス	 ● オン ○ オフ 				
₩ ¤″ →	スイッチ		ソーシャルログイン設定					
50 ××74 >			Facebookクライアント ID	Facebook クライブントID				
			Facebookシークレット ID	Facebook $\nu - 2 \nu_2 + \text{ID}$				
			Facebook認証 ドメイン	Facebook認識ドメイン				
			GoogleクライアントID	GoogleクライアントID				
			$Google \nu - \mathcal{I} \nu \neq \vdash \mathrm{ID}$	$Google \flat = \mathscr{P} \flat \varkappa \models ID$				
			Google記証 ドメイン	GoogleiZiif ドメイン				
			自動時間設定					

図 8-20 プロファイル設定 - アクセスポイント - デバイス設定

以下の設定項目が表示されます。

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

	項目	説明			
		外部シスログサーバ設定			
外部シス	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			
(キャプ	ティブポータルログ)	応しています。			
「保存」を	モ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、語 ド(p.76)」を参照して	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 てください。			
注意	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。				
注意 「ソーシャルログイン設定」は、DNC-100 管理下でキャプティブポータル認証を使用している場合のみ適用される機能です。					
アクセスポイント - パフォーマンス設定					

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

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th>10:40:07 2023-03-08</th><th>4</th><th>2</th><th>*</th><th>JP</th></nuclias<>	Default			10:40:07 2023-03-08	4	2	*	JP
(i) ダッシュポード	19 70771h	プロファイルッ Siteo 、Networko 、アクセスポイント、バフ	*-*72					
	Sites							
	Site2	2.4GHz 5GHz1 5GHz2(トライバンド) LA	N					
000 1000	③ Network2							
○ フロブ計画	アクセスポイント	ワイヤレス	オン マ					
🗙 ike 🗸 🗸	SSID	ワイヤレスモード	802.118X/n/g/bBEA:	~				
• プロファイルを作成	VLAN 带坡航晨遍化	データレート	Auto ~					
 プロファイル設定 ファームウェアの更新 	RF最適化 スケジュール	ビーㅋン問題 (40-500)	100					
 SSL証明書 決許代行システム 	デバイス設定	DTIM問題 (1-15)	1					
	WLAN M-FIVEY	ζ WMM (Wi-Fi $\neg \nu \neq \beta \neq \epsilon \tau$)						
<u>∎</u> ¤% →	ワイヤレスリソース	ACKタイムアクト (2.4GHz, 64~200)	64 µs					
50 2274 ->		≫ ∎ — FGI	新 定 >					
		$\operatorname{IGMP}\nolimits\!$	無効化 ~					
		マルチキャストレート	無动化 ~					
		マルチキャスト管域航コントロール	無効化 ~					
		最大マルチキャスト帯域軸	100 kbps					
		HT20/40384	和文Foc、別のMRRR市にも週川されます。 石勁化 ~					

図 8-21 プロファイル設定 - アクセスポイント - パフォーマンス設定(「2.4GHz」「5GHz 1」「5GHz 2(トライバンド)」タブ)

2.4GHz/5GHz 1/5GHz 2(トライバンド)

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

記明。
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。
ドロップダウンメニューをクリックして、ネットワークで使用されるワイヤレスモードを選択します。
・ 選択肢:(2.4GHz の場合)「802.11ax/n/g/b 混在」「802.11g/b 混在」「802.11n のみ」
(5GHz 1/5GHz 2 の場合)「Mixed 802.11n/a」「802.11a のみ」「802.11n のみ」「Mixed 802.11ax/ac/n/a」
ドロップダウンメニューをクリックして、無線のデータレートを選択します。
ワイヤレスモードが「802.11g/b 混在」(2.4GHz)または「802.11a のみ」(5GHz 1/5GHz 2)の場合にのみ設定できます。
ビーコン間隔の値を入力します。
• 初期値:100
DTIM 間隔の値を入力します。
• 初期値:1
ドロップダウンメニューをクリックして、Wi-Fi マルチメディア(WMM)機能を有効または無効にします。
ワイヤレスモードが「802.11g/b 混在」(2.4GHz)または「802.11a のみ」(5GHz 1/5GHz 2)の場合にのみ設定できます。
ACK タイムアウト値を入力します。
• 初期值:64
-

項目	説明
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。
	ワイヤレスモードが「802.11g/b 混在」(2.4GHz)または「Mixed 802.11n/a」「802.11a のみ」(5GHz 1/5GHz 2)の場合
	にのみ設定できます。
マルチキャスト帯域幅	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。「マルチキャスト帯域幅コントロール」が有効の場合に設定します。
域幅	 初期値:100
HT20/40 共存	ドロップダウンメニューをクリックして、HT20/40 共存機能を有効または無効にします。
	2.4GHz 帯の「チャネル幅」で「自動 20/40MHz」を選択した場合に指定可能です。
DHCPOFFER をマルチ	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
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:(「802.11g/b 混在」「802.11a のみ」の場合)「20MHz」
	(「802.11ax/n/g/b 混在」「802.11n のみ」「Mixed 802.11n/a」の場合)「20MHz」「自動 20/40MHz」
	(「Mixed 802.11ax/ac/n/a」の場合)「20MHz」「自動 20/40MHz」「自動 20/40/80/160Mhz」

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.76)」を参照してください。

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

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

LAN

<nuclias< th=""><th>Default</th><th>10:40:13 2023-03-08</th><th>R</th><th>2</th><th>*</th><th>JP</th></nuclias<>	Default	10:40:13 2023-03-08	R	2	*	JP
ダッシュポード						
	CP プロファイル	プロファイル > Sitez > Networkz > アクセスポイント > パフォーマンス				
100 E=9 >	Site1					
- 1-80V	Site2	2.4GHz 5GHz1 5GHz2 (トライバンド) LAN				
600	③ Network2					
◎ フロア計画	アクセスポイント	SIP (スパニングフラ 一) 一 複数のLANボート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。		1		
¥ 278 -	SSID			**	ンセル	
	VLAN					
• プロファイルを作成	带域幅最適化				8175	
 プロファイル設定 	RF最適化				PRIP	
• ファームウェアの更新	スケジュール					
• SSLEEU]#	デバイス設定					
• 決許代行システム	パフォーマンス					
「 レポート >	WLANパーティション					
	ワイヤレスリソース					
国 ログ >	スイッチ					

図 8-22 パフォーマンス設定(「LAN」タブ)

「LAN」タブをクリックした場合、以下の設定項目が表示されます。

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



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.76)」を参照してください。



「STP(スパニングツリー)」の設定は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて (p.141)」をご確認ください。

第8章 設定

アクセスポイント - WLAN パーティション

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

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

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



図 8-23 プロファイル設定 - アクセスポイント - WLAN パーティション(「2.4GHz」「5GHz 1」「5GHz 2(トライバンド)」タブ)

以下の設定項目が表示されます。

項目	説明			
クライアント間通信				
プライマリ SSID/ マル	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 SSID 1-7	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。

リンクインテグリティ

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

<nuclias< th=""><th>Default</th><th></th><th>10:40:24 2023-03-08</th><th>🖉 🚨 🔫 ле ч</th></nuclias<>	Default		10:40:24 2023-03-08	🖉 🚨 🔫 ле ч
(b) ダッシュポード				
	CP プロファイル	プロファイル > Site2 > Network2 > アクセスポイント > WLANパーティション		
100 €= 2 >	Sites			
+ +####	Site2	2.4GHz 5GHz1 5GHz2(トライバンド) リンクインテグリティ 有線LANから無線へのアクセス		
000	Network2			
◎ フロア計画	アクセスポイント	5294279574 推动化 •		and the second se
🗙 aze 🗸	SSID			**242
	VLAN			
 プロファイルを作成 	带域轴最適化			保存
 プロファイル設定 	RF标直化			
 ファームウェアの更新 	スケジュール			
 SSL证明書 	デバイス設定			
 決許代行システム 	パフォーマンス			
レポート >	WLAN $r^{i} - \overline{r} + \tilde{r} \Rightarrow \exists \Sigma$	¢		
B	ワイヤレスリソース			
	スイッチ			
G VAFA >				

図 8-24 WLAN パーティション(「リンクインテグリティ」タブ)

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

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



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.76)」を参照してください。



「リンクインテグリティ」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて (p.141)」をご確認ください。

有線 LAN から無線へのアクセス

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

< nuclias	Default		10:40:26 2023-03-08	💄 🗶 JP
(b) ダッシュポード				
	CP プロファイル	プロファイル > Site2 > Network2 > アクセスポイント > WLANバーティション		
₩ <= > >	Site1			
► + # = 5	Site2	2.4GHz 5GHz1 5GHz2(トライバンド) リンクインテグリティ 有線LANから無線へのアクセ	х	
lou	Network2			
2 7 17 (Ha)	アクセスポイント	有線LANから無線へのデ クセス		
👻 212 🗸	SSID			キャンセル
 フワフイルを作成 ブロフイル改定 フアームウェアの実術 SSL運用法 決決化行レステム レポート レポート ログ システム システム システム 	VLAN 高気病は設置化 RFは適化 スケジュール・ サイイス定定 パフォーク・マンス VLANメーティション ウイヤレスラリース スイッチ	<		56 E

図 8-25 WLAN パーティション(「有線 LAN から無線へのアクセス」タブ)

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

	記別
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	

「保存」をクリックして設定を保存します。



設定 第8章

アクセスポイント - ワイヤレスリソース

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

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

設定>プロファイル設定>サイト>ネットワーク>アクセスポイント>ワイヤレスリソースに移動し、「2.4GHz」「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< th=""><th>Default</th><th>10:40:33 2023-03-08</th><th>Ą</th><th></th><th>×</th><th>JP v</th></nuclias<>	Default	10:40:33 2023-03-08	Ą		×	JP v
í ダッシュポード						
	CP プロファイル	プロファイル > Site2 > Network2 > アクセスボイント > ワイヤレスリソース				
	Site1					
- F#05	Site2	2.4GHz 5GHz 1 5GHz 2 (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 隣接AP検知				
	Network2					
S 707 that	アクセスポイント	ACL RSSIしきい値 10% V				
X 822 -	SSID	ニ エージングアウト				
 プロファイルを作成 	VLAN	エージングアウト RSSI v				
• 70771NM2	带域航景遍化					
 ファームウェアの単領 	RF最適化	RSSIL 3 い術 10 % V				
• SSLEEULE	スケジュール	of All In College				
a data Principal - 1	デバイス設定	1-20-1 ounts				
- Keiku zaza	パフォーマンス	□ 接続制限				
「 レポート ・	WLAN $r^2 - \vec{\tau} \neq \pm \nu$	< 二一乎說即限 (0~64) 20				
	ワイヤレスリソース					
	スイッチ	m腰九 有効化 ×				
50 2274 >						
		ネットワーク使用本 100 % ~		_		
				**	ンセル	
					保存	
						-

図 8-26 プロファイル設定 - アクセスポイント - ワイヤレスリソース(「2.4GHz」「5GHz 1」「5GHz 2(トライバンド)」タブ)

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

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

「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.76)」を参照してください。



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

- DAP-X2850/DAP-X2810 : [11n/ax Preferred] (2.4GHz)], [11n/ac/ax Preferred (5GHz)]
- DAP-3666/DAP-2680/DAP-2610: [11n Preferred (2.4GHz)], [11n/ac Preferred (5GHz)]

エアタイムフェアネス

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

<nuclias< th=""><th>Default</th><th></th><th></th><th>10:40:39 2023-0;</th><th>3-08</th><th>😍 🔀 JP 🗸</th></nuclias<>	Default			10:40:39 2023-0;	3-08	😍 🔀 JP 🗸
(x) ダッシュポード						
	CP プロファイル	プロファイル > Slte2 > Network2 > アクセスポイント	> ワイヤレスリソース			
100 x = 2 >	Site1					
A Fates	Site2	2.4GHz 5GHz1 5GHz2(トライバンド)	エアタイムフェアネス バン	ドステアリング 隣接AP検知		
000	③ Network2	7/2010				
◎ フロア計画	アクセスポイント					キャンセル
 スロファイルを作成 ブロファイルを作成 ブロファイルなどの ブロファイルなどの SSL証明度 民済代行レステム 区済代 インステム 	SSID VLAN 単純転送通化 RFは道化 スケジュール・ ポンイス度定 パフォーマンス WLANパーティション	<				9.44
🖬 ¤ 🎢 🔹 👌	ワイヤレスリソース スイッチ					
50 VXFA ->						

図 8-27 ワイヤレスリソース(「エアタイムフェアネス」タブ)

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



補足

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.76)」を参照してください。

「エアタイムフェアネス」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて (p.141)」をご確認ください。

バンドステアリング(5GHz 優先)

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

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

<nuclias connect</nuclias 	Default	10:40:41 2023-	23-08	٩	🗙 JP 🗸
	√ ク ブロファイル	プロファイル > Site2 > Network2 > アクセスボイント > ワイヤレスリソース			
	Sites				
- F#09	Site2	2.4GHz 5GHz1 5GHz2(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 時後AP使用			
000	③ Network2				
◎ フロブ計画	アクセスポイント	- 1797G		**	ンセル
¥ 858 🗸	SSID				
	VLAN				N.H.
 プロファイルを作成 	带域航量遮化				PRIF
 プロファイル設定 	RF最適化				
 ファームウェアの更新 	スケジュール				
• SSL证明记题	デバイス設定				
• 決済代行システム	パフォーマンス				
	WLAN / - F + > B >	<			
-	ワイヤレスリソース				
■ ¤ 7 →	スイッチ				
50 VXFA >					

図 8-28 ワイヤレスリソース(「バンドステアリング」タブ)

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

注意

隣接 AP 検知

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

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

<nuclias< th=""><th>Default</th><th></th><th>10:40:43 2023-03-08</th><th>ß</th><th>٢</th><th>🗙 л</th><th>P</th></nuclias<>	Default		10:40:43 2023-03-08	ß	٢	🗙 л	P
ダッシュポード	20 min mar / a	vin was de la Class. Matemánia - Sida a al de la Class de la constante de					
100 €= 2 →	Sites	プロフティル > Sille2 > Network2 > ノクセムホイント > ワイヤレスリソース					
. FREW	Site2	2.4GHz 5GHz1 5GHz2(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	關握AP換用				
000	Ø Network2	有物化			_		
♥ フロア計画	アクセスポイント				**:	ven.	
🗙 ikie 🗸 🗸	SSID						
• プロファイルを作成	VLAN 语放幅起途化					保存	
 プロファイル設定 	RFilien						
 ファームウェアの更新 SSL証明書 決済代行システム 	スケジュール デバイス設定 パフォーマンス						
レポート ・ ・ ・	$\mathrm{WLAN}^{_{\mathcal{F}}} = \overline{\tau} \mathrel{_{\mathcal{F}}} \mathrel{_{\mathcal{F}}} \mathrel{_{\mathcal{F}}} \mathrel{_{\mathcal{F}}} \mathrel{_{\mathcal{F}}} \mathrel{_{\mathcal{F}}}$	c					
⊡ ¤″ →	ワイヤレスリソース						
, 20 27A							

図 8-29 ワイヤレスリソース(「隣接 AP 検知」タブ)

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

■ 隣接 AP の確認

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



注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.76)」を参照してください。

補足 「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて(p.141)」をご 確認ください。

スイッチ - 一般 - RADIUS サーバ

補足 スイッチ製品は未サポートです。

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

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

<nuclias connect</nuclias 	Default			10:40:55 2023-03-08	Q	٩	×	JP v
$\textcircled{(k)} \mathscr{I} = \forall = I = I$								
₩ €=9 >	Q 707742	7 D 7 7 4 N > Sile2 > Network2 > ×4 > T >	、一規2 > KADIUSサーハ					
	Sites	RADIUSサーバを追加						
000 F# P 2	Network2							
◎ フロア計画	アクセスポイント	RADIUS + −×**						
A. 342	スイッナ	RADIUS:	1812	1.65525				
A NOC	-82	ALD TO THE	1014					
 プロファイルを作成 	RADIUS #	RADIUS シークレット*	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	8-32 X 7				
 プロファイル設定 	時間プロファイル							
 ファームウェアの更新 	DGS-1210		コピー 追加 クリア					
 SSL#915 SSL#915 		RADIUSサーバの最大数は32です。、残り32						
- Autority Arta		No. RADIUS+	RADIUS ポート RADIUS シークレット	デクション				
		<						
<u> 国</u> ログ ->								
40 ××××								
			データが見つかりません	しでした				
		1-50f0 トータルアイテム:0		« < <u>1</u> /1 > » [; v <-	-ジごとの7	アイテム	i.
						1		
						6	举任	

図 8-30 プロファイル設定 - スイッチ - RADIUS サーバ

■ 新規エントリの追加

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

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

2. 「追加」をクリックします。

■ 既存エントリの変更

既存エントリの設定を変更する場合は、対象サーバのごをクリックします。設定完了後、「保存」をクリックしてサーバ設定を保存します。 エントリを削除する場合は、対象エントリの mをクリックします。 設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

■ RADIUS サーバテーブルの表示・検索

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

RADIUSサーバの最大数は32です。. 残り31								
No.	RADIUSサーバ	RADIUSポート	RADIUSシークレット		アクション			
1	10.90.90.100	1812		Ŕ	e î			

図 8-31 RADIUS サーバテーブル



スイッチ - 一般 - 時間プロファイル

補足 スイッチ製品は未サポートです。

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

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

Connect	Default							10:	41:17 2023-03-	08		×	
🏹 ダッシュポード													
-	CP 707712	プロファイル > Site2	> Network2 > スイッチ >	> 一般 > 時間ブ	ロファイル								
a ∈ = y	Site1		4 10 10										
トポロジ	Site2	914707717	10 L 10 M										
	Network2		名前*										
3 フロア計画	アクセスボイント			1-32 character	rs								
	スイッナ		19211		()	4. SH 10							
	-#2		46.14	. rotatobale	() inth	12 J2 J 1							
プロファイル語家	RADIUS ⊕ − ×<			白曜日 月曜日	1 火曜日 水曜	日本曜日 金曜日	上曜日						
77-69-7058	時間プロファイル												
SSLEWIS	DGS-1210		[用]46世9[用]	00	~	00	~						
決済代行システム			69 - 2 BUTT										
			A.S. 1 milled	00		00	Ū						
レポート >		<		= e-	油加加	クリア							
ログ >		and the second second	NULL WAR and DE NO										
			100 A 80 8 0 C 7 1 1 2 2 9 0									-	ł
>>>>							换等	(方法 名前	×	トーワード'を検;	R	a	
		No. 名前	× 11			~	围始時間	×:	终了時間	< アクション			

図 8-32 プロファイル設定 - スイッチ - 時間プロファイル

■ 新規エントリの追加

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

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

2. 「追加」をクリックします。

■ 既存エントリの変更

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

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

■ 時間プロファイルテーブルの表示・検索

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

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

時間プロフ	ファイルの最大数は8	です。、残	197							
					検索方法	名前	~) (+-	ワードを検索	R
No.	名前	~	П	~	開始時間	~	終了時間	~	アクション	
1	weekday		月曜日 火曜日 水曜日 木曜日 金曜日		08:00		17:00		ľ ô	

図 8-33 時間プロファイルテーブル



スイッチ - 基本

補足 スイッチ製品は未サポートです。

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

設定 > プロファイル設定 > サイト > ネットワーク > スイッチ > [製品名] > 基本の順に移動します。 以下では、各機能について説明します。

VLAN 設定

このセクションでは、VLAN を追加、編集、または削除できます。

nuclias	Default					10:42:09 2023-03-08	ß	٩	×	J
③ ダッシュポード										
	CP プロファイル		プロファイル > Site2 > Network2	> スイッチ > DGS-1	210 > 基本					
1 1 1 1	Site1		IT AN REP							
トポロジ	Site2		VLANADE							
2	Network2		VLAN ID*							
ヨ フロデ計画	アクセスポイント			2-1004						
(iki:	スイッチ									
	902		說明							
JUJ74/PETFAC	RADIUS⊕ − × ^c									
70771 Mal	時間プロファイル			_	_					
77-49±700£0	DGS-1210			жала – 🤊 у	7					
SSL(0)]??	基本		VLANリスト							
次別111システム	IPv4 ACL					VLAN ID #-9-Fieldsk				
レポート →	アクセスポリシー	<		テーブル内のエント	・りの最大数は256です。,残り255					
] ¤ // >>	ポート設定			VLAN ID	說明	アクション				
	SNTP				Default	12				
0 2274 >				•	Denne	E				
			VOICE VLANADE						~	
			IGMPスヌービング設定						~	

図 8-34 プロファイル設定 - スイッチ - 基本 (VLAN)

■ VLAN の追加

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

■ VLAN リストの表示・検索

VLAN リストには、VLAN の概要が表示されます。

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

■ VLAN の編集・削除

「アクション」フィールドで、 ごをクリックして VLAN を編集します。設定完了後、「保存」をクリックして設定を保存します。 VLAN を削除する場合は、対象 VLAN の mをクリックします。 設定を中断する場合は、「キャンセル」をクリックします。

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



Voice VLAN 設定

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

ice VLAN#Dif			~
Voice VLAN	○ 有効化 ● 無効化		
Voice VLAN ID *	>選択	0, 0, 0, 0, 0現在この音声VLANに属するメンバーボート	
	2-4094		
Voice VLAN COS			
oice VLAN OUI			
OUIT Fレス	30110104116153120		
~2.7	ff:ff:ff:00:00:00		
說明]	1-20文字		
	ie m 2 4 7		

図 8-35 基本(Voice VLAN 設定)

■ 音声 VLAN の設定 / 音声 VLAN OUI の追加

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

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

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

■ 音声 VLAN OUI リストの表示・検索

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

OUIプドレス 🔺	> マスク ▲	~ 説明▲ ~	アクション
00:01:e3:00:00:00	ff:ff:ff:00:00:00	Siemens	2 î
00:03:6b:00:00:00	ff:ff:ff:00:00:00	Cisco	2 1
00:09:6e:00:00:00	ff:ff:ff:00:00:00	Avaya	C Î
00:0f:e2:00:00:00	ff:ff:ff:00:00:00	Huawei & 3COM	e î
00:60:b9:00:00:00	ff:ff:ff:00:00:00	NEC & Philips	1

図 8-36 基本 (Voice VLAN 設定 - Voice VLAN OUI)

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



IGMP スヌーピング設定

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

MPスヌービング設定	
IGMPスヌーピング	○ 有効化 ● 無効化
VLAN*	
	1-4094 例: 1-4,7もしくはall

図 8-37 基本(IGMP スヌーピング設定)

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

STP 設定

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

STP設定				
	RSTP	○ 有効化	● 無効化	
図 8-38 基	本(STP 設定)			

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

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

注意	設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76
)」を参照してください。

DHCP サーバスクリーン設定

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

ICPサーバスクリーン設定	
DHCPサーバスクリーン	○ 有効化 ● 無効化
許可されたDHCPサーバ IP	
	1エントリのみサポート 例:10.90. 90.90

図 8-39 喜保院(DHCP サーバスクリーン設定)

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

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



設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

ジャンボフレームの設定

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

ジャン	ボフレーム設定			
	ジャンボフレーム	○ 有効化	● 無効化	
図 8-40	基本(ジャンボフレ			

1. ジャンボフレームを有効または無効に設定します。

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

QoS

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

DSCPをCoSキューマ	ップに編集				
	DSCP/iñ 🔺 🗸	CoSキュー信 ▲	~	名前 🔺	
	0	0		Default	1
	1	0		Default	
	2	0		Default	
	3	0		Default	
	4	0		Default	

図 8-41 基本 (QoS 設定)

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

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

注意

設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

LBD 設定

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

LBD	定				
		LBD	○ 有効化	● 無効化	
図 8-42	LBD 設定				

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

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

注意	設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります	。詳細については、	「設定のアップロー	ド (p.76
)」を参照してください。			

DDP 設定

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

DDP設定				
	DDP	● 有効化	() 無効化	
図 8-43 DDP 設定				

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

ローカル資格情報設定

お使いのデバイスのユーザ名とパスワードが表示されます。

ユーザ名	admin	
パスワード		Ś

図 8-44 ローカル資格情報設定

スイッチ - IPv4 ACL

補足 スイッチ製品は未サポートです。

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

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

connect	Default					10:45:37 2023-03-08	1	٩	×	J
ダッシュポード	29 70771A	プロファイル > Site2 > Networks	2 > スイッチ > DGS-1210 > IPv4 ACL							
±1] → モニタ →	Site1									
- Fator	Sitez	ユーザ定義されたIPv4 ACLルー	- <i>x</i>							
00	③ Network2				a					
● フロア計画	アクセスポイント	シーケンス寄号			Auto					
2 設定 🗸	スイッナ		1-05535							
	一般	ポリシー	拒否	~	ブロトコル	すべて		~		
プロファイルを作成	RADIUS+	22.00-05	- the second		Will West and					
ファームウェアの更新	時間プロファイル	12, IS 70			AGAIN / Low					
SSL証明書	DGS-1210	送信先	サペイ	~	送信先ボート					
決済代行システム	基本									
A listen in the	IPV4 ACL	《 説明*								
l sacar	ポート設定						ai a tha tha that the the the the the the the the the th	19	τ	
117 ×	SNTP	テーブル内のユーザ定義されたエントリの損大賞は768です。残り768								
 AFX4 		シーケンス番 _m ~ ポリシー	~ ブロトコル → 送信元	~ 送信	元ポー、 送信先	→ 送信先ボー→ 説明	v	アクシ	s ×	
			データ	が見つか	0 1 + + 4.701 7	5				

図 8-45 プロファイル設定 - スイッチ - IPv4 ACL

■ ルールの作成

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

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

「追加」をクリックして、ルールを追加します。 「クリア」をクリックして、すべての設定値をリセットします。

■ ルールの編集・削除

「アクション」フィールドで、 ごをクリックしてルールを編集します。設定完了後、「保存」をクリックして設定を保存します。 ルールを削除する場合は、対象ルールの mをクリックします。 設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。



設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。
スイッチ - アクセスポリシー



補足 スイッチ製品は未サポートです。

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

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

<pre>should be a connect</pre>	Default		10:45:44 2023-09-08 🖉 🔕 💘 JP -
$\textcircled{(k)} \mathcal{I} \neq \mathcal{I} = dt + 1^{2}$	1 m 2 m 22		
₩ <u></u> €=# >	Q 707742	プロファイル > Site2 > Networ	22 > スイッナ > DGS-1210 > アクセスボリシー
	Sites		
COD FRIDY	Networks	ポリシー名*	
Ø 7 □ 7 計画	アクセスポイント	U ∈ − FRADIUS*	選択
A	スイッチ		
× exe			テーブル内のエントリの最大数は3です。.残り3
• プロファイルを作成	RADIUS #		No. RADIUSサーバ RADIUSポート RADIUSシークレフ アクション
 プロファイル設定 	時間プロファイル		
 ファームウェアの更新 	DGS-1210		
 SSL計明書 油法用行いまさり 	基本		
- addition 2 ad a	IPv4 ACL	¢	データが見つかりませんでした
1 L#-F >	アクセスポリシー		
Ē ¤∥ →	ポート設定 SNTP		
50 xx74 >		アクセスボリシータイプ	802.IX#-1-X-2-F v
		$\mathcal{T} \rtimes \mathbb{P}$ VLAN	Disabled \checkmark
		スイッチボート	0, 0, 0, 0 このボリシーを現在使用しているボート
			保存 リモット

図 8-46 プロファイル設定 - スイッチ - アクセスポリシー

■ アクセスポリシーの作成

次の項目が表示されます。

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

「保存」をクリックして、アクセスポリシー設定を保存します。

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



設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

スイッチ - ポート設定

補足 スイッチ製品は未サポートです。

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

nuclias	Default								10:45:52 2	023-03-08	8	×																						
) ダッシュポード	19 707736			Sitan > Naturalm > 7	d with a DCS int	as de seer																												
€= <i>\$</i> →	Sites			sites > metworks > ~	4 7 7 5 DG3-121	0 3 % ~ P 80E																												
- hates	Site2		10 Ports	20 Ports 26 Ports	28 Ports	52 Ports																												
	Network2						検索方法 VLAN	v #-191	ブ 全てのタイプ 、	+-7-	ドを検索	R																						
フロア計画	アクセスポイント											Ø																						
設定 ~	スイッチ		- determined	v 1.v.h v	ポートルイプン	VIAN	* TO S D & VI ANY	debzer v	DaF	PSTP	× IBD																							
プロファイルを作成	-#2				10 1 2 1 2 m	T La La Y	al of Carrie Cartan		102		200																							
プロファイル設定	RADIUS+		1	Default	アクセス	1	-	有効化	有効化	有効化	無効化																							
ファームウェブの更新	DGS-1910		2	Default	アクセス	1		有効化	有効化	有効化	無効化																							
SSL証明書	基本																								3	Default	アクセス	1		有効化	有効化	有効化	無効化	
決済代行システム	IPv4 ACL	<	4	Default	アクセス	1		有効化	有効化	有効化	無効化																							
⊳dr−} →	アクセスポリシー		5	Default	アクセス	1	21	有効化	有効化	有効化	無効化																							
р <i>7</i>)	ポート設定		6	Default	アクセス	1		有効化	有効化	有効化	無効化																							
	SNTP		7	Default	アクセス	1	-	有効化	有効化	有効化	無効化																							
システム >			8	Default	アクセス	1		有効化	有効化	有効化	無効化																							
			9	Default	アクセス	1	1	有効化	有効化	有効化	無効化																							
			10	Default	アクセス			水油化	有効化	水油化	無効化																							

図 8-47 プロファイル設定 - スイッチ - ポート設定

■ 対象範囲の指定 / ポートの検索

- ・ 以下のフィルタリング項目を指定し、関連するキーワードを入力して 🔯 をクリックして検索を開始します。
 - 「検索方法」:「VLAN」「Port」「Access Policy」
 - (VLAN を指定した場合)「ポートタイプ」:「全てのタイプ」「アクセス」「トランク」
- テーブルには以下の項目が表示されます。
- ・「ポート(番号)」「リンク」「ポートタイプ」「VLAN」「許可された VLAN」「ポートステート」「PoE」「RSTP」「LBD」「DDP」「ポートシャットダウンスケジュール」「PoE 供給スケジュール」「アクセスポリシー」

■ ポート設定の変更

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

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



設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

スイッチ - SNTP 設定

補足 スイッチ製品は未サポートです。

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>10:4</th><th>5:57 2023-03-08</th><th>ß</th><th>٩</th><th>×</th><th>JP</th></nuclias<>	Default								10:4	5:57 2023-03-08	ß	٩	×	JP
(b) X v V a dt - F														
(回) モニタ >>	CP 707744	プロファイル > Site2 >	Network2 > スイッチ:	> DGS-1210 >	SNTP									
-76	Site1	自動時間設定												
トポロジ 000	Sites			SNTP	サーバを有久	0 fL								
	© Network2													
	アクセスポイント		SNTP+	IPアドレ		名								
🗙 182	スイッチ			The Mar										
and the first state			SNIP#-//2	IPTFU										
· Jujjian () Brit	RADIUS +	タイムゾーン設定												
 フロノテイル改正 	時間プロファイル		タイムゾーン	(GMT+o	9:00) Osaka	Sapporo, To	kyo							
 ファームウェアの更新 	DGS-1210													
 SSL証明書 	基本			- +	タイムを有	幼化								
 決済代行システム 	IPv4 ACL	K	DST開始 (24時間)					at						
	アクセスポリシー													
-	ポート設定		DST终了 (24時間)					at						
1 D / >	SNTP													
システム >			DSTオフセット	60				~						
													687	

図 8-48 プロファイル設定 - スイッチ - SNTP 設定

次の項目が表示されます。

項目	説明						
	自動時間設定						
SNTP サーバを有効化	チェックボックスをクリックして、SNTP サーバを有効または無効にします。						
SNTP サーバ 1	システム時刻を取得するプライマリ SNTP サーバの IPv4 アドレスまたはドメイン名を指定します。						
SNTP サーバ 2	セカンダリ SNTP サーバの IPv4 アドレスまたはドメイン名を指定します。						
	タイムゾーン						
タイムゾーン	ローカルタイムゾーンを選択します。						
サマータイムを有効化	チェックボックスをクリックして、サマータイムを有効または無効にします。						
DST 開始(24 時間)	DST(サマータイム)を開始する月、日、時刻を指定します。						
DST 終了(24 時間)	DST(サマータイム)が終了する月、日、時刻を指定します。						
DST オフセット	ローカル DST オフセットとして構成する時間を指定します。						
	・ 選択肢:「30」「60」「90」「120」(分)						
	・ 初期値:「60」(分)						

「保存」をクリックして、設定を保存します。



設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード(p.76)」を参照してください。

ファームウェアの更新

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

設定>ファームウェアの更新>サイト>ネットワークの順に移動します。

<nuclias connect</nuclias 	Default	1	0:46:59 2023-03-08	4	2 ×	JP
$(f) \text{if } y \neq y = y - y$	10 ファールウェアの明新	ファールウェアの単純 Siter SNetworks				
101 ▲Φ <= β →	Sites					
A 1802	S Networki	オンラインチェックアップデートファームウェア ファームウェアの手動更新				
ooo フロ7計画	Site2	ダモデルのフィートウィアフィイルをアップロード		7472-		
★ 設定 ~		(二、オジル茶号/ハードウェアパージョン 現在のファームウェアパージョン(…~ 新しいファームウェア −	<i>9 9</i> − × H × 7 7		714	
 プロファイル設定 						
 ファームウェアの更新 SSL証明書 決済代行システム 						
- ۲ ۲ III		モデルを見つけることができません。				
I □ Ø						
LO 22754)						
		illefeidill Illefe >				
				逾用	クリア	
		実行ステータス				

図 8-49 ファームウェアの更新

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

■ ファームウェアの手動更新

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



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 (o/o
結果	実行時間 → 、 名前
	利用可能な結果はまだありません。

図 8-50 ファームウェアアップグレード - 実行ステータス

SSL 証明書

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

設定 > SSL 証明書 > サイト > ネットワーク に移動します。

<pre>succession connect</pre>	Default			10:47:16 2023-03-08	\$	×	JP v
(K) ダッシュポード							
₩ <= y >	CP SSL証明書	SSL証明書 > Site1 > Network1					_
	Site:	SSL証明書を更新(アクセスポイントのみ					
666 F#P2	Sitez						
😂 フロア計画		ファイルから証明書をアップロード	799¥				
🗙 ike 🗸							
		ファイルからキーをアップロード	ブラウザ				
 プロファイルを作成 プロファイル設定 							
 ファームウェアの更新 					アップロ	— F (
 SSL証明書 		defende and					
• 決済代行システム		Lirx7=9.4					
lin ⊨ k →		····································					
₩ ¤% →		結果実行質	·問 ▼ → 名前 → IPアドレス	✓ MACアドレス ✓ モデル番号。	.~ 結果 ~		
50 VXFL >							
				2			
			warmen was a later of a	3.8.3 i. 3 i. x			
							_

図 8-51 SSL 証明書

「SSL 証明書を更新」セクションでは、以下の設定項目が表示されます。

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

「アップロード」をクリックして、ファイルのアップロードを開始します。

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

決済代行システム ※本項目は日本ではサポート対象外となります。

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

設定>決済代行システムに移動します。

<nuclias< th=""><th>Default</th><th>10:47:21 2023-03-08</th><th>1</th><th>2</th><th>×</th><th>JP v</th></nuclias<>	Default	10:47:21 2023-03-08	1	2	×	JP v
() XVV=N-F						
100 €= Ø →	又抵款定					
tany	Paypalizifit* USD ~					
◎ フロア計画	Paypal クライブントID*					
🗙 ere 🗸 🗸	Pareal $\nu = 2 \mid \nu \neq 1$					
 プロファイルを作成 						
• プロファイル設定	オブション [★] 期間 ○ 分 ✓ 費用 ○ -					
• ファームウェアの更新						
 SSL証明書 	月間 −つ選択 ∨ 費用 +					
 決済代行システム 						
				6	HF .	
■ □ 7 >						
50 vata >						
						-

図 8-52 決済代行システム

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

「保存」をクリックして設定を保存します。

第9章 レポート

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

アクセスポイントのレポート

ピークネットワークアクティビティ

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





図 9-1 アクセスポイント - ピークネットワークアクティビティ

■ 対象範囲の指定

■ レポート項目

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

時間別ネットワークアクティビティ

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

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



図 9-2 アクセスポイント - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

ドロップダウンメニューからサイトとネットワークを選択し、日付を選択後、 🗟 をクリックしてレポートを表示します。レポートが生成されたら、 🗈 をクリックしてレポートをローカル PDF ファイルに保存します。

■ レポート項目

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

日別ネットワークアクティビティ

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

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



図 9-3 アクセスポイント - 日別ネットワークアクティビティ

■ 対象範囲の指定

■ レポート項目

以下のレポートが表示されます。

• 毎日のトラフィック使用量と接続クライアント数

最もアクティブな AP

特定のアクセスポイントのトラフィック使用量を表示します。

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



図 9-4 アクセスポイント - 最もアクティブな AP

■ 対象範囲の指定

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

■ レポート項目

以下のデータが画面右上に表示されます。

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

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

■ マップの作成

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

■ マップの編集・削除

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

注意 v1.2.0.9b1をご利用の場合、既知の問題により日本語表示では左側のメニューに「最もアクティブな AP」メニューが表示されません。本レポートを表示、設定するには英語表示に切り替えてください。

スイッチのレポート

時間別ネットワークアクティビティ

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

<u> </u>	
Care man	
700 52	

補足 スイッチ製品は未サポートです。

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

nuclias connect	Default	15:34:08 2022-12-02 🤌 🔇 💉
シン ダッシュボード	ワイセレスカットワークになける新聞別統計	金ヶ町サイト
47 300 € = ∮ →		
	時間労働後がクライテント強と過去プロ国の先期	
● フロア計画	按照 2 2 4 7 2 1 放	■ 2022/12/02 ■ 平均 ■ 高
🖌 設定 >		
・ アクセスポイント	1000 0100 03:00 04:00 04:00 05:00 06:00 07:00 08:00 05:00 10:00 12:00 12:00	200 1500 1600 1500 1600 1700 1800 1900 200 2100 2200 0500
ピークネットワークアク ディビディ		
時間別ネットワークアク ディビディ	時間別トラフイックの洗用量と過去7日間の実験	
日別ネットワークアクテ イビティ		
最もアクティブなAP	+ 2.7 x × 2(沈用量(MB) 1 y	2022/12/02 📕 平均 📕 務
×424 >		
1 × >		
0 2774 V		
	10:00 01:00 05:00 05:00 05:00 05:00 01:00 05:00 10:00 11:00 10	200 13:00 14:00 5:00 16:00 17:00 18:00 19:00 at:00 at:00 a3:00

図 9-5 スイッチ - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

ドロップダウンメニューからサイトとネットワークを選択し、日付を選択後、
園をクリックしてレポートを表示します。レポートが生成されたら、 ■をクリックしてレポートをローカル PDF ファイルに保存します。

■ レポート項目

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

日別ネットワークアクティビティ

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

補足 スイッチ製品は未サポートです。





図 9-6 スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

■ レポート項目

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

トップランキング

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

補足 スイッチ製品は未サポートです。

<nuclias< th=""><th>Default</th><th></th><th></th><th>10</th><th>6:21:59 2022-12-0</th><th>2</th><th></th><th>×</th><th>3</th></nuclias<>	Default			10	6:21:59 2022-12-0	2		×	3
(b) グッシュボード									
₩ += / >	スイッチのトップランキング統計	全てのサイト 🗸	全てのネットワーク 〜	2022.11.22	2022.12.01	龖	R		
-20	トップ絶トラフィック (Tx)		トップ総トラフィ	i > ⊅ (Rx)					
550 F#P2		💼 総トラフィック (Tx)				一般日	77197	(Rx)	
◎ フロア計画									
🗙 設定 >									
📓 (z=1) 🔹 👻									
 アクセスポイント > 									
• スイッナ									
時間別ネットワークアク ティビディ 日別ネットワークアクテ									
イビティ トップランキング	トップポートトラフィック (Tx)		トップポートトラ	デフィック (Rx)					
e مراجع		💼 総ポートトラフィック(Tx)				総ポートト	ラフィック	(Rx)	
- yz74)									
20									

図 9-7 スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

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

第10章 ログ

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

デバイスシスログ

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

ログ > デバイスシスログに移動して、ログ情報を表示します。

<nuclias< th=""><th>Default 16:51:14 2022-19-19 🦉 🔕 🤻</th><th>JP v</th></nuclias<>	Default 16:51:14 2022-19-19 🦉 🔕 🤻	JP v
$\textcircled{(k)} \mathcal{T} := \mathcal{T} = \mathcal{V}$		
$\begin{bmatrix} \underline{W} \\ \underline{A} \\ \underline{A} \end{bmatrix} \in = \mathcal{I} $ \rightarrow	₹(0 7 [×] (33) T~(0€<374 ∨ T~(0775)7+ 2022.12.12 ■ 2022.12.19 ■ F (F)F(X ∨ 4-0)-F(6) = R	
tere s	サイイスシスログ キャプライブゼーラルログ	
○ 7 □ 7 計画	受信時間 ∨ ログ時間 × V デバイスタイプ × 名前 ∨ 臣アドレス ∨ ファシリティ ∨ セベリティ ∨ ディレクティブサーバ ∨ メッセージ	
~	2022-12-19-16(4803 2022-12-1511(35550 72+2.44/2) dag666 kernelmessage Notice Dec 1511(3550 Dft FL.	
× 82 ,	2022-12-19 154(Rog 2022-12-15 11:55:50 プクキスギイン) dap3666 kernel messages Notice Dec 15 11:55:50 Dft FL.	
📓 v#-1 🔹 >	2023-13-19 154443 2023-13-15 115230 7.7 4.3 47.4 2 dap3666 kernel messages Information De: 15 115230 Eth	
🖬 o 17 🔹 👻	2022-12-19 1634441 2022-12-19 1152128 7.7 4.7 #4 >) dap2666 kernal messages Notice Dec 19 1152128 1 4.941	
* #44343##	2022-12-19 1614414 2022-12-19 1132228 79 4 3 4 4 1 2 1 dap3666 kernel messages Infirmation Dec 19 1132228 1 4 4 1	
 システムイベントログ 	2022-12-19 1654440 2022-12-19 1152228 7.7 4.7 4.7 >) dap3666 krral mesages Information Dec 19 115228 1 (NPA	
* 7×1×07	2022-12-19 16144137 2022-12-15 1152124 7.9 * X #4 × > 1 dap3666 kernel messages Information Dec 15 1152124 Assoc.	
 	2022-12-19 1634437 2022-12-19 1152224 7.9 €.X.#4. >) dap3666 krral mesages Infirmation Dec 19 1152224 4.4.4.4.	
• 77-1	2022-12-19 16344137 2022-12-15 1152124 7.7 #.7.#4.>) dap3666 kernel messages Information Dec 15 1152124 1 INFA	
Q0 2274 →	2022-12-19 (63:44:37 2022-13-15 11:52:24 7.9 ± 3.4"4 >) dag3666 karnal mesagar Notice Dec 15 11:52:24 957Hz.	
	2022-12-9 16344337 2022-12-9 1535224 7.7 4.7 #4 > 1 dag666 kernal mesager Notice De 15 1152124 1 95Hz.	
	2022-12-19 163-4437 2022-12-15 1152124 7.9 + 3. + 4. + > 1 dapg666 kernel memagere Information. Dec 15 1152124 1 = 14.+ ma.	
	2022-12-19 16344:37 2022-12-19 1152124 7.9 4.7 4.4 >) dag3666 kreal mesages Information Det 15 1152124 (1994)	
	2022-12-19 16344137 2022-12-15 1152124 7.9 #3.#4.+>) dap3666 kernel messages Information. Dec 15 1152124 Assoc.	
	202212-1916:44:37 2022-12-1511:52:24 7.9 ≪ 7.4 ×) dap3666 kmml messages Notice Dec 15 11:52:24 50Ht	
	2022-12-19 16/42:49 2022-12-15 11:50:26 7 / * * * * / 2 / dap3666 kernel messages Information Dec 15 11:50:26 / Assoc.	
	1-901(39) 1-7+7474339	7.6

図 10-8 デバイスシスログ

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

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

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

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

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

システムイベントログ

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

ログ > システムイベントログに移動します。

<nuclias< th=""><th>Default</th><th></th><th></th><th></th><th></th><th></th><th>16:51:18 2022-12-19 🦉 🚨 💌 JP 🗸</th></nuclias<>	Default						16:51:18 2022-12-19 🦉 🚨 💌 JP 🗸
$(f) \mathcal{I}' \succ \succ = \mathcal{K} = V$			(Areature			m) (
$\begin{array}{c} [\underline{\mathrm{Mil}} \\ \underline{\mathrm{A}} \\ \underline{\mathrm{A}} \\ \underline{\mathrm{A}} \end{array} \hspace{0.1 in} \in = \mathcal{I} \hspace{1.1 in} \rightarrow \hspace{1.1 in}$			金くロケハ4	X30 T~004~21340	2022.12.12	2022.12.19	
	□ 21時間 ▼	オペントタイプ	< デバイスタイプ <	\$ \$ \$ \$ \$ \$ \$ \$ \$ \$	10 プドレス ∨	MACアドレス	* 194-5
○ 7 □ 7計画	2022-12-19 14:10:33	デバイス管理	アクセスポイント	Networks	10000	and a description of the local distance of t	Force change the device status to offline due to the keep-alive messa
¥2 107 .	2022-12-15 16:38:27	デバイス管理	アクセスポイント	Networka	presidential	sectorie d'als	Force change the device status to offline due to the keep-alive messa
	2022-12-15 16:07:27	デバイス管理	アクセスポイント	Networks	10000		Force change the device status to offline due to the keep-alive messa
<u></u>	2022-12-15 10:04:27	アハイス管理	7/2/8/2/	Networks	and the second sec	and the second sec	Force change the device status to omine due to the lossp-alive messa
■ • 7 ×	2022-12-15 10:01:27		77*384>1	Networks			Force change the device status to offline due to the keen alive messa
* 7×125207	2022-12-15 15:55:27	デバイス管理	アクセスポイント	Networka	standard to	and sold strates	Force change the device status to offline due to the keep-alive messa
• 5372440107 • 7//307	2022-12-15 10:09:07	款定		Networks			Force change the configuration due to the configuration is incompat
 監査ログ 	2022-12-15 10:04:04	欲定		Networka			Force change the configuration due to the configuration is incompat
• 77-1							
- 4 [₹] × 0							
	1-50 of 9 トータルアイテム: 5						 < 1 /1 >> > 50 → ページごとのアイテム

図 10-9 システムイベントログ

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

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

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

デバイスログ

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

ログ > デバイスログに移動して、レポートを表示します。

<nuclias< th=""><th>8</th><th>Default</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>16:51:20 2022-12-19 🦉 🚨 🛪 JP</th></nuclias<>	8	Default								16:51:20 2022-12-19 🦉 🚨 🛪 JP
ダッシュポード					ACD7/1220	オペイの動作さ	ਸਤ ਹੈ	ongo.10.10 📾	0000.10.10	m P7FVX v +-7-P682 D D
107 e=9	>							lans	,	
E FRAS		□ ∅明間 ▼	× デバイスタイプ	~ 名前	~ IP 7	ř v z	 MAC7 FPX 	~ 操作推到	~ 給照	~ ログ詳細
2 7 7 7 11 25		2022-12-19 16:48:51	アクセスポイント	dap268o		10. C	10000	テォネルもしくはIPア	F	Channel. 2.4GHz: 11, Channel. 5GHz 1: 48.
9 · · · · · ·		2022-12-19 16:48:13	アクセスボイント	dap3666	-	- 11	10.100	チャネルもしくはIPア	F	Channel. 2.4GHit: 3, Channel. 9GHit 1: 116.
K RE	>	2022-12-19 16:48:13	アクセスボイント	dap3666		1.1	10.00	チャネルもしくはIPア	۶	Channel. 2.4GHz: 3, Channel. 9GHz 1: 116.
副 レポート	>	2022-12-19 16:45:31	アクセスボイント	dap3666			10.00	クライブントのブロッ	. Success	Client MAC: , Primary
a		2022-12-19 16:45:28	アクセスポイント	dap268o	10	1. C	1000000	クライブントのブロッ	. Success	Client MAC: , Frimary
デバイスシスロ3	7	2022-12-19 16:44:36	アクセスポイント	dap3666		10.00	10.000	クライブントをブロッ	2 Success	Client MAC:
· >>=	100	2022-12-19 16:44:34	アクセスポイント	dap268o				クライアントをブロッ	2 Success	Client MAC: , Primary
+ + < 1 × 0 / /		2022-12-19 16:44:21	アクセスボイント	dap2680	10	10. C		チャネルもしくはIPブ	F	Channel. 2.4GHz: 11, Channel. 5GHz 1: 64.
 ・ ・		2022-12-19 16:44:12	アクセスボイント	dap268o		- Transford	-	テォネルもしくはIPア	۴	Channel. 2.4GHz: 11, Channel. 5GHz 1: 36.
• 77-1		2022-12-19 16:43:21	アクセスボイント	dap2680	10	10		チャネルもしくはIPプ	F	Channel. 2.4GHz: 11, Channel. 5GHz 1: 64.
20 VX74	>	2022-12-19 16:43:11	アクセスポイント	dap268o		10.00		テォネルもしくはIPア	۴	Channel. 2.4GHz: 11, Channel. 5GHz 1: 36.
		2022-12-19 16:43:08	アクセスボイント	dap3666		10. IT	100.000	設定をアップロード	Success	Upload Configuration
		2022-12-19 16:43:02	アクセスポイント	dap268o		10.00	10000	チャネルもしくはIPア	ŕ	Channel. 2.4GHz: 1, Channel. 5GHz 1: 36.
		2022-12-19 16:42:58	アクセスポイント	dap268o		10.0		設定をアップロード	Success	Upload Configuration
		2022-12-19 16:42:43	アクセスボイント	dap3666		10.01	10.00	設定をアップロード	Success	Upload Configuration
		2022-12-19 16:42:33	アクセスポイント	dap268o		10.00		設定をアップロード	Success	Upload Configuration
		2022-12-19 16:42:01	アクセスボイント	dap3666		1.1	10.000	デバイス設定を同期す	é Success	Channel. 2.4GHz: 3, 5GHz 1: 108, Synchronize Configu
		1-50 of 183 1-9×749	4:183							< 1 /4 > » 50 ッ ページごとのアイテム

図 10-10 デバイスログ

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

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

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

監査ログ

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

ログ>監査ログに移動して、レポートを表示します。

	Default 16:49:32 2022-12-02 & 🖉 🔳 💘 🦉
() #79=#-F	
₩ += 9 >	全ての資件タイプ v オペマのオブジェクトエマ 2022.11.25 節 2022.12.2 節 ユーザ名 v ホーワードを決定 🔃 🕑
. Land	ログ時間 マーマー 操作権別 マーユーザ名 マーオブジェクトエン スノッセージ
666 14192	2022-12-02-15-46:05 i歳加 admin 最もアクティブな Mnet active AP report 2Fマップ has been added.
♥ 7 □ 7計画	2022-12-02 15:33:57 ログイン admin ログイン Login on 127,0.0.1.
× 87E >	2022-12-02-12:54/56 ログブクト admin ログブクト Logutton 127.0.0.1.
-x-+ →	2022-12-02 12:07:50 編集 admin プロファイル設定 The SNTP configuration of switch series DGS-12:10 in network Network: has been changed.
🗐 o7 🗸	2022-12-02 11:46:26 P I 4 V admin P I 4 V Login on 127,0.0.1.
· #KAZUZO#	2022-12-02 11:43:00 ログブクト admin ログブクト Logout on 127,0.0.1.
 システムイベントログ 	2022-12-02 10:47:01 編集 admin プロファイルを作成 Device type Switch with series DGS-1210 has been supported in Network. Network.
• 7×1×07	2022-12-02 10:47:01 篇集 admin プロファイルを作成 The username / password of device type Switch has been changed in Network Network 1.
 ・	2022-12-02 10146140 P 274 2 admin P 274 2 Login on 127,0.0.1.
• 79-1	2022-12-02 10:09:00 ログブクト admin ログブクト Logout on 127:0:0.1.
50 2754 >	2022-12-02 09:52141 P I A > admin P I A > Login on 127.0.0.1.
	2022-11-25 17:30:25 編集 admin プロファイル設定 Upload Configuration of network Network: Network: has been applied immediately.
	2022-11-25 16:05:35 編集 admin プロファイル設定 Upload Configuration of network Network: Network: has been applied immediately.
	2022-11-25 16103356 編集 admin プロファイル設定 VLAN in network Network 1 has been changed.
	2022-11-25 16:02:40 編集 admin プロファイル設定 Upload Configuration of network Network: Network: has been applied immediately.
	2022-11-25 16:02:30 編集 admin プロファイル設定 VLAN in network Network1 has been changed.
	1-500f36 +-ダルブイラム:36 (() 1)/1 シッ 50 v パージニとのブイラム

図 10-11 監査ログ

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

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

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

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

アラート

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

ログ>アラートに移動して、レポートを表示します。

< nuclias	Default					16:51:24 2022-12-19	😍 💘 jp 🗸
(i) #772#-1							
100 e=9 >			オペマのアラート	4421 × 2025	2022.12	19 曲 IPアドレス v ホーワードを検索	R
* 1.0000	ログ時間 マニー・キット	2-2 ~ 名前 ~	IPアドレス v	MAC7 Fレス	2.2.2.1 ≤ ≤ ≥ 1 ≤ ≤ ≥ 1	$\lambda = -\omega$	プクション
666 F 414 2	2022-12-19 15:22:17 Networ	rkı dap3666	10.00	10000	デバイスオフライン	Device is disconnected.	Û
○ 7 □ 7 計画	2022-12-19 15:09:55 Networ	rkı dap3666	10.00	10000000000	デベイスオフライン	Device is disconnected.	8
🗙 RE 🔹 >	2022-12-19 15:08:55 Networ	kı dap3666	10.00	10000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because t	t
📓 v#-1 🔹 >	2022-12-19 15:08:51 Networ	rkı dapz680	10.000	10000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because $\boldsymbol{t}_{\cdot\cdot}$	0
🗐 o 17 🗸 🗸	2022-12-19 15:04:39 Networ	kı dap3666	1000	10000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because $\ensuremath{t}\xspace$.	Û
	2022-12-19 15:04:36 Networ	rkı dapz680	10.000	10000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because $t_{\rm s}$	0
 vx744~v+p5 	2022-12-19 14:52:24 Networ	rkı dap3666	1000	10000	デベイスオフライン	Device is disconnected.	Û
• #×4207	2022-12-19 14:22:23 Networ	rkı dap2680	100.000	100000000	デバイスオフライン	Device is disconnected.	t
 ・ ・ ・	2022-12-19 14:10:33 Networ	rkı dap2680	100.000	10000	デベイスオフライン	Device is disconnected.	8
• 77-1	2022-12-19 14:09:03 Networ	kı dap3666	100.000	1000	デバイスオフライン	Device is disconnected.	t
G SAFA >	2022-12-19 12:17:45 Networ	rkı dap3666	10.00	10000	プロファイルは適用されませ…	Success: Failed to create SSIDs for some of your APs because t	8
	2022-12-19 11:30:53 Networ	kı dap3666			デバイスオフライン	Device is disconnected.	Ū
	2022-12-19 10:55:41 Networ	rkı dap2680	100.000	10000	デバイスオフライン	Device is disconnected.	0
	2022-12-15 18:49:21 Networ	rkı dap3666	and the second second	Sector and the	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because $\ensuremath{t}\xspace.$	ŧ
	2022-12-15 18:49:18 Networ	kı dap2680			プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because t	0
	2022-12-15 18:27:34 Networ	rkı dap3666	100 million (1990)	1000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because t	8
	2022-12-15 18:27:31 Networ	kı dap2680	100.000	10000	プロファイルは適用されませ	Success: Failed to create SSIDs for some of your APs because t	t
	1-50 0f 29 トータルアイテム:29					« (1 /1 > » 50 v	ページごとのアイテム

図 10-12 アラート

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

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

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

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

第11章 システム管理

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

デバイス管理

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

システム > デバイス管理に移動します。

∢ nuclias connect	Default 10:56:15 2023-03-08 🖉 🚨 💘 JP 🗸
()) ダッシュポード	
₩ •=>	(ジネットフーク) 11/21 年3月22 Sites
- F###	デバイスタイプ 全てのタイプ ◇ 脱添方法 ローカルIPアドレス キーワードを脱添 (2) Site2
	© Network2
₩ フロア計画	□ ステータ…× ローカルIPアドレ…× MACアドレス × モデル番号 × ハードウェア…× ファームウェ…× 管理された時間 ×
🗙 設定 >	172.16.1.46 arealedania da DAP-2680 2A1G v2.00B08 2023-03-08 10:26:00
「「レポート >	
🖬 ¤ // >	
50 ××74 ×	< c
 デバイス管理 	
 ユーザ管理 	
 設定 	
Nuclias Connectについて	

図 11-1 デバイス管理 - 管理タブ

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

■ 管理デバイスリスト / 非管理デバイスリストへの移動と削除

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

■ ネットワークの移動

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

■ 表示項目

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

表示項目を変更するには、 📰 をクリックします。

- ・ステータス
- ・ ローカル IP アドレス
- ・ MAC アドレス
- モデル番号

- ・ ハードウェアバージョン
- ・ ファームウェアバージョン
- ・ バックアップファームウェアバージョン
- 管理された時間 / 非管理になった時間

補足 管理配下のアクセスポイントに関して、以下の仕様があります。

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

ユーザ管理

ユーザステータス

ユーザステータス画面では、登録されているユーザプロフ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 / 削除したりすることができます。

システム > ユーザ管理に移動して、ユーザステータス情報を表示します。

<pre><nuclias connect<="" pre=""></nuclias></pre>	Default 12:54:55 2023-03-08
() ダッシュボード	すべてのユーザ ユーダ会計1(1,1,1,2,0,4,0)
● モニタ	> ユーザステータス ユーザ指則
	ユーザ名 > メールアドレス > メールアラー> ログインス> 役割 > 権限ステータ> 作成日時 > 直近のログイン時> アクショ
● フロア計画	admin 有類化 • システム 有効化 2023-03-08 09:16: 2023-03-08 12:54: 区
🗙 設定	y
レポート	
ш и //	»
Jo vata	
 デバイス管理 	
 ユーザ管理 	
 設定 	
• リソース	
• Nuclias Connectにつ	10°C

図 11-2 ユーザ管理 - ユーザステータスタブ

■ ログインステータスの確認

「ステータス」欄には、ユーザのログイン状態が表示されます。

- ・
 ●はユーザがログイン状態であることを示します。
- ・
 ●はユーザがログオフしていることを示します。
- ユーザプロファイルの作成 / 編集
- ユーザプロファイルを作成するには、「ユーザを追加」をクリックします。
 既存のユーザプロファイルを編集するには、ユーザのアクション欄で C をクリックします。
- 2. 以下の項目を設定します。
 - 「ユーザ名」
 - 「パスワード」
 - 「メールアドレス」
 - 「メールアラートを受信」
 - 「権限」
 - 「権限ステータス」
 - 「設置場所」
 - 「電話番号」
 - 「説明」

「権限」では、以下のユーザ権限を割り当てることができます。

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

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

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

⊛ ユーザを作成		
ユーザ名*	1	
パスワード*		
メールアドレス*		
メールアラートを受 信	● 有効化 ○ 無効化	
権限*	ルート管理者 ~	
権限ステータス*	● 有効化 ○ 無効化	
設置場所		
電話番号		
説明		
	作成 キャン	ノセル
	作成 キャン	/セル

ユーザ権限

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

システム > ユーザ管理に移動し、「ユーザ権限」タブを選択します。

<nuclias< th=""><th>Default</th><th></th><th></th><th>11:53:29 2022-12-05</th><th>I 🔕 🔀 JP 🗸</th></nuclias<>	Default			11:53:29 2022-12-05	I 🔕 🔀 JP 🗸
(3) Ø ∨ ∨ ± #− F	すべてのユーザ ユーザ合計1(↓	1 40 50)			ユーザを通加
$\begin{array}{c} (\underline{w})_{1}^{\ast} & \underline{*} = g \\ \underline{*} & \underline{*} \end{array} \rightarrow \begin{array}{c} (\underline{w})_{1}^{\ast} & \underline{*} = g \end{array}$	ユーザステータス ユーザ権限				_
550 F####	Site1				
◎ 7 = 7計画	6 Network1	権限のないユーザ	権限のあるユーザ		
	Site2		admin (システム管理者)		
🗙 設定 >					
[3] ∨*-+ →			»		
■ ¤# >			*		
× 4954 62					
・ デバイス管理					
• ユーザ管理					
 設定 					
 リソース 					
・ Nuclias Connectについ て					保存

図 11-4 ユーザ管理 - ユーザ権限タブ

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

設定

```
「設定」画面には、以下のタブが表示されます。
「一般」
「接続」
「SMTP」
「バックアップ&リストア」
「REST API」
「シングルサインオン (SSO)」
「アラート」
「FOTA」
```

一般

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

システム > 設定に移動して、「一般」タブを表示します。

< nuclias connect	Default	12:55:31 2023-03-08 🦉 🚨 😤 JP -
$ \ \qquad \qquad$		
100 200 €=2 >		
- 	カスタマイズ設定	
○ 707計画	例關係: Default	
🗙 ikiz 🕠	0 <i>2</i>	
-1-1- ×	(A)	
± ₽/ →	ドラッグ数ドロップ ロゴファイルをここへ プラウザ	
50 SX74 V	ロゴファイルはPNGもしくはJGP回復ファイル形式である必要があります。	
• デバイス管理	認証コードを表示 「行動化 ン	
 ユーザ管理 サン 	<u>現</u> 任	
• 17-X		
 Nuclias Connectについて 	デバイス設定	
	Ial Japan ~	
	タイムゾーン (GMT+09:00) Osaka, Sapporo, Tokyo ~	
	ライブバケット開始 1分 ×	
	9.47	

図 11-5 設定 - 一般タブ

「カスタマイズ設定」セクションでは、以下の設定項目が表示されます。

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

「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
王	ドロップダウンメニューをクリックして、ネットワーク内のアクセスポイントの国を選択します。
	「Japan」から設定変更しないでください。
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
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時間を選択します。
	・ 選択肢:「1分」「2分」「3分」「4分」「5分」

「保存」をクリックして設定を保存します。

接続

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

システム>設定に移動し、「接続」タブをクリックします。

<nuclias< th=""><th>Default 12:55:42 2003-09-08 🖉 🔕 💘 JP</th></nuclias<>	Default 12:55:42 2003-09-08 🖉 🔕 💘 JP
(★) ダッシュポード	
₩. 	- 16 (895 - 3011F - 27777778-57477) - Kaol AFL - 2777777472 (3330) - 775 F DUA
- ・ ポロジ	· 保健定定
◎ フロブ計画	Ø~(X79±X7FbX, 172.16.1.50 ∨
🗙 設定 🔷	ー このアドレスを変更する場合、必要に応じてダバイスを平動で検出して言語して ください。
「」 レポート ・ ・	デバイスアクセスボート このボートを変更する場合、"CiProgram Files (x86) [Nuclias connert]Core]config [appconfig.json" へも移動してボート番号を変更し、サーバを得起
u //)	熱してください。その後、必要に応じて半動で歩バイスを約枚出し、管理してください。
50 VAFA •	-)
 デバイス管理 	Webアクセスボート 30001 プラウザからアクセスできる有効なポートであることを確認してください。
 ユーザ管理 設定 	保有
 リソース Nuclias Connectについて 	SSL版明月在安定所
	証明書をアップロード プラクザ
	\$-27970-F 72999
	<i>Q.(r)</i>

図 11-6 設定 - 接続タブ

「接続設定」セクションでは、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

「SSL 証明書を更新」セクションでは、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

SMTP

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

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

<nuclias< th=""><th>Default</th><th>12:55:53 2023-03-08 🖉 🚨 💉 JP</th></nuclias<>	Default	12:55:53 2023-03-08 🖉 🚨 💉 JP
(b) ダッシュポード	一般 接接 SMTP バックアップ&リストア REST API シングルサインオン (SSO) アラート FOTD	A
100 €= Ø →		
	カスクマイズ設定	
◎ フロア計画	SMIP $\psi \rightarrow i^{\pm}$ $\psi \rightarrow i^{\pm}$	
🗙 設定 🔷 🔸	₩~- 1.* 25 ¥	
「」 レポート >	送得元メールアドレス* 送信元メールアドレス	
<u>ت</u> ۵۶ ک	送留元 送留元	
 システム デバイス管理 	484.1974949	
 ユーザ管理 設定 	∞ y 2 − F 2 4 7 UTF-8 v	
• J7-x	認証 アノニマス マ	
• Nuclias Connectについて	7x1×-k 7x1×-k	
	R #	

図 11-7 設定 - SMTP タブ

以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。



注意 v1.2.0.9 以降のバージョンでは、SMTP 認証のユーザ名は @ を含むメールアドレス形式のみ受け付けられます。ログインアカウント形式を 使用している場合、v1.2.0.9へのアップグレード以降、メールアドレス形式に変更が必要となります。

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

バックアップ&リストア

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

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

■ 自動バックアップ

コンフィグレーションの自動バックアップ設定を行います。

自動バックアップ	有効化 ~
時間間隔	7 H 12:00 V
バックアップファイル	
バックアップバス	C:\Program Files (x86)\Nuclias connect\web\Backup 褒更

図 11-8 自動バックアップ設定

「自動バックアップ設定」セクションには、以下の設定項目が表示されます。

項目	説明
自動バックアップ	自動バックアップを有効 / 無効に設定します。
時間間隔	バックアップ間隔を設定します。
バックアップファイル	バックアップするファイルの種類を選択します。
	 選択肢:「設定」
バックアップパス	ファイルの保存先を指定します。

「保存」をクリックして設定を保存します。

■ バックアップ設定

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



図 11-9 バックアップ設定

「バックアップ設定」セクションには、以下の設定項目が表示されます。

項目	説明
上書き	本項目にチェックを入れると、ハードディスクが一杯に近くなった場合に古いログを上書きします。
設定	• 現在の設定を保存するには「すぐにバックアップ」をクリックします。
	・ 保存した設定をダウンロードするには「ダウンロード」ボタンをクリックします。
	• 保存した設定を削除するには「削除」ボタンをクリックします。
ログ	・ 現在のログを保存するには「すぐにバックアップ」をクリックします。
	 保存したログをダウンロードするには「ダウンロード」ボタンをクリックします。
	・ 保存したログを削除するには「削除」ボタンをクリックします。

■ リストア設定

コンフィグレーションのリストアを行います。

設定	ファイルを選択	リストア
	設定	設定 ファイルを選択

「リストア設定」セクションには、以下の設定項目が表示されます。

項目	説明
設定	「ファイルを選択」をクリックして保存済みのバックアップファイルを選択し、「リストア」ボタンをクリックして設定 を復元します。

注意 リストア後、Nuclias Connect コアサーバおよび Web サーバを再起動する必要があります。再起動後、再度ログインしてください。

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

REST API

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

システム > 設定に移動し、「REST API」タブをクリックします。

< nuclias	Default 12:56:29 2023-03-08
(F) ダッシュボード	
ن ح الم	- R 1860 2011 - 227) 27 @ 3 A F / A E D I AFI - 227/27 4 7 3 7 (330) - 17 - F F U IA
	REST API
● フロア計画	ネットワークIDのないネットワークには、REST APIともアクセスできないことに注意してください。 PFST API 無効化
🗙 設定 🔷 👌	

🗐 ¤# >	
- AFR •	
 デバイス管理 	
 ユーザ管理 	
 設定 リソーマ 	
 Nuclias Connectについ 	τ

図 11-11 設定 - REST API タブ

以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

シングルサインオン(SSO)

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

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

<pre><nuclias connect<="" pre=""></nuclias></pre>	Default			12:56:31 2023-03-08	<u>@</u>	💘 JP 🤇
(i) ダッシュボード	55 15755 CO.CO.	A P				
モニタ >	THE 1200 SMIP NY	2/7/&yAF/ RESIAFI	55976945457 (330)	J J F FOIA		
▶ポロジ	シングルサインオンを使用すると	、一つのNucliasアカウントを使用し	てNucliasクラウドボータルもしく	はNuclias Connectボータル にアクセス	できます。	
② フロア計画	このコントローラが30日を超え (SSO)オブションを有効化して In addition, the backup and restr	てオフラインになると、シングルサイ て、Nueliasアカウントに再度ログイ: ore function does not save SSO settin	ンオン(SSO)オブションが自動的 (する必要があります。 gs, please configure SSO settings ag	向に無効化されることに注意してくださ ain if device configuration has been rest	い。シングルサインオン ored.	
* 設定 >	シングルサインオン	を有効化				
「」レポート >	Nucliasアカウント*					
■ 1 / >	Nucliasパスワード*		長さ	は8~64です。		
		アカウントを作成				
 デバイス管理 		適用				
 ユーザ管理 						
 設定 						
• リソース						
• Nuclias Connectについて						

図 11-12 設定 - シングルサインオン(SSO)タブ

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

■ アカウントの登録

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

	<pre>c nuclias</pre>	
新しいアカウント されます。カスタ す。	へと組織は、選択した地域内 ₽マーサービスは選択された	のサーバーに作成 国に転送されま
サーバの地域	ŧ	
Asia		·
E		
Japan		

図 11-13 地域 / 国の選択

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

<pre>/ nucli</pre>	26
by I	D-Link
ЕХ—Л	
フルネーム	
パスワード	0
新しいパスワードの確認	0
組織名	
Japan	
Asia/Tokyo(UTC+09:00, DST)	-
住所	
) 私はこれらを全て読み、同意しま <u>プライバシー</u>) D-Link製品のアップデートやオフ: せします。	す。 : <u>利用規約</u> 並びに ァーをメールでお知ら
私は人間です	۲

図 11-14 アカウント情報の入力

- 3. 入力後、CAPTCHA 認証を行い、「アカウントの作成」をクリックします。
- **4.** アカウント作成後、登録したメールアドレスへ Nuclias(verify@nuclias.com)から認証メールが送信されます。メール内に記載されたアクティ ベーション用の URL をクリックし、Nuclias アカウントのアクティベーションを行ってください。

■ シングルサインオン設定

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

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

______ 「保存」をクリックして設定を保存します。

■ Nuclias Connect ポータルへの接続

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

步	ッシュボ	- F ~	J						
						タイプ: 全て	• 状腺:	金T •	Q 検索 @
#	状醚	名前	ホスト	₩₹₽	ネットワーク	デバイス	クライアント	バージョン	アクション
1	٠	Default	470 843 (0,420 849 849 114	1	1	1/1	0	1.2.0.9	€起数 - 形除

図 11-15 Nuclias Connect ポータル

Nuclias Connect ポータルでは、以下の項目が表示されます。

項目	説明
状態	Nuclias Connect ポータルと DNC-100 間の接続ステータスを表示します。
名前	Nuclias Connect の名前を表示します。
ホスト	デバイスの IP アドレスとパブリック IP アドレスの両方を表示します。
サイト	DNC-100 によって管理されるサイトの数を表示します。
ネットワーク	DNC-100 によって管理されるネットワークの数を表示します。
デバイス	DNC-100 によって管理されるデバイスの数を表示します。
クライアント	DNC100 によって管理されるデバイスに接続されているクライアントの数を表示します。
バージョン	DNC-100 のソフトウェアバージョンを表示します。
アクション	「起動」をクリックして、DNC-100のインタフェースを開きます。ファイアウォールやルータを介した通信の場合、IPマッ
	ピングが必要です。
	「削除」を選択して、Nuclias Connect ポータルから DNC-100 のリンクを解除します。(「削除」は、デバイスがオフライ
	ンの場合にのみ使用できます。)

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

アラート

アラートタブでは、アラート / メール通知を行うイベントの種類を設定できます。

システム>設定に移動し、「アラート」タブをクリックします。

<nuclias connect</nuclias 	Default				12:56:54 2023-03-08	<u>k</u>	٩	*	JP v
(一般 接続 SMTP パッ	クアップ&リスト:	ア RESTAPI シングルラインオン(SSO)	アラート FOTA					
₩ <u></u> €=\$									
Fainst	サイト/ネットワーク	イベント							
◎ フロア計画		アラート	メールアドレス						
* 202 >	ファームウェアの更新に失 取しました	>							
la v#−t →	デバイスはネットワークか ら削除されました。								
<u>ار میں اور اور اور اور اور اور اور اور اور اور</u>	プロファイルが変更されま した								
- × ×7× •	プロファイルを適用できま せんでした。	V							
 デバイス管理 ユーゼ党印 	新しいファームウェアリリ ース								
• 設定	デバイスイベント								
・リソース		アラート	メールアドレス						
 Nuclias Connectについて 	デバイスが再起動されました。 た。	~							
	デバイスオフライン	~							
	デバイスオンライン								
	ポートリンクダウン								
	プロックされたポート	~							
		保存							

図 11-16 設定 - アラートタブ

■ アラートの設定

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

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

■ 生成されたアラートの確認

生成されたアラートは、ログ>アラートに移動して確認できます。

■ 電子メールアラートの設定

電子メールでアラートを受信するには、以下の設定を行います。

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

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

FOTA

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

システム > 設定に移動し、「FOTA」タブをクリックします。

< nuclias	Default 12:57:06 2023-03-08
(注) ダッシュボード	
100 €=9 >	- TR 1997 Solif ハッツリッフィクストナ RESIAPI シングルサインオン (SSU) ファート FULA
the stars	自動撮影が作前になっている場合、システム>設定>アラート内の新しいファームウェアリリースのアラート設定およびメール設定が作物になることに注意してください。
◎ フロア計画	自動的にファームウェアパージョンを確認
🗙 設定 🔷 🔸	報認問題 24 (1-720)時間
レポート >	<u>8.7</u>
■ ¤ // →	
50 8×74 ×	
• デバイス管理	
 ユーザ管理 	
 設定 	
 リソース Nuclias Connectについて 	

図 11-17 設定 - FOTA タブ



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

リソース

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



システム > リソースに移動して以下の画面を表示します。

図 11-18 リソース

Nuclias Connect について

「Nuclias Connect について」画面には、Nuclias Connect のバージョンが表示されます。

```
システム > Nuclias Connect についてに移動して情報を表示します。
```

<pre>< nuclias connect</pre>	Default		12:57:24 2023-03-08 🖉 🚨 💘 JP 🗸
(F) ダッシュポード	バージョン: 1.2.0.9b1 (14/Jan/2020 18:12:39について	·····································	ペートされました。) オンライン更新
1000 €=\$ >			デバイスタイプ 全てのデバイスタイン 絵志方法 チデル委員 シーターデン会社会 [5]
555 F##\$	モデル番号 エー・ソフトウェアバージョン ゴ	ハードウェアバージョム	2011年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日
◎ フロア計画	DAP-2230	A1, A2	Nuclias Connect Wireless N PoE Access Point
🗙 設定 🔹 🔸	DAP-2310	B1, B2	Nuclias Connect Wireless N PoE Access Point
レポート >	DAP-2360	B1, B2	Nuclias Connect Wireless N PoE Access Point
	DAP-2610	Aı	Nuclias Connect AC2300 Wave 2 Access Point
	DAP-2620	Aı	Nuclias Connect AC1200 Wave 2 Wall Plate Access Point
So vafa v	DAP-2622	Aı	Nuclias Connect AC1200 Wave 2 Wall Plate Access Point
• デバイス管理	DAP-2660	A1, A2	Nuclias Connect AC1200 PoE Access Point
 ユーザ管理 設定 	DAP-2662	Aı	Nuclias Connect AC1200 Wave 2 Access Point
• <i>リ</i> ソース	DAP-2680	Aı	Nuclias Connect AC1750 Wave 2 Access Point
• Nuclias Connectについて	DAP-2682	Aı	Nuclias Connect AC2300 Wave 2 Access Point
	DAP-2695	A1, A2	Nuclias Connect AC1750 PoE Access Point
	DAP-3315	Aı	Wireless N Exterior Access Point
	D48-0666	4.	Nunlise Connert & Cronn Wave a Outdoor & onese Paint
	1-20 of 32 トータルアイテム: 32		《 く 1 /2 > >> 20 v ページごとのアイテム
		© 2018-202 Terms o	2 D-Link Corporation. All rights reserved.

図 11-19 Nuclias Connect について

Nuclias Connect のバージョン情報の下には、サポートされる製品のリストが表示されます。 「オンライン更新」をクリックすると、更新情報がある場合、製品のリストが更新されます。

注意 現在、日本でサポートされる製品は DAP-X2850、DAP-X2810、DAP-2610、DAP-2680、DAP-3666 のみです。(「Nuclias Connect 対応機器 (p.7)」を参照)

【付録】機能別サポート製品 / バージョンについて

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

項目	サポートされる製品 / バージョン		
	スタンドアロンモード	DNC-100 管理モード	
プロファイル設定 - アクセスポイント - St	SID - セキュリティ		
高速ローミング(802.11 k/r)	• DAP-3666	• DAP-X2850	
		• DAP-X2810(v1.20r032以上)	
		• DAP-3666	
		・ DAP-2610(v2.06B06r097 以上)	
Enhanced Open	• DAP-X2850	• DAP-X2850	
	・DAP-X2810(v1.20r032以上)	・ DAP-X2810(v1.20r032 以上)	
	• DAP-3666	• DAP-3666	
	• DAP-2610(v2.06B06r097以上)	• DAP-2610(v2.06B06r097以上)	
WPA3	• DAP-X2850	• DAP-X2850	
	• DAP-3666	• DAP-X2810(v1.20r032以上)	
	• DAP-2610(v2.06B06r097以上)	• DAP-3666	
	• DAP-X2810(v1.20r032以上)	• DAP-2610(v2.06B06r097以上)	
ネットワークアクセス保護	• DAP-X2850	• DAP-X2850	
	• DAP-X2810	• DAP-X2810(v1.20r032以上)	
	• DAP-2680	• DAP-3666	
	• DAP-2610	• DAP-2680 (v2.00B08r051 以上)	
		• DAP-2610(v2.01B05r073以上)	
ブロファイル設定 - アクセスボイント - St	SID - ユーザ認証		
外部キャフティフホータル認証	-	• DAP-X2850	
		• DAP-3666	
		• DAP-2610 (v2.06B06r097以上)	
		• DAP-X2850	
		• DAP-2610(v2.06B06r097以上)	
クリックスルー認証	• DAP-X2850	• DAP-X2850	
	• DAP-3666		
		• DAP-2610 (V2.06B06r097 以上)	
	• DAP-2010(V2.06B061097 以上)	• DAP-72850	
		• DAP-5000 • DAP 2610 (y_2 06P06r007 (y_1 E)	
		• DAP-2010 (V2.000001097 LL)	
		• DAP $X2810$ (v1 20r032 1V H)	
		• DAP-72810 (V1.201032 1/L)	
		• DAP-2610 ($\sqrt{2}$ 06B06r097 [$\sqrt{2}$]	
セッションタイトアウト		• DAP-X2850	
		• DAP-X2810 (v120r032 LV H)	
		• DAP-3666	
		• DAP-2610 (v2.06B06r097 以上)	
リモート RADIUS 認証	・ DAP-2610 (v2.06B06r097 以上)	• DAP-X2850	
		• DAP-2610 (v2.06B06r097 以上)	
	• DAP-X2850	• DAP-X2850	
	• DAP-2610 (v2.06B06r097 $k/ +$)	• DAP-2610 (v 2.06B06r097 L/L +)	
- ア カワンティングリーハ改正			
ノロノアイル設定 - アクセスホインド - 3. Hotspot20	DAP-3666	• DAP-3666	
Thorspore $プロファイル設定 - アクセスポイント - R$	F 是商化	• DAI-3000	
		• DAP-X2850	
		DAP-3666	
		• DAP-2680 (v_2 00808r051 $ v_1 $ +)	
		• DAP-2610 (v2.01805r073 1) +)	
パフォーマンス設定	l		
STP (スパニングツリー) *1	• DAP-X2850	• DAP-X2850	
	• DAP-3666	• DAP-3666	

【付録】機能別サポート製品/バージョンについて

項目	サポートされる製品 / バージョン	
WLAN パーティション	· ·	
リンクインテグリティ	• DAP-X2850	• DAP-X2850
	• DAP-X2810	• DAP-X2810(v1.20r032以上)
	• DAP-2680	• DAP-2680 (v2.00B08r051 以上)
	• DAP-2610	• DAP-2610 (v2.01B05r073 以上)
ワイヤレスリソース		
エアタイムフェアネス	• DAP-X2850	• DAP-X2850
	• DAP-X2810(v1.20r032以上)	• DAP-X2810(v1.20r032以上)
	• DAP-3666	• DAP-3666
	• DAP-2680	• DAP-2680(v2.00B08r051以上)
	• DAP-2610(v2.06B06r097以上)	• DAP-2610 (v2.06B06r097 以上)
隣接 AP	• DAP-X2850	• DAP-X2850
	• DAP-X2810	• DAP-X2810(v1.20r032以上)
	• DAP-3666	• DAP-3666
	• DAP-2680	• DAP-2610(v2.06B06r097以上)
	• DAP-2610	

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

※ Nuclias Connect 対応製品のみ掲載しています。