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。

目次	
*	5
本マニュア 100 対象 4	5
第1章 製品概要	6
Nuclias Connect (DNC-100) ICOLVZ	6
サポート機能	6
推奨システム要件	7
Nuclias Connect 対応機器	7
第2章 ソフトウェアのセットアップ	8
Windows への Nuclias Connect インストール	8
ソフトウェアのインストール Nucline Connect サーバの中海	8
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	16
データベースプロファイルの設定 サーバ IP アドレスの絵奏	18 10
ッーハド アドレベの検索 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	20
Nuclias Connect へのログイン アクティベーション	
アフリィーション 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	27
Nuclias Connect アブリケーションを使用した AP の検出と設定 ラットロークプロファイルの削除	
ネットワーフラロファイルの前線 管理対象アクセスポイントの確認	
ファームウェアのアップロード	
第 3 章 Nuclias Connet の管理インタフェース	40
Nuclias Connect への接続	
ワイサート ユーザプロファイル	
個人情報	43
セキュリティ	
第4章 ダッシュボード	45
	16
	40
ゲクセスホイント ワイヤレスクライアント	
接続されたクライアント	
ブロックされたクライアント	
第6章 設定	49
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	
SSID	
VLAN	63
VLAN リスト ポートリスト	
VLAN を追加 / 編集	63
PVID 設定	
〒 場置の 最適化	64
スケジュール	
デバイス設定	67
ハノォーヾノム設正 WLAN パーティション	68
ワイヤレスリソース	72
ファームウェアアップグレード ccl =エ四圭	

Ίը

لي_

Ξh

гб

目次

ц	
 第7章 レポート	78
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	
第8章 ログ	82
SNMP トラップ	
シスログ	
システムイベントログ	
デバイスログ	
第9章 システム管理	86
<u>第9章 システム管理</u> デバイス管理	<u> </u>
<u>第9章 システム管理</u> デバイス管理 ューザ管理	86
<u>第9章 システム管理</u> デバイス管理 ユーザ管理 ユーザステータス	86
<u>第9章 システム管理</u> デバイス管理 ユーザ管理 ユーザステータス ユーザ権限	86
<u>第9章 システム管理</u> 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	86
第9章 システム管理 デバイス管理 ユーザ管理 ユーザ管理 ユーザステータス ユーザ椎限 ーサ権限 設定 ー般	86 86 87 87 87 88 88 88 89 89
第9章 システム管理 デバイス管理 ユーザ管理 ユーザ管理 ユーザステータス ユーザ権限 ローザ権限 設定 一般 接続	86 86 87 87 87 88 88 89 89 90
第9章 システム管理 デバイス管理 ユーザ管理 ユーザアクラータス ユーザ権限 設定 一般 接続 SMTP	86 87 87 87 88 88 89 89 90 90 91
第9章 システム管理 デバイス管理 ユーザ管理 ユーザを理 ユーザステータス ユーザ権限 ローザ権限 設定 一般 接続 SMTP バックアップ バックアップ	86 87 87 87 87 88 88 89 89 90 90 91 92
第9章 システム管理 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 REST API	86 87 87 87 88 88 89 89 90 90 91 91 92 93
第9章 システム管理 デバイス管理	86 86 87 87 87 88 88 89 89 90 90 91 91 92 93 94

٦.μ

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1000AP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/Trap 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/Trap 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
- 国の選択
- ・ 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

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	1000 台	100 台
推奨 CPU	8 世代 Intel® Core ™ i7 プロセッサ	Intel® Core ™ i5 プロセッサ 3.2 GHz
推奨 RAM	16G DDR3	8G DDR3
推奨ストレージ容量	4TB	2TB
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-2610	DAP-2610/A1	R2.01B05r073
DAP-2680	DAP-2680/A1	R2.00B08r051

※ 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 Connet の管理インタフェース (p.40)」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 DAP 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.27)」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、新規に新しい Nuclias Connect をインストールする手順を推奨します。
- 1. 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。
- 2. 「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 1.0.2.11 Se	tup — 🗆 🗙
P () () () () () () () () () (Welcome to the Nuclias connect 1.0.2.11 Setup Wizard
	Next > Cancel

図 2-1 Nuclias Connect - セットアップウィザード

3. 「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。



4. 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。

rt Configuration				
et the port which Nu	lias connect to Listen.			2
Nuclias connect will Listening Port. Click	sten the following port. To Next to continue.	listen to a different	port, modi	fy the
Port Settings				
Web Port:	30001			
CoreServer Port:	8443			
Port check pass!				Check
	-		_	

図 2-3 Nuclias Connect - ポート設定

5. 「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。

itabase Service Environment Check Theoling MongoDB database service requir	red by the Nucliss connect
חפראווק אוטווקטטט טמנמטמצפ צפו אוכפ רפקטו	
MongoDB status summary	
A Service named " MongoDB ":	Not installed
MongoDB service running status:	Not running
The running MongoDB version:	
Nuclias requires a database service prov a new MongoDB 4.0.17', the installation as a MongoDB service on the server. If you can let Nuclias to connect a remote	ided by MongoDB 4.0.17. So if you choose 'Insta will try to install MongoDB 4.0.17 and register it you choose 'Use an existing MongoDB 4.0.17', MongoDB service.
Install a new MongoDB 4.0.17	OUse an existing MongoDB 4.0.17

図 2-4 Nuclias Connect - MongoBD サービスステータスのチェック

6. 「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, usei	rname and pass	word	
MongoDB Port:	27010			
User name:				
-	[
Password:]		

図 2-5 Nuclias Connect - MongoDB データベース設定

 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。 8. 「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。

「Install」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。

hoose Install Location					-
Choose the folder in which to install Nuclias connect 1.1	0.2.11.				am
Setup will install Nuclias connect 1.0.2.11 in the followi older, click Browse and select another folder. Click Ins	ng folder. 1 itall to start	fo install the inst	in a dif allation	ferent 1.	
Destination Folder					
Destination Folder C:¥Program Files (x86)¥Nuclias connect			Brow	se	
Destination Folder			Brow	se	
Destination Folder C:¥Program Files (x86)¥Nuclias connect ipace required: 200.3MB ipace available: 131.3GB			Brow	se	
Destination Folder			Brow	se	

図 2-6 Nuclias Connect - インストールフォルダの指定およびインストールの開始

- 9. 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手順に 進みます。
- WinPcap セットアップウィザード画面が表示されます。WinPcap をインストールすると、Windows 環境でリンクレイヤのネットワークアクセ スが可能になり、アプリケーションがプロトコルスタックをバイパスしてネットワークパケットをキャプチャおよび送信できるようになります。 これらの機能には、カーネルレベルのパケットフィルタリング、ネットワーク統計エンジン、およびリモートパケットキャプチャのサポートが 含まれます。

「Next>」ボタンをクリックしてセットアップウィザードを開始します。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。

😽 WinPcap 4.1.3 Setup	— D. X
	Welcome to the WinPcap 4.1.3 Setup Wizard This Wizard will guide you through the entire WinPcap installation. For more information or support, please visit the WinPcap home page. http://www.winpcap.org
	Next > Cancel

図 2-7 WinPcap - セットアップウィザード

- **11.**「License Agreement (使用許諾)」画面が表示されます。WinPcap を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。
 - 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。

WinPcap 4.1.3 Setup				
Vin Pcap	License Agreemen Please review the lic	t ense terms be	efore installing W	'inPcap 4.1.3.
Press Page Down to see the	e rest of the agreemen	ıt.		
Copyright (c) 1999 - 2005 f Copyright (c) 2005 - 2010 (Copyright (c) 2010 - 2013 f All rights reserved. Redistribution and use in sc	VetGroup, Politecnico o CACE Technologies, Da Viverbed Technology, S Durce and binary forms	di Torino (Italy avis (California San Francisco with or with	r). a). (California). out modification.	are
permitted provided that the 1. Redistributions of source conditions and the following 2. Redistributions in binary	Following conditions a code must retain the disclaimer. form must reproduce t	are met: above copyrio the above cop	ght notice, this lis	st of is list of ↓
If you accept the terms of t agreement to install WinPca	he agreement, click I / p 4.1.3.	Agree to conti	nue, You must a	ccept the
		< Back	I Agree	Cancel
] 2-8 WinPcap - 使序	月許諾			

12. 「Install」ボタンをクリックしてインストールを開始します。

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。

😚 WinPcap 4.1.3 Setup		×
Win Pcaf	Installation options Please review the following options before installing WinPca 4.1.3	эр
Automatically start	the WinPcap driver at boot time	
Jullsoft Install System v2.46	< Back Install Car	ncel

図 2-9 WinPcap - インストール開始

13. WinPcap のインストールが完了すると、セットアップウィザードの完了画面が表示されます。「Finish」ボタンをクリックして、インストールウィ ザードを終了します。

😽 WinPcap 4.1.3 Setup	- D. X.
	Completing the WinPcap 4.1.3 Setup Wizard
	WinPcap 4.1.3 has been installed on your computer.
	Click Finish to close this wizard.
Cart !!	
Carlor and	
1220	
	< Back Finish Cancel

図 2-10 WinPcap - セットアップウィザードの完了

14. WinPcap がインストールされると、Nuclias Connect セットアップウィザードがインストールを続行します。

「Windows セキュリティの重要な警告」画面に、Serverside 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。

15. 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。「Next」ボタンをクリックします。

		con
moleted		
(NOT_STOPPABLE, NO	T_PAUSABLE, IGNORES_SHUTDOWN)	~
WIN32_EXIT_CODE : 0 (0×0)		
SERVICE_EXIT_CODE : 0 (0×0)		
CHECKPOINT : 0x0		
WAIT_HINT : 0x7d0		
PID : 13436		
FLAGS :		
Start Nuclias connect Web server successf	ully.	
Create shortcut: C:¥ProgramData¥Microso	ft¥Windows¥Start Menu¥Programs¥Nuclia	1
Iompleted		~
		_
	Z Back Next > Con	e al

16. 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。「Reboot now(今すぐ再起動)」を選択し、「Finish」をクリックします。



図 2-12 Nuclias Connect - セットアップウィザードの完了

17.「はい」を選択し、コンピュータを再起動します。

🛄 Nucl	ias connect 1.0.2.11 Set	tup >	
Δ	Do you wish to reboot	the system?	
	はい(^)	いいえ(N)	
図 2-13	再起動確認メッセージ		

18. インストール後、「Nuclias Connect Service Configurator」、「Nuclias Connect」のショートカットがプログラム一覧に次のように表示されます。



図 2-14 Windows ショートカットメニュー

Nuclias Connect サーバの実行

ここでは、Nuclias Connect サーバアプリケーションの実行方法について説明します。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。



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 Connect Service Configurate をクリックして Nuclias Connect Setup を開きます。本画面には、「Restart/Stop Services」および「Launch a Browser to Manage the Network」ボタンがあります。

368

■ 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.32)」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 Bock Next
© 2019 D-Link Corporation English 🗸 🧹

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. サーバの地域と国を選択し、「Next」をクリックします。アカウントは、選択した地域および国のサーバ内に作成されます。

ct server region) and country.
	nuclias
	by D-Link
Your new account	t and organization will be created on servers
within the region	selected. The customer service will be forward u selected.
	Restander 20
Server region	17
	-
Country	
	÷
	Next
	Already have an account? Log in



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。

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

「Create account」をクリックして続行します。

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

図 2-18 アカウント情報の入力

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



図 2-19 完了画面

4. Nuclias アカウントは、使用前に検証される必要があります。verify@nuclias.com から、認証リンクが記載された電子メールが届きます。認証リ ンクをクリックして、Nuclias アカウントをアクティベートしてください。

認証完了後、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、ログイン手順を省略できます。

< nuc	by D-Link
Email	
Password	٢
Stay logged in	
Log	şin
Forgot password	Create account

図 2-20 ログイン画面

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://192.168.10.1:30001 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、 Nuclias connect Service Configurat... 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 Conne	ect		
1.0.2.11			"
Restart Services	Stop Services		
Launch a Browser to	Manage the Network]	
Copyright(C)2018-2020 [)–Link. All Rights Reser	ved.	

- 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、 いい Nuclias connect
 Web ブラウザを開きます。



図 2-22 Nuclias Connect ログイン画面

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

補足

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

	Your password	
	Please input the captch 1557	Forgot ponoverd?
	Login	
	© 2019 D-Link Corporation	çish v
図 2-23	アカウント情報入去	カオプション

3. Web ブラウザが開き、サーバに正常に接続すると、パスワード変更ダイアログが表示されます。最初のログイン後に、デフォルトのパスワードを変更する必要があります。

パスワードを割り当てる場合は、強力なパスワードを使用することをお勧めします。新しいパスワードの長さは5~16文字である必要があります。 大文字と小文字、数字、記号を組み合わせることで、強力なパスワードを作成できます。

< nuclias connect
You need to change your password after the first login. Strong password consisting of 5 - 16 characters is required. Combine uppercase letters, lowercase. letters, numbers and symbols. Do not include common words or names.
Jold password
new password
confirm password
Modify
© 2019 D-Link Corporation English 🗸
 図 2-24 パスワードの変更

注意 一般的な単語や名前は使用しないでください。

現在のパスワードを「old password」フィールドに入力し、「new password」フィールドに新しいパスワードを入力します。 「confirm password」フィールドに同じパスワードを入力して、入力内容を確認します。「Modify」をクリックして処理を完了します。 **4.** 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が変更 された場合は、Nuclias Connect Core サーバを再起動する必要があります。

			ta been energea.	
Device Access Address	Pick one	~		
Device Access Part	8443			
Country	Pick one	×		
Time Zone	Pick one		×	

補足

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

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。

<pre><nuclias connect<="" pre=""></nuclias></pre>		Default						試用 (6 日)	、クリックしてアク	71-1	🕽 🤻 јр
🚯 Ø782#-F									_		
[11] ユン エータ	>	15:30	15:45	16:00	16:15	16:30	15:30	15:45	16:00	16:15	16:30
🗙 設定	>				ダウンリンク 📕	アップリンク					
「」 レポート	>										
国 ログ	>	チャネル利用]率								
50 vx74	>	2.4GH27	キャネルのAP	- 6 -	8	0	10				

図 2-26 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 Connect は、20日間の試用版とし この期間を超えてNuclias Connect を引き は、以下のリンクを使用して詳細情報を登 Connect を有効にしてください。	て提供されています。 歳き使用したい場合 登録して、Nuclias
メールアドレス	
パスワード	
アカウントがありませんか?	トぐに登録
	次へ 終了

図 2-27 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 ∨
Pick one ~
適用 終了

図 2-28 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 2-29 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 DAP 製品を管理するために必要なネットワークプロファイルを Nuclias サーバからエクスポートする方法について 説明します。Nuclias Connect アプリの機能を説明する追加情報も含まれています。

ネットワークプロファイルのエクスポート

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

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

<nuclias< th=""><th>Default</th><th>🔕 Ҟ JP 🗸</th></nuclias<>	Default	🔕 Ҟ JP 🗸
(デ) ダッシュポード	全てのサイト v 合計1ネットワーク 合計1/1オンフインAP 合計0クライアント	ネットワークを追加
■】 まニタ >	サイト名 * * ネットワーク名 * * 合計デバイス * オンラインデバビ クライアント * プロファイル * 検出 *	アクション
🗙 設定 🔷 🔪	site1 Network1 1 1 0 🕑 🗋 🔍	C O
• プロファイルを作成		
 プロファイル設定 ファームウェブブッブグ レード SSL証明書 決許代行システム 		
Image: 1 → 1		
E = 7 >		
Go vata >		
	1-15of1 k-\$k7f7£:1	ページごとのアイテム

図 2-30 プロファイルを作成

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

一般 接続 SMTP バック	アテップ REST API シングルサインオン(SSO)
接統設定	
デバイスアクセスアドレス	その他 ~ 192168.0.60
デバイスアクセスボート	8443 ポートを変更するには、"Ct\Program Files (x86)\Nuclias connect\Core\config\appconfig.json" へ移動し、必要に応じてポート番号を編集してく
コプサーバアクセスポート	8443
Webプクセスポート	30001
	87

図 2-31 設定 - 接続タブ

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

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

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

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

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

※現在 Android アプリからの管理はできません。2021 年 Q1 にリリースされるアプリケーションを利用することで可能になります。

クイックセットアップ

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



図 2-32 Nuclias Connect アプリ(iOS)

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

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

STEP 1: プロビジョニングプロファイルの選択

- 1. 「Quick Setup」をタップすると、「STEP 1」画面が表示されます。
- **2.** 「Provision File」をタップして、使用可能なローカルプロファイルのリストを表示します。ローカルに保存されているプロファイルが存在しない場合は、プロファイルをダウンロードする手順を示すポップアップページが表示されます。
- 3. Nuclias Connect コントローラへ接続しプロファイルをダウンロードするには、「Download Profile」を選択します。



図 2-33 STEP 1 - プロファイルのダウンロード

- 4. Nuclias Connect コントローラの接続が確立されると、「Provision File」フィールドにエントリが表示されます。
- 5. 「Provision File」をタップして、ローカル AP プロビジョンプロファイルを選択します。次の図では、エントリ Nuclias_test_Network1 を使用できます。

<	Quick Setup
•	0
STEP 1:	
Please select an A Access Points.	P Provision Profile to push to suitable
Provision File	nüclias.connect_test_Network132 >
storage, please gi steps there to get	to the Nuclas Connect and follow the a suitable AP Provision profile.

図 2-34 STEP 1 - プロビジョンプロファイルの選択

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



図 2-35 STEP 1 - プロビジョンプロファイルの選択

■ STEP 2: アクセスポイント検出範囲の定義

処理が続行され、アプリは前の画面に戻ります。「STEP 1」の画面で「Next」をタップして続行します。「STEP 2」画面が表示されます。この画面から、 L2/L3 ワイヤレスネットワークに接続されているスタンドアロン DAP を検出することができます。

- 1. L2 フィールドのボタンをタップして、L2 ネットワークで検出を有効にします。また、L3 フィールドのボタンをタップして、L3 ネットワーク で検出を有効にします。
- 2. 「From」および「To」フィールドに IP 範囲を入力します。追加ボタン(→)をタップして、新しい IP 範囲エントリを作成します。削除ボタン
 (●)をタップして、定義済みの範囲エントリを削除します。
- 3. 「IP range」フィールドで、開始 IP アドレスと終了 IP アドレスを指定します。範囲を定義した後、「Next」をタップして検出プロセスを開始します。

11 T 10 10 10 10	G 9:2	8 AM	1.3	6 4% 💻
<	Quick	Setup		
-		-		-0
STEP 2:				
Discover sta wireless net	indalone Access I works	Points in	L2/L3	
L2				0
				0
L3				
C3	192.168.1.50	to	192.168.1.20	0 0

図 2-36 STEP 2 - アクセスポイント検出範囲の定義

■ STEP 3: アクセスポイントへのプロファイル適用

- 1. ネットワーク範囲のスキャンが終了すると、「STEP 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. DAP の横にあるラジオボタンをタップして選択します。STEP 1 で選択したローカルのプロビジョニングファイルが、選択した DAP にプッシュ 配信されます。
- 3. 「Push Provision File」をタップして続行します。

中華電信 🗢	9:49 AM	0 61%
<	Quick Setup	5
•		
STEP 3:		
heck the settings f he Access Points yo	or each Access Point be ou want to push the prov	low then select ision file to.
Siscovered AP List		ی چ
DAP-2662	19	2.168.1.166
41.00	00.443	Ca.CC.35-10

図 2-37 STEP 3 - アクセスポイントの選択

4. DAP ログインのポップアップウィンドウが表示されます。選択した DAP へのアクセスを許可するユーザ名とパスワードを入力します。



図 2-38 STEP 3 - アクセスポイントへのログイン

5. 「Apply (適用)」をタップして、ログインプロセスを続行します。「Modify IP Information」画面が表示されます。これらの表示項目は変更する ことができます。詳細については、次の表を参照してください。

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

- 6. 「Apply(適用)」または「Cancel(キャンセル)」をタップして、処理を続行します。プロビジョニングファイルは、選択した DAP デバイス(複数可)にプッシュされます。STEP 3 の画面に戻り、プッシュ機能のステータスが表示されます。検出された DAP には、プッシュ機能の状態が 正常または失敗のいずれかの状態で表示されます。以下の図を参照してください。
- 7. 「Finish(終了)」をタップしてプロセスを完了します。処理に失敗した場合は、「Push Provision」をタップしてプッシュ機能を再試行します。



図 2-39 STEP 3 - プロファイルの適用

Nuclias Connect サーバへの接続

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

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



図 2-40 Nuclias Connect アプリ - トップ画面

Welcome 画面が表示されます。過去にペアリングされた Nuclias Connect サーバが存在しない場合は、新しい Nuclias Connect ペアリングを作成するように求められます。追加(+) ボタンをタップして、処理を開始します。



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

項目	記明
Specify NucliasConnect	アプリとペアリングする Nuclias Connect サーバのセキュアな URL/IP アドレスを入力します。
URL/IP Address	
Specify a reference name	ペアになる Nuclias Connect サーバを簡単に識別するための名前を入力します。
User name	Nuclias Connect サーバにアクセスする権限を持つユーザ名を入力します。
Password	Nuclias Connect サーバにアクセスする権限を持つユーザのパスワードを入力します。
Login	「Login」をタップして、ログイン処理を開始します。

4. 「Login」をタップして、ログイン処理を開始します。



図 2-42 利尻リーハベのロワイン画面

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



図 2-43 Nuclias Connect サーバのリスト

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

atl 46		3:36 PM	100%
<		Nuclias Connect	
		nucli	as connect
-		61.216.1	55.111:30001
	test		
			٩
		Lonin	
		cogin	

図 2-44 ログイン画面

8. ログイン認証が完了すると、ダッシュボードが表示されます。Nuclias Connect ダッシュボードには、現在定義されているサイト、ネットワーク、 アクセスポイント、クライアントが表示されます。



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

スタンドアロンアクセスポイントの検出と設定

■ DAPの検出

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

1. 「Standalone Access Point」をタップします。



図 2-46 Nuclias Connect アプリ - トップ画面

- 2. L2 フィールドのボタンをタップして、L2 ネットワークで検出を有効にします。また、L3 フィールドのボタンをタップして、L2 ネットワーク で検出を有効にします。
- 3. 次に、「From」および「To」フィールドに IP 範囲を入力します。追加ボタン(⊕)をタップして、新しい IP 範囲エントリを作成します。削除 ボタン (━)をタップして、定義済みの範囲エントリを削除します。

	₫ 4G	9:3	89 AM		0 63%		
<		Discover A	ccess	Point			
Discove vireless	r stand netwo	alone Access f rks	Points in	L2/L3			
.2)	
.3)	
> Fro	m	192.168.1.50	to	192.168.1.2	00	•	
		+ Add ar	n IP Ra	inge			
	1	Dis	cover				
	?	Dis	cover				

- 4. 検出範囲を定義した後、「Discover」をタップして検出プロセスを開始します。または、ページの下部にある「Configure Access Point Profiles」をタッ プして、ローカルプロファイルを追加または削除します。詳細は「プロファイル設定(p.52)」を参照してください。
- 5. ネットワーク範囲のスキャンが終了すると、検出されたアクセスポイントが一覧表示されます。

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



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



図 2-49 アクセスポイントへのログイン

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

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

「IP Info」タブには以下の項目が表示されます。


図 2-50 IP 情報の設定

「Wireless」タブには以下の項目が表示されます。

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

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

1 🗢	4:27 PM	99%
Cancel	DAP-2680	
IP Info	Wireless	Client
SSID-1		
SSID Name		dlinkii
Security		Open System
SSID-2		0
SSID-3		0
Wireless Informatio	n	
Radio Band		2.4G × 5G
Radio 2.4G Mod	e Mixed 802.11n	, 802.11g and 8
Radio 5G Mode		Mixed 802.11ac
Country Code		United States
Copy & Save Config	uration	
Apply Configura	ition	
Save Configurat	ion	

図 2-51 ワイヤレス設定

ネットワークプロファイルの削除

プロファイルを削除するには、以下の手順を実行します。

1. 左上のメニューをタップします。



2. 「AP Provision Profile」を選択します。



- 図 2-53 Nuclias Connect アプリ メニュー項目
- 3. 対象のプロファイルを選択して削除します。



図 2-54 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、Nuclias Connect 管理インタフェースから、モニタ>アクセスポイントに移動します。ドロップダウンメニュー をクリックして、サイトと利用可能なネットワークを選択します。使用可能な AP 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。

「No.」、「アクション」、「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。

< nuclias	Default
ダッシュボード	T D B T B B T B B B B B B B B B B B B B
₩ . €=\$ *	教会方法 ローカル目プドレス キーワードを検索 10
 アクセスポイント ワイヤレスクライアント 	No ステータニ アクション ローカルIPアドレージ MACアドレス ° モデルタイプニ ネットワーク ° クライアニ 24Gチャネル ° 5Gチャネル1 ° 最終更新情報 °
× 🐹 ,	1 🕒 🖰 🕃 🖂 192.168.0.50 40.9bxcd.0c.64:d0 DAP-2480 Network1 0 11 112 2020.01.09.17:19:41
₽ <i>″</i> >	
50 VX74 >	

図 2-55 モニタ - 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すると、個別または複数の DAP 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>ファームウェアアップグレードの順に移動し、サイトとネットワークを選択して使用可能な DAP モデルを表示します。
- 2. 次の画面で、「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。
- 3. 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**:「開始時間」フィールドで「即時」を選択し、「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**:「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。

エデルタイルードウェアパージ	- V T V T T-	ムウェアパージョン	× 77-60-7774	7.5/= 1/
C/MB// 1/22// 2				
DAP-2680/2A1G				双击
開始時間	9165			

図 2-56 ファームウェア アップグレード

第3章 Nuclias Connet 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」

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。

	Nuclias connect
<u>kn</u>	Nuclias connect
<u><n< u=""></n<></u>	Nuclias connect Service Configurat
<u><n< u=""></n<></u>	Uninstall

図 3-1 Nuclias Connect アプリケーション

「Nuclias Connect」を選択すると、クライアントアプリケーションが開きます。

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、このアプリケーションは既定の Web ブラウザを開き、ローカルホストに接続します。ローカルホストは、コンピュータ自身の IP アド レスに接続するためのローカル接続方法です。

または、リモートコンピュータから、コントローラ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(Internet Explorer または Google Chrome 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。

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。必要に応じて、ログインユーザ名、パスワード、CAPTCHA 要件を入力します。 「ログイン」を選択して Nuclias Connect を入力します。

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。

< nuclias connect
ログインアカウント メールアドレス/ユーザ名
パスワード キャプチャを入力して 2 / 33 パスワードを忘れた場合
ログイン © 2019 D-Link Corporation 日本語 〜

図 3-2 Nuclias Connect へのログイン

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。
- 2. 「システム情報を設定し、「次へ」をクリックします。ウィザードを中止するには「終了」をクリックします。

💘 システム設定		×
デバイスアクセスアドレスもしくはポートを	変更する場合、Nuclias Connectコアサーバの再起動が必要となります。	
デバイスアクセスアドレス	その他 ~	
	192.168.0.60	
デバイスアクセスポート	8443	
国	Japan v	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸 🗸	
		次へ 終了

図 3-3 ウィザード-システム設定

3. 「ネットワークを追加」画面が表示されます。

Ҟ ネットワークを追加		
サイト	newSite v	
ネットワーク名	Networkı	
		戻る 次へ 終了

図 3-4 ネットワークを追加

- 4. 「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。
- 5. 「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「終了」をクリックします。

6. 「ネットワーク設定」画面が表示されます。ワイヤレス設定とデバイス設定を入力して、ネットワーク設定を定義します。「次へ」をクリックして次に進みます。前の画面に戻るには「戻る」をクリック、ウィザードを中止するには「終了」をクリックします。

ネットワーク設定		13
ワイヤレス設定		
SSID名	dlink	
セキュリティ	WPA>+→ >	
SSIDパスワード*	\$	
	── ゲストSSIDを追加(オブション)	
ゲストSSID名		
デバイス設定		
開	Japan 🗸	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸 🗸	
ユーザ名	admin	
バスワード**	\$	
		戻る 次~

7. 「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「終了」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)			
IP ~	192.168.1.150	- 192.168.1.200	
一つ選択 ~			+
			次~ 終了

図 3-6 ネットワーク設定を検出

注意 本画面の「レイヤ3(IP)」ディスカバリは、同一セグメント内の AP のみ検出することが可能です(L2 ディスカバリと同範囲)。異なるセ グメントに AP を配置する場合、以下のいずれかの方法でネットワークの割り当てを行ってください。ネットワークの割り当て後は、異な るセグメントの AP 管理が可能となります。

- ・ モバイルアプリのL3 ディスカバリを使用して AP を検出し、ネットワークを割り当てる
- 同一セグメントに AP を配置しネットワークを割り当てた後、本来の場所に設置する

8. 「AP を検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを一覧表示します。デバイスが検出された場合は、そのデバイスを選択して「適用」をクリックし、ネットワークプロファイルをインポートします。「管理」タブをクリックして、 定義済みのデバイスを選択し、このネットワークに追加することもできます。

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

図 3-7 AP を検出

注意 異なるセグメントの「管理」ステータスの AP については再検出されません。管理 / 非管理 AP のネットワークの移動や削除については、「デ バイス管理」を参照してください。

ユーザプロファイル

管理者のアカウント情報を設定します。

個人情報

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

🛃 ユーザブロファイル		×
レ レ な か よ 学 座 者 置 後 ま よ 、 、 、 、 、 、 、 、 、 、 、 、 、	個人情報 セキュリティ 情報 ユーザ名* admin 設置場所 二 龍話番号 二 説明 二	n
		1000 C

図 3-8 ユーザプロファイル - 個人情報

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。

。 ユーザブロファイル		>
\frown	個人情報 セキュリティ	
	バスワードを変更	
	>* スワー k**	
admin	新しいバスワード*	
システム管理者	パスワード確認*	
TANKA CANIMAG		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 3-9 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、接続されているすべてのアクセスポイントとワイヤレ スクライアントの情報の概要が表示されます。

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



図 4-1 ダッシュボード

第5章 モニタ

- 「アクセスポイント」
- 「ワイヤレスクライアント」

アクセスポイント

左側のパネルからモニタ>アクセスポイントをクリックすると、トラフィック使用量の時間毎の推移と各アクセスポイントのステータスが表示され ます。この画面では、アプリケーションによって管理されているすべての接続されたアクセスポイントのレポートを表示できます。 また、「サイト」、「ネットワーク」などの検索条件を使用して、要件に沿ったレポートを生成できます。

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

< nuclias	⊟ Default									×	JI
ジ ダッシュポード											
₩ ₹=\$	全ての	サイト	~ 全ての)ネットワーク ∨	日本: 1/1 アク	7セスポイント					
• アクセスポイント	合計グ	ウンロード:0B	yte 合計 アップロ	a — F: o Byte							
• ワイヤレスクライア	MB						● ダウンロ	- F (MB) 🖪	アップロー	F (MB)	
🗙 設定	> 1										
「」 レポート	>										
- - - - - - - - - - - - - -	>										
20 VX74	× 0	8:00 19:00 00:0	00 21:00 22:00	23:00 00:00 01:00 02:	00 03:00 04:00 05:00	06:00 01:00 08	.00 09:00 10:00 U	.00 v2:00 v3:0	14:00 15:0	¹⁰ 16:00	5
						0					
	アクセン	ペポイント									
						検索方法	カルIPアドレスッ	キーワードな	検索	Q	
	No	ステータ.::	アクション	ローカルIPアドレ~	MACアドレス ~	モデルタイプ*	ネットワーク	× クライア.×	2.4Gチャン	*ル[]	
	1	•		192.168.0.50	40:9b:cd:0c:64:d0	DAP-2680	Network1	0	11		

図 5-1 モニタ - アクセスポイント

本画面には以下の項目が表示されます。

項目	説明
使用量	画面上部には、指定されたサイトおよびネットワークのダウンロード / アップロードトラフィック使用量が表示されます。
アクセスポイント	画面下部には、検出されたすべてのワイヤレスクライアントの一覧が表示されます。

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

◎をクリックして検索を開始します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

ワイヤレスクライアント

接続されたクライアント

左側のパネルからモニタ>ワイヤレスクライアントをクリックすると、「接続しているクライアント」画面が表示されます。この画面では、アプリケーションによって管理されているすべての接続されたクライアントのレポートを表示できます。

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

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



図 5-2 モニタ-ワイヤレスクライアント(接続されたクライアント)

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

■ レポート項目

このレポートには、このアプリケーションによって管理されるアクセスポイントに接続されているワイヤレスクライアント接続の一覧が表示されま す。クライアント毎に以下の情報を表示することが可能です。

- ・「ネットワーク」
- ・「IP アドレス」
- ・「IPv6アドレス」
- ・「MAC アドレス」
- 「認証タイプ」
- •「OS(キャプティブポータルクライアントでのみ使用可能)」
- ・「アップロード」
- ・「ダウンロード」
- ・「チャネル」
- $\lceil RSSI (dBm) \rfloor$
- 「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**をクリックすると、「接続しているクライアント」画面が表示されます。「ブロックされたクライ アント」タブをクリックします。この画面では、アプリケーションによって検出されたすべてのブロックされたクライアントのレポートを表示でき 「サイト」、「ネットワーク」の検索条件を使用して、要件に沿ったレポートを生成できます。

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

<nuclias< th=""><th>Default 🕘 🗙 JP 🗸</th></nuclias<>	Default 🕘 🗙 JP 🗸
ダッシュボード	接続しているクライアント プロックされたクライアント
🕎 E=9 🗸 🗸	合計 0 プロックされたクライアント 全てのサイト > 全てのサイト > (2)
 アクセスポイント ワイヤレスクライアン 	No アク ネットワーク × MACアドレス × 両波数等 × SSID × 認証タイプ ×
🗙 設定 >	
「「」 レポート >	
軍 ログ >	
50 vafa >	
	ブロックされたクライアントは存在しません。
	8
	1・20 of 0 トータルアイテム:0 《 く 1 /1 〉 》 20 v ページごとのアイテム

図 5-3 モニタ-ワイヤレスクライアント(ブロックされたクライアント)

「検索」フィールドで、ドロップダウンメニューをクリックし、サイトを選択してから、ネットワークを選択します。 🔯 をクリックして検索を開始 します。検索条件を満たす全ての関連デバイスが、レポートに表示されます。

■ レポート項目

このレポートには、ブロックされたワイヤレスクライアント接続の一覧が表示されます。レポートには以下の項目が表示されます。

- 「No.」
- ・「アクション」
- ・「ネットワーク」
- ・「MAC アドレス」
- ・「周波数帯」
- **SSID**
- ・「認証タイプ」

第6章 設定

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

プロファイルの作成

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

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

 ※ ダクシュポード ※ ホニタ 、 ** ひてフィムを作成 * プロファイル設定 * ブロファイル設定 * ファームりェブアップグ * SSL線明環 * 決済代行システム ※ レポート 、 								-	K JP 🗸
 ⇒ == 2 → ブロファイルを作成 → ブロファイル設定 → ブロファイル設定 ○ ブームショニアブッブグ > SSL証明時 - 決済代行システム □ レポート 、 	全てのサイト >	合計1ネットワーク 合計1/	コオンラインAP イ	合計 <mark>0</mark> クライア:	× F			ネットワー	クを追加
 ✓ RZ ✓ プロファイルを作成 ✓ プロファイル設定 ファームウェブアップグ SSL属明度 政府代行システム 区目 レモート → 	サイト名 🔺	ゞ ネットワーク名 ▲	✓ 合計デバイ	オンラインぶ	クライアン.::	プロファイ.::	検出	アクショ	×
 ・ プロファイルを伴成 ・ プロファイル設定 ・ ファームタェアアップダ ・ ジレード ・ 以前代行システム ・ レポート 、 	site1	Network1	1	1	0	60	Q	e î	
 プロファイル設定 フェームウェアアップグ SL証明書 決済代行システム レポート 、 									
えい レポート シ									
E 17 >									
50 vx74 >									
	1・15 of 1 トータルアイテ	·L:1		~	< 1	/1 > >	15 ~	ページごとの	アイテム

図 6-1 プロファイルを作成

「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。

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	
プロファイルの編集 🗹	サイトの詳細ページを開き、選択したサイトのセキュリティ、アクセスコントロール、ユーザ認証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Q	「検出ネットワーク設定」画面を開きます。この画面から、L2 プロトコル層に配置されているデバイス、または特定の
	IP アドレス / プレフィックスサブネット IP を検索できます。条件を定義したら、「次へ」をクリックします。「検出開始」
	をクリックして、デバイスを検出します(「設定可能」「管理」タブ)。
ネットワークを編集	「ネットワークを編集」面画を開きます。この画面から、ネットワーク設定を編集したり、新しいサイトまたは既存のサ
	イトに移行したりすることができます。
ネットワークを削除 💼	選択したネットワーク設定を削除します。

ネットワークの追加

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

サイト	newSite v	
ネットワーク名	Networkı	

図 6-2 ネットワークを追加

- 2. 「サイト」ドロップダウンメニューから既存のサイトを選択するか、新しいサイト (newSite) を選択し、空のフィールドにサイトの名前を入力 します。
- 3. 「ネットワーク名」フィールドに、新しいネットワークを識別する名前を入力します。「次へ」をクリックして続行するか、「終了」をクリック して前の画面に戻ります。
- **4.** 「ネットワーク設定」画面が表示されます。ワイヤレス設定とデバイス設定を入力して、ネットワーク設定を定義します。「次へ」をクリックして次に進みます。前のページに戻るには「戻る」をクリック、設定プロセスを中止するには「終了」をクリックします。

* ネットワーク設定		
ワイヤレス設定		
SSID名	dlink	
セキュリティ	WPA-自動-パーソナル ッ	
SSID>** 7 - F**	Ø	
	「 ゲストSSIDを追加(オプション)	
ゲストSSID名		
デバイス設定		
国	Japan v	
タイムゾーン	(GMT+09:00) Osaka, Sapporo, Tokyo 🗸	
ユーザ名	admin	
パスワード*	Ø	
		戻る次へ

図 6-3 ネットワークの設定

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

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

 V 	* 3 (IP)				
IP	v	192.168.1.150	- 192.168.1.200		
一つ選択				+	

図 6-4 ネットワーク設定を検出

- 注意 本画面の「レイヤ3(IP)」ディスカバリは、同一セグメント内の AP のみ検出することが可能です(L2 ディスカバリと同範囲)。異なるセ グメントに AP を配置する場合、以下のいずれかの方法でネットワークの割り当てを行ってください。ネットワークの割り当て後は、異な るセグメントの AP 管理が可能となります。
 - ・ モバイルアプリのL3 ディスカバリを使用して AP を検出し、ネットワークを割り当てる
 - 同一セグメントに AP を配置しネットワークを割り当てた後、本来の場所に設置する
- 6. 「AP を検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを一覧表示します。デバイスが検出さ れた場合は、そのデバイスを選択して「適用」をクリックし、ネットワークプロファイルをインポートします。「管理」タブをクリックして、 定義済みのデバイスを選択し、このネットワークに追加することもできます。

設定可	能管理					
	ステート 、	IPアドレス	MAC7 FUR ~	モデルタイプ:	NMS URL	ヾ ネットワーク
	スタンドアロ	192.168.0.50	40:9b:cd:0c:64:d0	DAP-2680	192.168.0.60:8443	
	٢				_	>

図 6-5 AP を検出



異なるセグメントの「管理」ステータスの AP については再検出されません。管理 / 非管理 AP のネットワークの移動や削除については、「デ バイス管理」を参照してください。

第6章 設定

プロファイル設定

プロファイル設定機能では、既存のネットワークを管理することができます。

- 1. 設定>プロファイル設定に移動して、既存のサイトを表示します。
- 2. サイトを選択し、次いで利用可能なネットワークを選択すると、編集可能なすべての設定が表示されます。
 - 「SSID」、「VLAN」、「帯域幅最適化」、「RF 最適化」、「スケジュール」、「デバイス設定」、「パフォーマンス」、「WLAN パーティション」、「ワイ ヤレスリソース」

<nuclias< th=""><th>Default</th><th></th><th>😍 💘 JP 🗸</th></nuclias<>	Default		😍 💘 JP 🗸
(デ) ダッシュボード	CP プロファイル	プロファイル > siter > Network:	
107 30 €=Ø >	site1		^
🗙 ike 🗸 🗸	③ Network1	設定をアップロード	
 プロファイルを作成 プロファイル設定 ファームウェデアップグレード SSL証明法 	SSID VLAN 帶城輛最適化 RF最適化	Indefinêndi Kanê ~	通用 クリア
• 決済代行システム	スケジュール	実行ステータス	
「」 レポート >	デバイス設定	 適用ステータス 0/1 	
回 ログ > 、 、 、 システム >	WLANパーティション ワイヤレスリソース	結果 実行時間 名前 IPアドレス MACアドレ	ス ~ モデルタイ…~ 結果 ~
		利用可能な結果はまだありませ	th.

図 6-6 プロファイル設定

■ 設定のアップロード

ネットワークを選択した後、本画面から設定のアップロード機能を利用できます。

サイトまたはネットワーク設定の更新を有効にするには、設定をアクセスポイントにアップロードする必要があります。 「設定をアップロード」セクションで、「開始時間」ドロップダウンメニューをクリックし、アクセスポイントに設定を更新する時間(「即時」または「時間を選択」)を選択します。「時間を選択」を選択した場合は、設定をアップロードする日時を設定します。「開始時間」を定義した後、「適用」をクリックしてアップロードを開始します。

「クリア」をクリックして、定義済みの設定を削除します。

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

■ ネットワークの各種ワイヤレス設定

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

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

SSID

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

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

<pre>snuclias connect</pre>	Default							3	C JP
$(\mathbf{k}) \mathcal{I} = \mathbf{r} = \mathbf{r}$	Ø 707712	プロファイル > site1 > 1	Vetwork1 > SSID						
140° += ≠ >	site1								
🗙 872 -	Ø Networki	インデックス・	/ 周波数号 - /	SSID	× セキュリティ	アクセスコントローエ	ユーザ認証・	アクション	
	SSID	プライマリ	2.4GHz	dlink	WPA-パーソナル	無効化	無効化	Z	
 プロファイルを作成 プロファイル設定 	VLAN	プライマリ	5GHz 1	dlink	WPA-パーソナル	無効化	無効化	C	
 ファームウェアアップダレード SSL証明書 	带城幅量適化 RF最適化	プライマリ	5GHz2 (トライパ	dlink	WPA-パーソナル	無効化	無効化	Ľ	
● 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								
E □ // >>	WLANパーティション ワイヤレスリソース								
Go ≥×₹4 →	site2	< セキュリティ							~
		アクセスコントロール							~
		ユーザ認証							~
		ホットスポット2.0							~
								ia <i>n</i> i / 2 9	7

図 6-7 プロファイル設定 - SSID

セキュリティ

プロファイル > site1 > Network1 > S	SID			
セキュリティ				
ワイヤレス設定				
周波数带	2.4GHz v	インデックス	SSID 1 \vee	
SSID *		文字コード	UTF-8 ~	
SSIDプロードキャスト	有効化 ~	WMM (Wi-Fiマルチメデ イブ)	有効化 🗸	
セキュリティ	オーブンシステム	~		
802.11 k/v/r	無効化 v こ です。	の機能は、互換性のあるモデルの特定のファームウ	ェアバージョンでのみ利	用可能
セキュリティ設定				
暗号化	無効化 ~	キーサイズ	64ビット v	
キータイプ	HEX ~			
卡一值				
	プロファイル > sites > Networks > S セキュリティ ワイヤレス設定 周波数帯 SSID・ SSIDプロードキャスト セキュリティ 802.11 k/v/r セキュリティ設定 暗号化 キータイプ キー値	プロファイル > sites > Networks > SSID	フロファイル> sites > Networks > SSID t + t + = y + i r + t + = y + i r + t + = y + i r + = y + i	フロファイル> sites > Networks > SSID $ \begin{array}{c} $

図 6-8 セキュリティ

「セキュリティ」セクションでは、以下の設定項目が表示されます。

項目	説明
周波数帯	ドロップダウンメニューをクリックして、無線周波数帯域を選択します。
	・ 選択肢:「2GHz」「5GHz 1」「5GHz 2(トライバンド)」
インデックス	ドロップダウンメニューをクリックして「SSID index」を選択します。新しい SSID を作成するには、最初に本項目を選
	択します。
	・ 選択肢:プライマリ、SSID1-SSID7

項目	説明
SSID	ワイヤレスネットワーク名を入力します。SSID はすべての周波数で同じである必要があります。また、選択した接続先のネットワーク名(SSID)が、Nuclias Connect で定義されているネットワーク名(SSID)と同じであることを確認してください。詳細については、アクセスポイント側のインタフェースで Basic Settings > Wireless Settings と Advanced
	Settings > DHCP Server > Dynamic Pool Settings を参照してください。「Domain Name」に Nuclias Connect で定義され たネットワーク名(SSID)が反映されるようにします。
文字コード	ドロップダウンメニューをクリックして、SSID エンコーディングで使用する文字コードを選択します。 ・ 選択肢:「UTF-8」「GB2312」 注意 現在の対応アクセスポイントでは UTF-8 はサポートされません。
SSID ブロードキャスト	ドロップダウンメニューをクリックして、ワイヤレス SSID の可視性を有効または無効にします。
WMM (Wi-Fi マルチメディア)	ドロップダウンメニューをクリックして、Wi-Fi マルチメディアを有効または無効にします。
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 or Open」 「WPA パーソナル」 「WPA エンタープライズ」(RADIUS サーバが必要) 「802.1X」
高速ローミング (802.11 k/v/r)	802.11 k/v/r 機能を有効または無効にします。 注意 DAP-2610、DAP-2680 は未サポートです。

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

■ 「セキュリティ」項目を「オープンシステム」に設定した場合

セキュリティ設定			
暗号化	有効化 ~	キーサイズ	64ビット v
キータイプ	HEX ~		
キー値*		ŝ	

図 6-9 セキュリティ(オープンシステム)

項目	説明
	セキュリティ設定
暗号化	ドロップダウンメニューをクリックして、WEP オープンシステムの暗号化を有効または無効にします。
キーサイズ	ドロップダウンメニューをクリックして、WEP キーのサイズを選択します。
	・ 選択肢:「64 ビット」「128 ビット」
キータイプ	ドロップダウンメニューをクリックして、WEP キーのタイプを選択します。
	・ 選択肢:「ASCII」「HEX」
キー値	オープンシステムの WEP 暗号化キーを入力します。

■ 「セキュリティ」項目を「WPA パーソナル」に設定した場合

WPA==− ド	Auto(WPA or WPA2) 🔍	暗号化タイプ	自動 🗸
パスフレーズ*	do	グループキー更新間隔	3600

図 6-10 プロファイル設定 - SSID (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:「Auto(WPA or WPA2)」「WPA2 or WPA3」「WPA2 only」「WPA3 Only」

項目	説明
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。「WPA2 or WPA3」または「WPA3 Only」モード
	の場合、「AES」のみ指定可能です。
	 選択肢:「自動」「AES」「TKIP」
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。

■ 「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

WPA=- F	Auto(WPA or WPA2) 🗸		
暗号化タイプ	自動	グループキー更新間隔	3600
ネットワークアクセス保護	無効化 🗸		
ライマリRADIUSサーバ制	定		
RADIUS #-/*		$\not \approx - \not *$	1812
RADIUSシークレット <mark>*</mark>	95		
ックアップRADIUSサーィ	《設定(オブション)		
RADIUS #-~		$\pi - 1$	1812
RADIUSシークレット	\$		
ライマリアカウンティング	ブサーバ設定		
ブカウンティング 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	Ś		
	/グサーバ設定(オブション)		
ックアップアカウンティン			
ックアップアカウンティン アカウンティングサーバ		アカウンティングポート	1813

図 6-11 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:「Auto(WPA or WPA2)」「WPA2 only」「WPA3 Only」			
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。「WPA3 Only」モードの場合、「AES」			
	のみ指定可能です。			
	・選択肢:「自動」「AES」「TKIP」			
グループキー更新間隔	WPA グループキーの更新間隔の値を入力します。			
ネットワークアクセス保護	ネットワークアクセス保護機能を有効または無効にします。			
プ	プライマリ RADIUS サーバ設定 / バックアップ RAIUS サーバ設定(オプション)			
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。			
ポート	RADIUS サーバのポート番号を入力します。			
RADIUS シークレット	RADIUS サーバのシークレットを入力します。			
プライマリアカウンティングサーバ設定 / バックアップアカウンティングサーバ設定(オプション)				
アカウンティングモード	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。			

■「セキュリティ」項目を「802.1X」に設定した場合

+一更新問題	300		
『ライマリRADIUSサーバ記	投定		
RADIUSサ−パ*			1812
RADIUSシークレット★	gø.		
ドックアップRADIUSサーィ	*設定(オブション)		
RADIUSサーバ		$4^{\ell}-7$	1812
RADIUSシークレット	Ś		
[°] 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 ~		
アカウンティングモード アカウンティングサーバ	無効化 >	アカウンティングポート	1813
アカウンティングモード アカウンティングサーバ アカウンティングシーク レット	無効化	アカウンティングポート	1813
アカウンティングモード アカウンティングサーバ アカウンティングシーク レット :ックアップアカウンティ	無効化 ~	アカウンティングポート	1813
アカウンティングモード アカウンティングサーバ アカウンティングシーク レット ドックアップアカウンティ アカウンティングサーバ	無効化 ~	アカウンティングポート アカウンティングポート	1813

図 6-12 セキュリティ (802.1X)

項目	説明
	セキュリティ設定
キー更新間隔	キーの更新間隔の値を入力します。
	プライマリ RADIUS サーバ設定 / バックアップ RAIUS サーバ設定(オプション)
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットパスフレーズを入力します。
プライマリ	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

L				
アクション	無効化 ~			
MACアドレス	XX:XX:XX:XX:XX	XX	追加	
MACアドレスリストをア ップロード	ブラウザ		ブップロード ダウンロード	
	2.4GHz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 🔺	~ 削除	
フィルタ設定		データが見つかりま	せんでした	
アデレス	無効L V	サブオ	171721	
			追加	a
	IPフィルタの最大エ: IPアドレス ▲	ントリ数は 64です。 ,残り 64 〜 サブネットマス	、ク ~ 削除	

図 6-13 アクセスコントロール

「アクセスコントロール」セクションでは、以下の設定項目が表示されます。

項目	説明
	ACL
アクション	ドロップダウンメニューをクリックして、クライアントに適用するアクションを選択します。
	・選択肢:「許可」「拒否」「無効化」
MACアドレス	アクセスを許可または拒否するクライアントの MAC アドレスを入力し、「追加」をクリックします。
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、「追加」をクリックします。

第6章 設定

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

図 6-14 ユーザ認証

「ユーザ認証」セクションでは、以下の設定項目が表示されます。

項目	説明
認証タイプ	ドロップダウンメニューをクリックして、ワイヤレスクライアントに適用する認証タイプを選択します。
	・ 選択肢:「無効化」「Web リダイレクトのみ」「ユーザ名/パスワード」「リモート RADIUS」「LDAP」「POP3」「パスコー
	ド」「外部キャプティブボータル」「MAC アドレス」「SLA ログイン」
	注意 SLA ログインは DAP-2610、DAP-2680 では未サポートです。
アイドルタイムアウト	セッションタイムアウト値を入力します。
(2~1440)	
	ホワイトリストを有効化(認証タイプが「Web リダイレクトのみ」以外の場合)
ホワイトリストを有効	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。この機能は、「認証タイプ」が「Web リダイレクトのみ」
化	以外の場合に使用できます。
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 アドレスを人力し、「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。
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 インタフェース設定
IRIF ステータス	ドロップダウンメニューをクリックして、IP インタフェースの使用を有効または無効にします。
VLAN グループ	VLAN グループ名を入力します。
IP アドレスの取得	IP インタフェースの IP アドレス取得方法を選択します。
	・ 選択肢:「スタティック IP アドレス(手動)」「ダイナミック IP アドレス(DHCP)」
IPアドレス	IP インタフェースの IP アドレスを入力します。
サブネットマスク	IP インタフェースのサブネットマスクを入力します。
ゲートウェイ	IP インタフェースのゲートウェイを入力します。
DNS	IP インタフェースの優先 DNS アドレスを入力します。
	ユーザ名 / パスワード(認証タイプが「ユーザ名 / パスワード」の場合)
ユーザ名	ユーザ名を入力します。
パスワード	パスワードを入力し、「追加」をクリックします。入力値をリセットする場合は「Clear」をクリックします。
ユーザー名/パスワード	「ブラウザ …」をクリックして、ローカルコンピュータに保存されたユーザ名 / パスワードリストのファイルを選択します。
ファイルをアップロー	「アップロード」をクリックしてユーザリストを更新します。現在のユーザリストをダウンロードするには、「ダウンロー
1	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。

項目	説明
リモート RADIUS タイ	RADIUS サーバのタイプを選択します。(認証タイプで「リモート RADIUS」を選択した場合のみ)
プ	・ 選択肢:「SPAP」「MS-CHAPv2」
	LDAP(「認証タイプが「LDAP」の場合
サーバ	LDAP サーバの IP アドレスを入力します。
ポート	LDAP サーバのポート番号を入力します。
認証モード	ドロップダウンメニューをクリックして、認証モードを選択します。
	・ 選択肢:「シンプル」「TLS」
ユーザー名	LDAP データベースにアクセスして検索できる管理者のユーザ名を入力します。
パスワード	LDAP データベースにアクセスして検索できる管理者のパスワードを入力します。
ベース DN	LDAP データベースのベースドメイン名を入力します。
アカウント属性	アカウントの属性を入力します。
識別子	管理者の名前を入力します。「自動コピー」にチェックを入れると、入力済みの他のパラメータの値が反映されます。
	POP3(認証タイプが「POP3」の場合)
サーバ	POP3 サーバの IP アドレスを入力します。
ポート	POP3 サーバのポート番号を入力します。
接続タイプ	ドロップダウンメニューをクリックして、接続タイプを選択します。
	・ 選択肢:「なし」「SSL/TLS」
	パスコードリスト(認証タイプが「パスコード」の場合)
パスコードリスト	このネットワークに割り当てられ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」を選択します。選択後、ホームページの URL を入力します。
	Web リダイレクション(認証タイプが「MAC アドレス」以外の場合)
Web リダイレクション	チェックを入れると、Web サイトのリダイレクト機能が有効になります。
Web サイト	ドロップダウンメニューから「HTTP」または「HTTPS」を選択します。選択後、ホームページの URL を入力します。
スプラッシュページ	カスタマイズ(「認証タイプが「Web リダイレクトのみ」「外部キャプティブポータル」「MAC アドレス」以外の場合)
テンプレートの選択	ドロップダウンメニューをクリックして、使用するログインスタイルを選択します。
	・「プレビュー」をクリックして、選択したスタイルをプレビューします。
	・「ログインファイルをアップロード」をクリックして、新しいスタイルをアップロードします。
	・ 屁をクリックすると、選択したスタイルが削除されます。
	 ・ ・ 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。

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。

ホッ	トスポッ	ト
----	------	---

ホットスポット2.0		^
ホットスポット		
ホットスポット2.0	無約化 ~	
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	無効化 ~	
L2TIF	無効化 ~	
インターワーキング		
インターワーキング	無効化 ~	
アクセスネットワークタ イプ	プライベートネットワーク ~	
インターネット	無効化 ~	
ASRA	無効化 ~	
ESR	無効化 ~	
USEA	無効化 ~	

図 6-15 ホットスポット 2.0

「ホットスポット 2.0」セクションでは、以下の設定項目が表示されます。

説明	
ホットスポット	
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。	
ドロップダウンメニューをクリックして、OSEN(OSU Server-Only Authenticated L2 Encryption Network)を有効または	
無効にします。	
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。	
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。	
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。	
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。	
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	
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のタイプを選択します。	
・ 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」	
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。	
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。	
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 グループの値を入力します。	
Venue タイプの値を入力します。	
言語を選択し、Venue 名を入力します。	
Homogenous Extended Service Set (ESS) ID を入力します。サービスプロバイダネットワークを識別するために使用され	
ます。	
WAN メトリック	
アクセスポイントの WAN リンクステータスを選択します。	
・ 選択肢:「リンクアップ」「リンクダウン」「テストステートでのリンク」	

項目	説明
WAN 対称リンク	WAN対称リンクのステータスを「はい」「いいえ」から選択します。「はい」の場合、アップロード / ダウンロードは同
	し、「「「「」」」「「」」」「「」」」」「「」」」」」」」」」」」」」」」」」
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バシティの上限 に達している場合、「はい」を選択します。
WAN メトリックダウン ロードスピード(kps)	WAN 接続のダウンロードスピードを kbps 単位で入力します。ダウンロードスピードが不明な場合は 0 を指定します。
WAN メトリックアップ	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。
UDVXE-F (Kps)	
	リスト
ネットワーク認証タイ プ	接続ダイフを選択します。 ・ 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 リダイレクション」「DNS リダイレクション」 「http/https リダイレクション」「DNS リダイレクション」の場合は、URL を入力する必要があります。
利用可能な IP アドレス	利用可能な IP アドレスタイプを選択します。ネットワークへの認証後、 ホットスポットのオペレータやモバイルデバイ
タイプ	スによってこのアドレスタイプが使用されます。
	• 選択肢:「アドレスタイプは利用できません。」「利用可能なグローバル IP アドレス」「利用可能なポート制限された
	IPv4 アドレス」「利用可能なシングル NAT されたプライベート IPv4 アドレス」「利用可能なダブル NAT されたプライ
	ベート 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	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
74	る際に、それらのセキュリティ認証が使用されます。6 桁または 10 桁の 16 進数が入力可能です。
	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、 🗖 をクリックします。
EAP 方式	EAP 方式を入力します。
	・ 設定可能範囲: 0-4294967295
	- 🛨 をクリックして、認証 ID (0-255) とパラメータタイプ (0-4294967295) を入力します。入力値を削除する場合は、
	<mark>-</mark> をクリックします。
	「追加」クリックして、EAP 方式のエントリを追加します。
RFC 4282	RFC 4282 への準拠を「はい」「いいえ」から選択します。「追加」をクリックして、上記 NAI レルムの入力情報とともに
	エントリとして追加します。
	3GPP セルラーネットワーク
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
	 設定可能範囲:00-999
	接続機能
	IP フ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	ステータスを選択します。
	・ 選択肢:「クローズ」「オープン」「不明」
オペレータフレンド	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。
リー名	
	OSU (Onlin Sign-Up)
OSU SSID	OSU SSID を入力します。
USU サーバ URI	USU サーハ URI を人力します。
	OSU 方式リスト
OSU 方式	言語を選択し、OSU 方式を入力します。
OSU コンフィグ	OSU コンフィグ選択します。
	・
	USU 言語コードを選択しより。
しい ノレンドリー名	言語を選択し、USU ノレンドリー名を入刀します。
USU Nai	USU NAI を入力します。
USU サービス説明	USU サービス説明を人力します。

項目	説明
OSU アイコン言語コー	OSU アイコン言語コードを選択します。
۴	
OSUアイコンファイル	OSU アイコンのファイルパスを入力します。
パス	
OSU アイコンファイル	OSU アイコンのファイル名を入力します。
名	
OSU アイコン幅	OSU アイコンの幅の値を入力します。
	・ 指定可能範囲:0-256(px)
OSU アイコン高さ	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 SSID を追加する場合は、各セクションのパラメータを定義後に「追加」をクリックします。

■ 既存ルールの変更

ルールを変更する場合は、対象 SSID の 「をクリックします。設定完了後、「保存」をクリックしてルールを保存します。 ルールを削除する場合は、対象ルールの 「をクリックします。 設定を中断する場合は、「キャンセル」をクリックします。 入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

注意 設定が更新されたら、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.52)」 を参照してください。

VLAN

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

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

VLAN リスト

「VLAN リスト」タブを選	択すると、以下の設定項目が表示されます。
項目	説明
VLAN ステータス	ドロップダウンメニューをクリックして、VLAN を有効または無効にします。

「保存」をクリックして値を保存し、画面を更新します。「VLAN リスト」タブには、作成されたすべての VLAN のリストが表示されます。 🗹 をクリックして、既存の VLAN を変更します。

■をクリックして、既存の VLAN を削除します。

Q プロファイル ittai SSID VLAN 帯域磁道途化 R2環境化 スケジュール	ブロファイル > sib VLANステ ータス VLANリスト VLANリスト	81 > Network1 : 有効化 ポートリスト	 VLAN VLAN				
■ Network1 ■ Network1 SSID VLAN 帯域酸量迫化 IP 環境化 スケジュール	VLAN X 7 - 2 X VLAN Y X 1 VLAN VID **	有効化 ポートリスト	→ 「泉存 vr an sign/55年 print				
Network1 SSID VLAN 序場幅圧適化 RF最適化 スケジュール	VLAN X 7 - 9 X VLAN Y X F VLAN VID *	有効化	✓ 傑存 VI AN ≉ ight/运業 _ PUIT				
 SID VLAN 帯域幅差迫化 RF最適化 スケジュール 	VLAN X 7 - 2 X VLAN Y X F	有効化	✓ 保存 VII ANI+>治的/运業 PUT				
SSID VLAN 帯城幅遅迫化 RF環迫化 スケジュール	VLAN 7 Z F	*	ττι δhīse inchni/a≣nami pitrītī				
VLAN 帯城幅最適化 RF最適化 スケジュール	VLAN V Z F	*	WIANI会通知/編集 PWIT				
帝東幅載過化 RF最適化 スケジュール			X ANA A.A.M. OR COMP. AND 2002 A. R. B.A.)設定			
TO ADD AND CONSTRUCTION		VLAN名 ~	タグVLANボート	÷	アンタグVLANボート	アクシ	a
デバイス設定	1	default	LAN3		SSID7 (5G 2), SSID6 (5G 2), SSID5 (5G 2), S	. 21	D
パフォーマンス							
WLANパーティン ワイヤレスリソース							
site2							
	1-15 of 1 ト-	タルアイテム:1			1 /1 >> >> 15 v	ージごとの`	アイテム
		1-15 of 1 -	1-15of1 \->>ルアイテム、1	1-15 of 1 下一交ルアイテム: 1	1-15of1 h=9.1747L:1	1-15of1 h-2127/71/21	$1-15 \text{ of } 1 + -9 \text{ JV7} 4 \neq L, 1$ (((1 /1))) $15 \text{ v} + -9 \text{ d} \geq 0,$

図 6-16 プロファイル設定 - VLAN

ポートリスト

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

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。



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.52)」を参照してください。

帯域幅の最適化

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

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

<nuclias< th=""><th>Default</th><th></th><th>JE</th></nuclias<>	Default		JE
ダッシュボード	C プロファイル	プロファイル > site1 > Network1 > 帯域(NULLEZE IC
100 E=2 >	site1		
X 2012	③ Networkı	帯域幅最適化を有効化	無効化 ~
• プロファイルを作成	SSID	ダウンリンク 帯域幅	80 Mbps
 プロファイル設定 ファームウェアアップグ 	带城艇最適化	アップリンク 帯域幅	80 Mbps
レート SSL証明書	RF最適化 スケジュール	想縁転長率化ルールを追加	
 決許代行システム レポート > 	デバイス設定 パフォーマンス	☆ 2000年1月1日 1日 1	各クライアントの平均等域編を到り当て >
<u>朝</u> ログ >	WLANバーティション ワイヤレスリソース	周波数带	2.4GHz ×
· AFRY Or		SSIDインデックス	77379
		ダウンリンク スピード	80 Mbps ~
		アップリンク スピード	80 Mbps ~
			80 237
		周波数~ SSID 🔺 ~ タイプ	ダウンリンクスピーエ アップリンクスピーエ アクション
			データが見つかりませんでした

図 6-17 プロファイル設定 - 帯域幅設定

以下の設定項目が表示されます。

項目	説明
帯域幅最適化を有効化	ドロップダウンメニューをクリックして、帯域幅最適化機能を有効または無効にします。
ダウンリンク帯域幅	ネットワーク内のアクセスポイントのダウンリンク帯域幅の合計速度を入力します。
アップリンク帯域幅	ネットワーク内のアクセスポイントのアップリンク帯域幅の合計速度を入力します。
	帯域幅最適化ルールを追加
ルールタイプ	ドロップダウンメニューをクリックして、ルールタイプを選択します。
	・「各クライアントの平均帯域幅を割り当て」:ダウンリンク/アップリンクスピードの設定値を、各クライアントで平
	等にシェアします。
	・「この SSID に特定の帯域幅を割り当て」: すべてのクライアントで割り当てられた帯域幅を共有します。
	・「各クライアントの最大帯域幅を割り当て」:ダウンリンク/アップリンクスピードの設定値が、各クライアントの最
	大値となります。
	・「11a/b/g/n クライアントに異なる帯域幅を割り当て」:a/b/g/n のクライアントに異なる帯域幅を割り当てます。
	- 11b/g/n クライアント:10% / 20% / 70%
	- 11a/n クライアント:20% / 80%
周波数帯	ドロップダウンメニューをクリックして、ルールで使用される無線周波数帯域を選択します。
	 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、ルールで使用される SSID を選択します。
ダウンリンク スピード	各ステーションまたは指定された SSID のいずれかに割り当てるダウンリンク スピードを入力します。
アップリンク スピード	各ステーションまたは指定された SSID のいずれかに割り当てるアップリンク スピードを入力します。

■ 新規ルールの追加

新しくルールを追加する場合は、ルールの定義後に「追加」をクリックします。

■ 既存ルールの変更

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

「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。



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。

connect	Detault	
N ダッシュボード	C 70771A	プロファスルト> situs > Networks > RF放進化
₩ €=Ø >	site1	
🗙 1822	Network Network	RF 於週代
 プロファイルを作成 プロファイルを作成 プロファイル改定 ファームの マテムク・スアップダ SSL運用市 レポート ログ レポート ログ レステム 	SSID VLAN 潜域転送道化 アダジュール デルイス派遣 パフォーマンズ WLANパーティション フィオレスリフース	▲ 田田 6 ● 中田 □ 185+水和田 □ 1800/加田・

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

図 6-18 プロファイル設定 - RF 設定

以下の設定項目が表示されます。

項目	説明
調整周期	ドロップダウンメニューをクリックして、RF 周波数を調整する周期を 1 時間単位で設定します。
自動チャネル調整	ラジオボタンをクリックして、RF 干渉を回避するためにクライアントのチャネルを自動的に調整する機能を有効にしま
	す。
自動出力調整	「自動チャネル調整」が有効な場合に使用できます。ラジオボタンをクリックして、干渉が存在する場合にカバレッジを
	最適化するために AP 無線電力を自動的に調整する機能を有効にします。

「保存」をクリックして設定を保存します。



注意
設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.52)」を参照してください。

スケジュール

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

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

<nuclias connect</nuclias 	Default				×
ダッシュポード	C 70771N	プロファイル > site1 > Netv	vorku > スケジュール		
1 E-9	site1				
X ike 🗸 🗸	Networki Networki	ワイヤレススケジュ ール	無効化 ~		
 プロファイルを作成 プロファイル設定 	SSID VLAN	スケジュールルール	を追加		
 ファームウェアアップグ レード SSL証明書 	带域幅最適化 RF最適化	名前			
• 決済代行システム	スケジュール	127.37 A			
コレポート >	デバイス設定 パフォーマンス	SSID	dlink		
- ログ >	WLANバーディション	曜日	● 1週間中 ■ 曜日を選択		
20 2×74 >	9140299-2		日曜日 月曜日 火曜日 水曜日 木曜日 金曜日 土曜日		
		< ^{田子[四]}	 1日中 時間を選択 		
		開始時間	10:52 AM		
		終了時間	10:52 AM		
			夜間		
			ifi加 タリア		
		ステータヾ 名前 ▲	ヾ SSIDインデック…ヾ 日	× タイムフレーム × ワイヤレ× アクション	

図 6-19 プロファイル設定 - スケジュール

以下の設定項目が表示されます。

項目	説明
ワイヤレススケジュール	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、スケジュールのアクティブな日を設定します。
	・「1週間中」:1週間の全ての曜日でルールを有効にします。
	 ・「曜日を選択」:ルールを有効にする曜日を指定します。
時間	ラジオボタンをクリックして、スケジュールのアクティブ時間を選択します。
	・「1日中」:終日ルールを有効にします。
	 「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。

■ 新規ルールの追加

新しくルールを追加する場合は、ルールの定義後に「追加」をクリックします。

■ 既存ルールの変更

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

をクリックします。

「クリア」をクリックすると、設定が初期値に戻ります。



注意
設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.52)」を参照してください。

デバイス設定

「デバイス設定」画面では、このネットワーク内のアクセスポイントのログインおよびアクセシビリティ設定を表示および変更することができます。 本画面では、2.4GHz と 5GHz の両方の周波数帯域について、詳細なワイヤレス設定を行うことができます。

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

connect	Default		۵ 💌
🕥 ダッシュボード			
1 += x >	C 70774.0	プロファイル > site1 > Net	works テアイス設定
v ma 🗸	() Networki	管理者	
 プロファイルを作成 プロファイル後定 プロファイル後定 フロアイル後定 フレームウェアアップダ SSL原明液 レポート レポート ログ システム システム 	SSID VLAN 御城編載道化 耳塚道化 スケジュール デバイス度定 パフォーマンス WLANパーティション ワイヤレスリソース	ユーザ系 パスワード ヨンソール設定 コンソールプロトコ タイムアウト 自動時間設定 く	admin → 一 一 一 一 一 元 一 元 一 元 一 元 一 元 一 元 一 元 一
		NTPサーバ 国設定 国を選択	IFアドレス/Fメイン名 Japan ∨ 現期により、国政定が、未明、日本、期間またはイスラエルとして設定されているデルイスがグループ内にある場合、設定
		タイムゾーン	は20歳します。 (GAIT+05:00) Osaka, Sapporo, Tokyo テマータイムを有効化
		DST開始(24時 問)	$\begin{array}{c ccccccccccccccccccccccccccccccccccc$
		DST終了 (24時 問)	11 v o v in 11 v at o v i

図 6-20 プロファイル設定 - デバイス設定

以下の設定項目が表示されます。

項目	説明
	。 1993年1月1日(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1993年1月1日)(1
ユーザ名	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理ユーザ名を入力します。
パスワード	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理者パスワードを入力します。
	コンソール設定
有効化	チェックを入れると、コンソール機能が有効になります。
コンソールプロトコル	ラジオボタンをクリックして、ネットワーク内のすべてのアクセスポイントに適用されるコンソールプロトコルを
	選択します。
	・ 選択肢:「Telnet」「SSH」
タイムアウト	ドロップダウンメニューをクリックして、アクティブなコンソールセッションのタイムアウト値を選択します。
	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。
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
サマータイムを有効化	チェックボックスをオンにすると、サマータイム機能が有効になります。
DST 開始(24 時間)	ドロップダウンメニューをクリックして、サマータイム(DST)の開始日時を指定します。
DST 終了(24 時間)	ドロップダウンメニューをクリックして、サマータイム(DST)の終了日時を指定します。
DST オフセット(分)	ドロップダウンメニューをクリックして、DST オフセット(分)を選択します。
外部シスログサーバ	外部シスログサーバの IP アドレスまたはドメイン名を入力します。本機能は、キャプティブポータルログのみ対
(キャプティブポータルログ)	応しています。

「保存」をクリックして設定を保存します。



設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.52)」を参照してください。

注意

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

パフォーマンス設定

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

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

● グランボード ● ブロファイル ブロファイル ブロファイル ● ブロファイル ブロファイル ブロファイル ブロファイル ● Networks ● State ● State ● State ● ブロファイルを作成 ● SSID ● State ● State ● ブロファイルを作成 ● SSID ● Tetronks ● Tetronks ● ブロファイルを作成 ● SSID ● Tetronks ● ブロファイルを作成 ● SSID ● Tetronks ● ブロファイル 第フィート ● Tetronks ● ブロファイル 第フィート ● Solution Sol	
・ プロファイルを作成 ・ プロファイルを作成 ・ プロファイル確定 ・ プロファイル ・ プロファイル ・ プロー ・ ・ プロー ・ プロー ・ ・ ・	
・プロファイルを作成 ・プロファイルを作成 ・プロファイルを定 ・プロン ・プロ ・ ・ ・	
プロファイルを作成 SSID ワイヤレス オン レ プロファイル変定 VLAN ワイヤレスモード So2.10, So2.10 現在 マ プレーム・タンアファブグ 耐味細胞造化 ワイヤレスモード So2.10, So2.10 現在 マ SSL原明時 おりシュール アータレート Acto マ (以内代行ンステム デバイス設定 ビーコン同時(40-500) 100 100 ロレボート WLAN・イデイション DTHERE (40-50) 100	
アナームウェブアップダ レーデー 耐酸酸酸酸化 ワイヤレスモード 802.110, 80	
レート RF 脱迫化 SSLEIFI ガ ・ 決許代行システム スケジュール デバス 双定 レーコン 阿爾(40-500) 100 パフォーマンス WIAN (ティンコン WIAN (ティンコン	
・ 決許代行システム スケジュール ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	
$\frac{\pi}{2} + \frac{\pi}{2} + \frac{\pi}$	
71+レスリソース	
● システム ・ WMM (WLFIマルナメディア) 有効化 ∨	
د ACK # 1 & 7 % (2.4GHz, 48-200) 48 μه	
ショートGI 振动化 ~	
IGMPススーピング 類効化 ~	
マルチキャストレート 類効化 ッ	
マルチキャスト帯技術コントロール 無効化 マ タザチネット 知ら用品数等にも適用されます	
最大マルナキャスト型規模 100 bps 安安モムト 別の国政策等にも適用されます。	
HT20/40共存 新幼化 ~	
DHCPOFFERをマルテキャストからユニキャ ストに変更 第第第化 く	

図 6-21 プロファイル設定 - パフォーマンス設定

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

項目	説明
ワイヤレス	ドロップダウンメニューをクリックして、ネットワークの無線帯域をオンまたはオフにします。
ワイヤレスモード	ドロップダウンメニューをクリックして、ネットワークで使用されるワイヤレスモードを選択します。
	・ 選択肢:(2.4GHz の場合)「802.11ax 混在」「802.11g、802.11b 混在」「802.11n のみ」
	(5GHz 1/5GHz 2 の場合)「802.11n、802.11a 混在」「802.11a のみ」「802.11n のみ」「802.11ax 混在」
データレート	ドロップダウンメニューをクリックして、無線のデータレートを選択します。この機能は、ワイヤレスモードが「802.11g、
	802.11b 混在」(2.4GHz)または「802.11a のみ」(5GHz 1/5GHz 2)の場合にのみ使用できます。
ビーコン間隔	ビーコン間隔の値を入力します。
	 初期値:100
DTIM 間隔	DTIM intterval 値を入力します。
	 初期値:1
WMM(Wi-Fi マルチメ	ドロップダウンメニューをクリックして、Wi-Fi マルチメディア(WMM)機能を有効または無効にします。
<i>デ</i> ィア)	
ACK タイムアウト	ACK タイムアウト値を入力します。
	 初期値:48
ショート GI	ドロップダウンメニューをクリックして、ショート GI 機能を有効または無効にします。
IGMP スヌーピング	ドロップダウンメニューをクリックして、IGMP スヌーピング機能を有効または無効にします。
マルチキャストレート	ドロップダウンメニューをクリックして、マルチキャストレート値を選択します。
マルチキャスト帯域幅	ドロップダウンメニューをクリックして、マルチキャスト帯域コントロール機能を有効または無効にします。
コントロール	
最大マルチキャスト帯	マルチキャスト帯域幅の最大値を入力します。この機能は、「マルチキャスト帯域幅コントロール」が有効の場合にのみ
域幅	使用できます。
	 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。
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

項目	説明
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、802.11b 混在」「802.11a のみ」の場合)「20MHz」
	(「802.11an のみ」の場合)「20MHz」「自動 20MHz/40MHz」
	(「802.11ax 混在」の場合)「20MHz」「自動 20MHz/40MHz」「自動 20MHz/40MHz/80Mhz/160Mhz(5GHz 帯のみ)」

「保存」をクリックして設定を保存します。

スパニングツリー

< nuclias	Default		٩	×	JP v
() ダッシュボード					
107 → モニタ >	site	クロクナイル > sitel > Networki > ハクホーマンス			
* 222 -	③ Network1	2.4GHz 5GHz 1 5GHz 2 (トライバンド) LAN			
 プロファイルを作成 プロファイル設定 フェーノウ・マアーブグ 	SSID VLAN 带域朝録適化	STP (スパニングラ サー) 一般物化 ッ 脱散のLANポートを行ったデクモスポイントにのみ、この説を追加できます。			
 ・ レード ・ SSL証明書 ・ 決済代行システム 	RF最適化 スケジュール			保存	
	アバイス成正				
5 a/ >	WLANパーティション ワイヤレスリソース				
40 2274 >					

図 6-22 プロファイル設定 - パフォーマンス設定(スパニングツリー)

「LAN」タブをクリックした場合、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

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.52)」を参照してください。

WLAN パーティション

「WLAN パーティション」画面には、ワイヤレスパーティション設定が表示されます。これにより、関連付けられたワイヤレスクライアント間の通 信を有効 / 無効にできます。本画面では、2.4GHz と 5GHz の両方の周波数帯域について、詳細なワイヤレス設定を行うことができます。

設定>プロファイル設定>サイト>ネットワーク>WLAN パーティションに移動し、「2.4GHz」「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。

snuclias	Default						٢	*	JP ~
 	CP ブロファイル site1	ブロファイル> sitei> D	letworkı≻ W	LANバーティン	εv				
🗙 82£ 🔹 🗸	Networks SSID	2.4GHz 5GHz i クライアント間通信	5GHz 2 ()	ライバンド)	リンタインテグリティ	有線LANから無線へのアクセス			
 ブロファイルを作成 ブロファイル設定 フェームウェアアッゴ 	VLAN 密域幅最適化	ブライマリSSID	• 有効化	○ 無効化) #21*-Y				
ゲレニジ ・ SSL証明書 ・ 決済代行システム	RF最適化 スケジェール	マルチSSID 2	● 有効化	○ 無効化) #21=- F				
園 レポート >	デバイス設定 パフォーマンス	*≁≠SSID3	 有幼化 高幼化 	○ 無効化	○ ゲストモード				
■ マグ > □ システム >	71+231/-7	<i>◆ル</i> ≁SSID 5	• 有幼化	○ 無効化	0 #21×-1				
		☆ルチSSID 6	 有幼化 有幼化 	○ 無効化) ゲストモード				
			1.01L					(R .7	-

図 6-23 プロファイル設定 - WLAN パーティション

以下の設定項目が表示されます。

項目	説明
	クライアント間通信
プライマリ SSID/ マル	ラジオボタンをクリックして、WLAN パーティションへの SSID のメンバーシップを有効または無効にします。この SSID
チ SSID1-7	がゲストとしてこの WLAN パーティションにアクセスできるようにするには、「ゲストモード」を選択します。
「但左」たんしいんして訂	

「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.52)」を参照してください。

リンクインテグリティ

	Default					٢	×	JP v
	C 707712	ブロファイル> site1> Ne	twork1> WLANパーティン	a ×				
× 20€ ×	sites 😚 Networks	2.40Hz 50Hz 1	5GHz₂ (トライバンド)	リンタインテグリティ	。 有線LANから無線へのアクセス			
 プロファイルを作成 プロファイル設定 	SSID VLAN	リンクインテグリ ティ	無効化 🗸					
 ファームウェアアップ グレード SSL証明書 決済代行システム 	密域編最通化 RF最通化 スケジュール						保存	
園 レポート シ	アバイス設定							
बि ए <i>७ ></i>	WLANパーティ ワイヤレスリソース							
50 VX74)		c						

図 6-24 プロファイル設定 - WLAN パーティション(リンクインテグリティ)

「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				
リンクインテグリティ	ドロップダウンメニューをクリックして、ワイヤレスリンクインテグリティ機能を有効または無効にします。			
祝友」をクリック」で設定を保存します。				

「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.52)」を参照してください。

有線 LAN から無線へのアクセス

< nuclias	Default					٢	*	JP ~
くnuclias Connect ダンシュボード デ デ ジ	Default ダ ブワフイル sites ● Network: SSID VLAN 市場着化 スタジュール デバイス設定 パフォーマンス WLANパーティ	ブロフフイル> sitei> Ne 2.40Hz 50Hz : 海部LANから知 着へのアクセス	twork1> WLANパーティン gGHz2(トライベンド) 有効化 ッ	a ン リンタインテグリナイ	有線LANから無線への下タセス		K QA	JP ~
副 マグ >> い ジステム >>	WLANパーティ ワイヤレスリソース く							

図 6-25 プロファイル設定 - WLAN パーティション(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」タブをクリックした場合、以下の設定項目が表示されます。

項目	説明		
有線 LAN から無線への	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。



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.52)」を参照してください。

ワイヤレスリソース

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

設定>プロファイル設定>サイト>ネットワーク>ワイヤレスリソースに移動し、「2.4GHz」「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></th><th>😍 🔀 JP -</th></nuclias<>	Default		😍 🔀 JP -
(*) ダッシュボード	O 70771N	プロファイル > siltat > Networks > ワイヤレスリソース	
107 E=3 >	site1		
🗙 1820	Networki	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	
 プロファイルを中場 プロファイルを用場 ファームク・エア・ブレッジ SSL展明 比決代行システム レポート ログ コンプクク システム 	SID VLAN 初始編組造産 耳F振道化 スケジュール・ ディイス改定 パフォーマンス WLANパーティション フィヤレスリソース	 ACL RSSIL \$ 5 い鉄 エージングアウト エージングアウト RSSIL \$ 5 い鉄 RSSIL \$ 5 い鉄 ロ 5% データレート 6 302 ps ケーダ取制限 (o-64) ローダ取制限 (o-64) エロ吸先 イ い酸花 ホットワーク使用率 100 % 	627

図 6-26 プロファイル設定 - ワイヤレスリソース

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

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

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.52)」を参照してください。
エアタイムフェアネス

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

注意 WiFi 通信速度が遅いデバイスは、物理的な距離が長い場合や、信号強度が弱い場合、古いレガシーハードウェアの場合などにより、速度 の低下が発生している可能性があります。このような場合、エアタイムフェアネス機能を使用することでネットワーク全体のパフォーマン スを向上させることが可能です。設定>プロファイル設定>サイト>ネットワーク>ワイヤレスリソースに移動します。「エアタイムフェ アネス」タブをクリックして、現在の設定を表示します。

connect	200mun				3	🗙 л	/P ~
ダッシュポード	O プロファイル	プロファイル > sitei > Networki > ワイヤレスリソース					
₩ * = <i>9</i> >	site1	2.4GHz 5GHz 1 5GHz 2 (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			
 ★ 花花 * ブロファイルを作成 * ブロファイル度定 * ブロファイル度定 * ブレームウェブアップグ * SSLEFUR * 法許代行システム * はポート 、 * レポート 、 	SSID VLAN 耐燥磁道道化 耳片道道化 スケジュール・ デバイス設定 パフォーマンス WLANパーティション ワイヤレスリソース	Tixent.			1	W//	

図 6-27 プロファイル設定 - エアタイムフェアネス

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

注意
設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロー ド (p.52)」を参照してください。

第6章 設定

バンドステアリング(5GHz 優先)

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

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

< nuclias	Default		٢	×	JP v
ダッシュボード	😲 70771N	$\mathcal{T} \square \ \mathcal{T} \uparrow A \Rightarrow$ alfti > Networki > $\mathcal{T} A \neq \nu \times \mathcal{T} \lor - \varkappa$			
== = = > >	site1				
🗙 ikie 🗸 🗸	Networki Networki	2.4GHz 5GHz1 5GHz2(トライバンド) エアタイムフェアネス パンドステブリング			
 プロファイルを作成 プロファイルなど(プロフィルス() フニュムタェアアップダ SSL#明洪 決済代行システム レポート レポート ログ システム 	SSID マムAF 環境組織通作。 不好通作 スケジュール・ パイス次定 パイス次定 パイスマンス WLAN・ナーライション ワイヤレスリソース	4		₿đ¢	

図 6-28 プロファイル設定 - バンドステアリング

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

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード(p.52)」を参照してください。

ファームウェアアップグレード

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

設定 > ファームウェアアップグし	ード>サイト>ネッ	トワークの順に移動します。
-------------------	-----------	---------------

<nuclias< th=""><th>Default</th><th></th><th>×</th><th>JP 、</th></nuclias<>	Default		×	JP 、
(★) ダッシュポード	19 77-LDxTTyJ/V	$-i7 \tau - L \sigma_{\pi} T T_{\tau} \tau' \tau' \nu - F > site > Network:$		
107 E=3 >	site1			^
X 202 -	Networki	各モデルのファームウェアファイルをアップロード		I
• プロファイルを作成		モデルる/ハードウェアパーヾ ファームウェアパージン ファームウェアファイル アクション		
• プロファイル設定		DAP-2680/2A1G 愛見		
 ファームウェアアップグ レード SSL証明書 決済代行システム 				
国 レポート >				
転 ログ >				
50 \$274 >				Ĩ
		auto o tanta a tan a tanta a t) T	
		実行ステータス		
		適用ステータス o/o		
				~

図 6-29 ファームウェアアップグレード

以下の設定項目が表示されます。

項目	説明
変更	「変更」ボタンをクリックして、アップロードするファームウェアファイルを選択します。ファイルはモデル固有です。
開始時間	ドロップダウンメニューをクリックして、アクセスポイントにファームウェアをアップロードする日時を指定、または
	即時にアップロードを行います。
	・「即時」:すぐにファームウェアをアップロードします。
	・「時間を選択」:ファームウェアをアップロードする日時を指定します。

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

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

適用ステータス	0/1					
結果	実行時間 ▼	> 名前	* IPアドレス	Υ ΜΑCアドレス	✓ モデルタイプ	∽ 結果 >
			利用可能な結果	はまだありません。		

図 6-30 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。証明書の設定を完了するには、 SSL 証明書機能で証明書ファイルをアップロードする必要があります。

設定 > SSL 証明書 > サイト > ネットワーク に移動します。

<nuclias< th=""><th>Default</th><th></th><th>JP</th></nuclias<>	Default		JP
() X > S = dl - F			
141 E-9 >	CP SSL能明语	SSL ₂ (<i>n</i>)(<i>n</i>) > sitter > Network:	2
10	sitei	SSL证明潜走更新	- 1
🗙 設定 🔪	Setworka		
• プロファイルを作成		ファイルから証明漫をアップロード ブラウザ	
• プロファイル設定			
・ ファームウェアアップグ レード		ファイルからキーをアップロード プラウザ	
• SSL证明書			
Demon VATA		$\tau_{yy} \tau_{0} - F$	
			•
1 = / · ·		実行ステータス	
2 2 X74 >		< 2017-2-27 - 2/2	
10			
		結果 実行時間 ▼	
		利田可能か结果はまだありません	
		15/15/16/3 州山木(ある) - 5/7 あ とん。	

図 6-31 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	「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。
アップロード	
ファイルからキーを	「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	

「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>×</th><th>JP v</th></nuclias<>	Default	×	JP v
(b) ダッシュポード			
<u> </u>	交抵政定		
🗙 202	Paypali≣ft* USD ∽		
 プロファイルを作成 プロファイル設定 ファームウェアアップグ 	Paypal $\mathcal{P} \mathcal{P} \mathcal{A} \mathcal{T} \times \mathbb{P} \mathbb{D}^4$		
レード • SSL証明書	Paypal $\gamma = \partial \nu \gamma + *$		
 決済代行システム 	オプション* 開間 0 分 ~ 頁川 0 -		
	期日>連択 > 黄川 +		
G 2274 >		保存	

図 6-32 決済代行システム

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

第7章 レポート

- 「ピークネットワークアクティビティ」
- 「時間別ネットワークアクティビティ」
- 「時間別ネットワークアクティビティ」
- 「日別ネットワークアクティビティ」

ピークネットワークアクティビティ

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

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

nuclias connect	Default 🚨 🔀
S ダッシュポード	
₹ = Ø >	ワイオレスネットワークのよく利用されている時間 一つ選択 v 一つ選択 v 段 2020/01/04-2020/01/10
(設定)	過去7日間で最もクライアントが利用している時間 🗹 しきい銃: 催来:25%
v#−+ •	後アクイアンド版
ビ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 ティビディ 日別ネットワークアクテ ィビティ 最もアクティブなAP	
ログ >	00:00 01:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 18:00 19:00 20:00 21:00 22:00 24:00
) >x74 >	
	道法7月間で最6利用量の多い時間 「とちい伯: 藤平:25%
	0000 0100 0200 0300 0400 0500 0500 0500 0500 0500 05

図 7-1 ピークネットワークアクティビティ

以下のレポートが表示されます。

- ・ 過去7日間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 > 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 7-2 時間単位のネットワークアクティビティ

以下のレポートが表示されます。

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

日別ネットワークアクティビティ

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

レポート > 日次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 7-3 日別ネットワークアクティビティ

以下のレポートが表示されます。

• 毎日のトラフィック使用量と接続クライアント数

最もアクティブな AP

特定のアクセスポイントのトラフィック使用量を表示します。

レポート > 最もアクティブな AP に移動して、レポートを表示します。

<nuclias connect</nuclias 	Default				🚨 💘 лр
() ダッシュボード					
	CP 最もアクティブな。	APのマップ+	過去7日間で最もアクティブなAP	接続クライアント数の平均/最高:0/0	トラフィック使用量の平均/最高: 0.00 MB/0.00 MB
120 e-x /	2Fマップ	C î	2Fマップ		
🗙 設定 🔹 👌			< 2020/01/10 v > < 15:45	~ > &	
↓ #++					
・ ビ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					
 ・ 日別ネットワークアクテ 			•	•	
• 最もアクティブなAP					
國 ログ >					
			100	100	
Ld SAFA			HOLES.		
				D-Link DAP-2680	
				192.168.0.50	
			E C		

図 7-4 最もアクティブな AP

最もアクティブな AP のレポートを表示するには、マップを選択後に日時を指定し、 🗟 をクリックしてレポートを表示します。レポートの生成後、 🗈 をクリックしてレポートを PDF ファイル形式で保存することができます。

以下のデータが画面右上に表示されます。

- ・ 過去7日間の接続クライアント数の平均/最高
- ・ 過去7日間のトライ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。

■ マップの編集

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

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

■ マップの追加

新しいマップを追加するには、 🕂 をクリックして「最もアクティブな AP のマップを作成」画面を開きます。 「最もアクティブな AP のマップ名」にマッ プ名を入力します。 画像(サポートされているファイル形式:PNG または JPG、最大 10MB)をドラッグ&ドロップするか、 ローカルフォルダを参 照してイメージを選択し、 マップをカスタマイズします。

第8章 ログ

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

SNMP トラップ

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

ログ > SNMP トラップに移動して、レポートを生成および表示します。

<nuclias< th=""><th>Default 🕘 🔀 JP 🗸</th></nuclias<>	Default 🕘 🔀 JP 🗸
(ii) ダッシュポード	サベマのSXMPバージョッ サベマの汎用タイプ ∨ 2020.1.3 値 2020/04/10 値 IP7ドレス ∨ オーワードを検索 🕃 💈
101 10 10 10 10 10 10 10 10 10 10 10 10	夢母は唇 × トラップは唇 ★ × 次前 × IPアドレス × SNMPパー× トラップタイプ × トラップ対応
🗙 設定 🕠	2020-01-09 17:42-37 2020-01-09 18:41:44 D-Link DA. 192 16:80 S0 V1 entermineSection Transform (Fr. Transform) 13:61:41:171:10:37:60:57:20:12"Bindine Variable:13:61
「」レポート >	2020 01 09 17:03:01 2020 01:09 180:208 D-Link DA 192.168.050 V1 enterpriseSpecific ["TinpOID: 1.3.4.1.4.1.171.10.37.60.5.7.2.0.7"Binding Variable: 1.3.4.1
🗟 = 1 🗸 🗸 🗸	2020-01-09 17:03:01 2020-01-09 18:02:08 D-Link DA 192.168:0.50 V1 enterpriseSpecific ["TrapOID: 13.6.1.4.1.171.10.37.60.5.7.2.0.7;"Binding Variable: 13.6.1
 SNMPトラップ 	2020-01-09 17:03:00 2020-01-09 18:02:07 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
・ シスログ	2020-01-09 17:02:55 2020-01-09 18:02:02 D-Link DA 192:168:0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7";Binding Variable:1.3.6.1
 システムイベントログ 	2020-01-09 17:02:50 2020-01-09 18:01:57 D-Link DA 192:168:0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;"Binding Variable: 1.3.6.1
 デバイスログ 	2020-01-09 17:02-26 2020-01-09 18:01:34 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
50 ×274 >	2020-01-09 16:52:02 2020-01-09 17:51:09 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;"Binding Variable: 1.3.6.1
	2020-01-09 16-52-01 2020-01-09 17-51-09 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7,"Binding Variable: 1.3.6.1
	2020-01-09 16-52-01 2020-01-09 17:51:08 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 1.3.6.1
	2020-01-09 16:51:56 2020-01-09 17:51:03 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID:1.3.6.1.4.1.171.10.37.60.5.7.2.0.7;"Binding Variable:1.3.6.1
	2020-01-09 16:51:51 2020-01-09 17:50:58 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7,"Binding Variable: 1.3.6.1
	2020-01-09 16:51:27 2020-01-09 17:50:34 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TapOID: 13.6.1.4.1.1711.0.37.60.5.7.2.0.13";Binding Variable: 13.6.1
	2020-01-09 16:51:25 2020-01-09 17:50:32 D-Link DA., 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 13.6.1.4.1.171.10.37.60.5.7.2.0.13";Binding Variable: 13.6.1
	2020-01-09 16:51:10 2020-01-09 17:50:17 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7",Binding Variable: 1.3.6.1
	2020-01-09 16:51:10 2020-01-09 17:50:17 D-Link DA 192.168.0.50 V1 enterpriseSpecific ["TrapOID: 1.3.6.1.4.1.171.10.37.60.5.7.2.0.7", Binding Variable: 1.3.6.1
	2020-01-09 16:51:06 2020-01-09 17:50:13 D-Link DA 192.168.0.50 V1 coldStart ["TrapOID: "Binding Variable:1.3.6.1.4.1.171.10.37.60.2.1.1.1.1.5=40.9 v
	1-500d25 K-9277752:25
<u></u>	

図 8-1 SNMP トラップ

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

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

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

シスログ

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

ログ>シスログに移動して、ログ情報を表示します。

<nuclias< th=""><th>Default 😨 yr</th><th>></th></nuclias<>	Default 😨 yr	>
(F) ダッシュポード	サベズのセベリティ v サベズのファシリティv 2020.1.3 舗 2020/01/10 舗 IPアドレス v キーワードを検察 図 2	
1000 €=Ø →	2×09 ++97+1%-9+09	
× 2022 >	受信時間 ◇ ログ時間 ◆ ◇ 名前 ◇ IPアドレス ◇ ファシリティ ◇ セベリティン ディレクティブ…> メッセージ	
	2020-01-09 17:03:01 2020-01-09 18:02:08 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 18:02:08 192.168.0.50 5G:initiate Wireless	
🔄 = 17 🔹 👻	2020-01-09 17:03:01 2020-01-09 18:02:08 D-Link DA 19:21:68:0.50 kernel messages Notice Jan 09 18:02:08 19:21:68:0.50 2:4G3/nitiate Wirele	
 SNMPトラップ 	2020-01-09 17:02:55 2020-01-09 18:02:02 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 18:02:02 192.168.0.50 5G:Initiate Wireless	
• 520%	2020-01-09 17:02:47 2020-01-09 18:01:54 D-Link DA 192:168:0.50 kernel messages Notice Jan 09 18:01:54 192:168:0.50 24:G.Initiate Wirele	
 システムイベントログ デバイスログ 	2020-01-09 16:52:02 2020-01-09 17:51:09 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 17:51:09 192.168.0.50 5G:Initiate Wireless	
24274	2020-01-09 16:52:01 2020-01-09 17:51:09 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 17:51:09 192.168.0.50 2.4G3.nitiate Wirele	
50 2000	2020-01-09 16:51:56 2020-01-09 17:51:03 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 17:51:03 192.168.0.50 5G:Initiate Wireless	
	2020-01-09 16:51:48 2020-01-09 17:50:55 D-Uink DA 192.168.0.50 kernel messages Notice Jan 09 17:50:55 192.168.0.50 2.4Ginitiate Wirele	
	2020-01-09 16:51:10 2020-01-09 17:50:17 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 17:50:17 192.168.0.50 5G:hinitate Wireless	
	2020-01-09 16:51:10 2020-01-09 17:50:17 D-Link DA 192.168.0.50 kernel messages Notice Jan 09 17:50:17 192.168.0.50 2.4G:initiate Wirele	
	2020-01-10 10:13:11 1970-01-01 09:20:09 D-Link DA 192.168.0.50 kernel messages Notice Jan 01 09:20:09 192.168.0.50 5GHz Wireless Cha	
	2020-01-10 09:55:39 1970-01-01 09:02:38 D-Link DA 192.168.0.50 kernel messages Notice Jan 01 09:02:38 192.168.0.50 5G/trittate Wireless	
	2020-01-10 09:55:39 1970-01-01 09:02:37 D-Link DA., 192.168.0.50 kernel messages Notice Jan 01 09:02:37 192.168.0.50 2.4Ginitiate Wirele.,	
	2020-01-10 09:55:33 1970-01-01 09:02:32 D-Link DA 192.168.0.50 kernel messages Notice Jan 01 09:02:32 192.168.0.50 5G/initiate Wireless	
	2020-01-10 09:55:25 1970-01-01 09:02:24 D-Link DA 192.168.0.50 kernel messages Notice Jan 01 09:02:24 192.168.0.50 2.4G:https://doi.org/10.1010/02:24 192.0010/02:24.0000/02:24.0000/02:24.0000/02:24.0000/02:24.00000000/02:24.0000/02	
	1-50d15 トータルアイテム:15 ペインゴン・クラントのアイテム	
J		

図 8-2 シスログ

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

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

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

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

システムイベントログ

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

ログ > システムイベントログに移動します。

Default									×	1.
	すべてのイベントタイプッ	2020.1.3	前 2020/01/10	m	IPプドレス	~	キーワードを検索	5	B	6
ログ時間 マニン・イベント	タイプ ^ ネットワーク	 IPアドレス 	MACTFUR	・ メッセージ						
			=0							
		データが見て	つかりません	でした						
	Detailt	Detault	Pr <c01< br=""> P<<c01< td=""> 2000.13 ログ時間 * * 1 * メットワーク * IPアFレス</c01<></c01<>	Default	すべくのイベンドタイブ 2020.43 値 2020/01/10 値 ログ時間・ > イベンドタイブ > ホットワーク > IPアドレス > MACアドレス、> メッセーク データが見つかりませんでした	T+<<01+>> F4 2000.13 2000/01/0 IPT F1/2 ログ時間・ ~ イベントタイブ ~ ホットワーク ~ IPT F1/2 ~ MACT F1/2 ~ メッセーク レブ時間・ ~ イベントタイブ ~ ホットワーク ~ IPT F1/2 ~ MACT F1/2 ~ メッセーク レデータが見つかりませんでした	アイベロイベンドタイブ 2020.13 2020/0/10 IPアドレス ログ時間・ ・ イベンドタイブ * ホットワーク > IPアドレス × メッセーク レプ時間・ ・ イベンドタイブ * ホットワーク > IPアドレス × メッセーク レプ時間・ ・ イベンドタイブ * ホットワーク > IPアドレス × メッセーク レークが見つかりませんでした データが見つかりませんでした	TricsO1422F847y 2020.13 図 2020/00/10 IDT Fレス 、 #-ワードやR: ログ時間・ 、 イインドタイブ 、 ホットワーク 、 IDT Fレス 、 MACT Fレス 、 メッセーク メータービッド メータービッド ビデータが見つかりませんでした	Pr4<	Pretauti Preta Preta

図 8-3 システムイベントログ

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

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

デバイスログ

「デバイスログ」機能を使用すると、管理者は AP の埋め込みメモリからのアラートメッセージを表示できます。システム・メッセージとネットワーク・メッセージには、タイム・スタンプとメッセージ・タイプが含まれます。ログ情報には、デバイス設定の同期、ファームウェアのアップグレード、設定のアップロード、クライアントのブロックなどが含まれます。

ログ > デバイスログに移動して、レポートを表示します。

< nuclias	Default						🔔 🗙 JP 🗸
(b) ダッシュポード		すべての動作タ	۲ ۶ – ۲	2020.1.3	m	2020/01/10	 iPプドレス v キーワードでを放客 ip i i
₩ €=\$ >	ログ時間 👻 🗸 🗸	名前	/ IPアドレス ^	MAC7~	操作種別	◇ 結果 ~	ログ詳細
* 設定 >	2020-01-10 11:15:36	D-Link DAP-2680	192.168.0.50	40:9b:cd	ファームウェア	Cancel	The firmware version is the same.
[] レポート →	2020-01-10 10:13:22	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 108
₫ ¤% ×	2020-01-10 09:55:52	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 116
 SNMPトラップ 	2020-01-10 09:55:42	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36
・ シスログ	2020-01-09 17:48:08	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 1, Channel. 5 GHz: 112
 システムイベントログ 	2020-01-09 17:47:38	D-Link DAP-2680	192.168.0.50	40:9b:cd	デバイス設定を	Success	Configuration Failed to create SSIDs for some of your APs because these AP
• 774,409	2020-01-09 17:47:08	D-Link DAP-2680	192.168.0.50	40:9b:cd	登録デバイス	Success	Network1
40 \$X74 >	2020-01-09 17:43:20	D-Link DAP-2680	192.168.0.50	40:9b:cd	デバイスを削除	Success	Network1
	2020-01-09 17:42:36	D-Link DAP-2680	192.168.0.50	40:9b:cd	非管理へ移動	Success	Network1
	2020-01-09 17:03:13	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 112
	2020-01-09 17:03:03	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36
	2020-01-09 16:52:12	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 136
	2020-01-09 16:52:02	D-Link DAP-2680	192.168.0.50	40:9b:cd	チャネルもしく		Channel. 2.4 GHz: 11, Channel. 5 GHz: 36
	2020-01-00 16-51-22	D.1 int DAD.2680	102 148 0 50	40-9h-ed	/ اعالفيد 4		Channal 24 Gbir 11 Channal 5 Gbir 126 🗸 🗸
	1 - 50 of 16 トータルア	イテム:16					《 (1 /1) 》 50 v ページごとのアイテム

図 8-4 デバイスログ

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

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

第9章 システム管理

- 「デバイス管理」
- 「ユーザ管理」
- 「設定」
- 「接続」

デバイス管理

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

システム > デバイス管理に移動します。

<nuclias< th=""><th>Default</th><th></th><th>🔮 📉 jp 🗸</th></nuclias<>	Default		🔮 📉 jp 🗸
(*) ダッシュボード	A >> > 7 - 7	住用 非位用	
■ <u> ま</u> - タ)	site1		非管理に移動
* 182 ,	③ Networki	□ ステータ> ローカルPアドレ_> NATIPアドレス > MACアドレス > モデルタイプ > ハードウェアパニ ファー	ムウェア※ 管理:
「」レポート 、		□ ● 192.168.0.50 192.168.0.50 #07#07#1#00 DAP-2680 2A1G v2.00	2020-01-0
<u>ت</u> ۲ ،			
50 2×74 ×			
• デバイス管理			
 ユーザ管理 			
 設定 		c	
 Nuclias Connectic ついて 			
		٤	>
		1-50 of 1 ト−タルアイテム: 1	」ページごとのアイテム

図 9-1 デバイス管理 - 管理デバイス

「管理」「非管理」タブを選択して、管理対象デバイスまたは非管理対象デバイスのリストを表示します。

■ 管理デバイスリスト / 非管理デバイスリストへの移動と削除

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

■ ネットワークの移動

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

■ 表示項目

デバイスのリストは、以下の基準によってソートすることができます。

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

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

ユーザ管理

ユーザステータス

ユーザステータス機能を使用すると、登録されているすべてのユーザプロファイルの現在のステータスを表示したり、プロファイルを編集したり、 削除したりすることができます。「ログインステータス」には、ユーザのログイン状態が表示されます。

 はユーザがログイン状態、
 はユーザがログオフしていることを示します。

システム>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。

< nucli	as ect		Default									JP 🗸
<u>(5)</u> 9 v	i> a.∦− F		すべてのユーザ	ユーザ合計1 (i i i o i o)							ユーザを追加
107 e =	3	>	ユーザステータス	ユーザ権限								_
🗙 設定		>	ユーザ名 🔺	~	メールアドレス	v	ログインステェ	後期 ~	権限ステータス ~	作成日時 ~	直近のログイン時間…^	アクショ
×۲ 🖫	- 1	>	admin				•	システム管	有动化	2020-05-22 16:35:56	2020-11-30 16:31:16	Ø
i 07		>										
G 27	£∓											
• 71.	イス管理											
• =	ザ管理											
• 設定 • Nucl	ias Connect	10711										
			1-10 of 1 トータル	アイテム:1						< <u>1</u> /1 >	» 10 v ≈−9	ごとのアイテム

図 9-2 ユーザ管理 - ユーザステータス

■ ユーザプロファイルの編集

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

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

使用可能なユーザプロファイルは以下の通りです。

- ・ システム管理者 (admin): これはオペレータアカウントであり、削除することはできません。
- ルート管理者:このサーバ上のすべてのサイト/ネットワークを管理できます。
- ローカル管理者:自分のネットワークを管理できます。
- ・ ルートユーザ:このサーバ上のすべてのサイト/ネットワークを表示できます。
- ローカルユーザ:自分のネットワークを表示できます。
- フロントデスクスタッフ:パスコードを生成および管理できます。

ユーザ権限

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

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

<nuclias< th=""><th>Default</th><th></th><th></th><th>🔮 💌 JP 🤅</th></nuclias<>	Default			🔮 💌 JP 🤅
ダッシュポード	すべてのユーザ ューザ合計	1 (🍰 1 🍰 0 🐇 0)		ユーザを追加
世界 王二夕 >>	ユーザステータス ユーザ権	Щ		
🗙 設定 🔹 ,	site1	Matthews and the	NW et al	
「 レポート 、	Network1	権限のないユーザ		
ログ >			admin (ルート町中石)	
			»	
 デバイス管理 			«	
 ユーザ管理 				
 設定 				
• Nuclias Connect (2004				

図 9-3 ユーザ管理 - ユーザ権限

■ ユーザの追加

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

■ ユーザの承認 / 承認解除

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

設定

一般

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

システム > 設定に移動して、システム情報を表示します。

<nuclias< th=""><th>Default</th><th>😍 🔀 JP 🛛</th></nuclias<>	Default	😍 🔀 JP 🛛
()) グッシュボード	- 「「「「「「」」」を発行す パックオップ DECT API シングルサインオン(SSC1)	
1111 → → →		
🗙 設定 🔹 👌	カスタマイズ最変	
↓ #-+ >	組織名 Default	
Ē ₽/ →	p d'	
50 ××74 ×	(f)	
• デバイス管理	ドラック&ドロップ ロゴフォイルをここへ ブラウザ	
 ユーザ管理 設定 	ロゴファイルはPNGもしくはJGP画像ファイル形式 である必要があります。	
• Nuclias Connecticou	ログインキャプチャ 有効化 、	
	# #	
	デバイス設定	
	III Japan 🗸	
	タイムゾーン (GMT+og:coo) Osaka, Sapporo, Tokyo い	
	クイブバケット開闢 1分 ∨	
	94 7	

図 9-4 システム - 一般

「カスタマイズ設定」セクションでは、以下の設定項目が表示されます。

項目	説明
組織名	組織名を入力します。
Ĕ	「ブラウザ」をクリックして、インタフェースロゴとして使用するファイルを選択します。ローカルファイルは、ファイルのパスを指定するか、ファイルをフレームにドラッグ&ドロップして選択できます。PNG または JPG 形式のファイルがサポートされます。
ログインキャプチャ	ドロップダウンメニューをクリックして、CAPTCHA 認証機能を有効または無効にします。

「保存」をクリックして設定を保存します。

「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
国	ドロップダウンメニューをクリックして、ネットワーク内の AP の国を選択します。
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
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」

接続

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

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

<nuclias< th=""><th></th><th>Default</th><th></th><th>🔫 🛛 JP</th></nuclias<>		Default		🔫 🛛 JP
()) ダッシュボード	e	一般 路梯 SMTP バック	デッチ RECTAPI シングルサインナン (CON)	
<u>111</u> € = 9	>			
🗙 設定	>	接続設定		
-*-+	>	デバイスアクセスアドレス	172.16.1.54 v	
a •7	>	デバイスアクセスボート	8443	
10 2774	~		ポートを変更するには、"C:\Frogram Files (x86)\Nuclias connect\Core\config\appconfig.json" ~移動し、必要に応じてポ 	
 デバイス管理 ユーザ管理 		コアサーバアクセスボート	8443	
• 設定 • Nuclias Connes て	etic 211	Webアクセスボート	30001 स्व	
		SSL証明書を更新		
		ファイルから証明書をアッ プロード	7207	
		ファイルからキーをアップ ロード	7944	
			發行	

図 9-5 システム - 接続

「接続設定」セクションでは、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

「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	「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。
アップロード	
ファイルからキーを	「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	

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。

、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。
----------------------	----------	------------------

💘 JP 🗸

図 9-6 システム - SMTP

以下の設定項目が表示されます。

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

バックアップ

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

システム > 設定に移動し、「バックアップ」タブをクリックしてバックアップ設定を表示します。

<nuclias connect</nuclias 	Default	JP -
₩ +=9 >		
🗙 設定 🔹 >	自動バックアップ混定	
<u>温</u> レポート >>	目動パックテップ 再効化 🗸	
i = / >	响和机构 7 日 12:00 V	
10 VXF4 ~	1.077077771.4 RE ×	
 デバイス管理 ユーザ管理 	ペックアップ・オス C\Program Files (x86)\Nuclias connect(web\Backu 気更	
 設定 	すべてのファイルを保存するのに十分なハードディスクサイズがあるかを確認してください。	
	パックアップ設定	
	 上書き(ハードディスクがいっぱいになったら古いログを上書き) 設定 すぐにパックアップ 課 	
	◎グ (底は90日). +くにく>クアップ ြ ြ	
	リストア設定	
	設定 ファイルを留税 リメープ	

図 9-7 システム - バックアップ

以下の設定項目が表示されます。

項目	説明
	自動バックアップ設定
自動バックアップ	自動バックアップを有効 / 無効にします。
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。
	バックアップ設定
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
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。

「保存」をクリックして設定を保存します。

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。

REST API

「REST API」タブでは、REST API の有効化 / 無効化を設定します。

システム>設定に移動し、「REST API」タブをクリックします。

< nuclias		Default	JP 🗸
ダッシュボート	F	- 絵 接接 SMTP バックテップ BEST APL シングルナインオン (SSO)	
111 9	>	10. Dige course in 53,5,3,5,5, course see to 5,5,5,7,1,5,9, (2000)	
🗙 設定	>	REST API	
	>	REST API 無効化 ~	
i • 7	>		
Lo XFA			
• デバイス管理			
 ユーザ管理 			
• 設定			
• Nuclias Conne て	actic つい		

図 9-8 システム - REST API

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します。
REST API キー	REST API キーが表示されます。
	FREST API キーをコピーします。

「キーを再生成」をクリックして REST API キーを再生成します。

シングルサインオン(SSO)

「シングルサインオン」タブでは、Nuclias アカウントを Nuclias Cloud および Nuclias Connect ポータルの両方でアクセス可能に設定することができ ます。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。



参照 アカウント登録手順は「アカウントの登録」を参照してください。

システム>設定に移動し、「シングルサインオン」タブをクリックします。

Inuclias connect	Default	٢	*	JP v
(b) ダッシュボード	一般 接続 SMTP バックテップ RESTAPI シングルサインオン (SSO)			
₩ <u>₩</u> €=9 >				
🗙 設定 >	シングルサインオン(SSO)では、1つのNucliasブカクントを使用して、NucliasクラクドボータルまたHNuclias Connectボータルにアクセスできょ	はすにアクセスでき	ます.	
<u>清</u> レポート >	このコンドローン・かけ自転よオンシオンの時代、シングがガイオオン(GOU)オンションは日朝町に一般がになることに注意していたさい。シンジルシ ヨンを有効にして、Nucliasアカウンドに開発ロジオンナる必要があります。	(1 2 1 2 (220)	122	
u مراجع الم	Nucliasシングルサインオンを 有効にする			
G ≫≭₹4 ×	Nucliasブカウント*			
 デバイス管理 ユーザ管理 	Nuclias/1×7−1* Estil 8~64℃1.			
 設定 	アカウントを作成			
・ Nuclias Connectについ て		通用		

図 9-9 システム - シングルサインオン (SSO)

以下の設定項目が表示されます。

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

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。

グッシュボード						
	×−9 ≥>:1.0.2.11 (14/Jan/2020 18:12:3914	hillionaic 297974	ベートされました。)	オンラ	イン更新
+=9 >					-	
設定 >	T72247	* 周波政府 > 1 /	* <u>N-FOIDN-212</u>	* 400		
v#−+ >	DAP-2230	92910 201811	A1, A2	Nuclias Connect Wireless N PoE Access Point		
2/2	DAP-2310	シングル	B1 B2	Nuclias Connect Wireless N POE Access Point		
M 9	DAP-2610	デュアル	A1	Nuclias Connect AC1300 Wave 2 Access Point		
<i>∨</i> ,774 ~	DAP-2620	デュアル	A1	Nuclias Connect AC1200 Wave 2 Wall Plate Access Point		
デバイス管理	DAP-2660	デュアル	A1, A2	Nuclias Connect AC1200 PoE Access Point		
設定	DAP-2662	デュアル	A1	Nuclias Connect AC1200 Wave 2 Access Point		
Nuclias Connectにつ て	DAP-2680	デュアル	A1	Nuclias Connect AC1750 Wave 2 Access Point		
	DAP-2682	デュアル	A1	Nuclias Connect AC2300 Wave 2 Access Point		
	DAP-2695	デュアル	A1, A2	Nuclias Connect AC1750 PoE Access Point		
	DAP-3315	シングル	A1	Wireless N Exterior Access Point		
	DAP-3666	デュアル	A1	Nuclias Connect AC1200 Wave 2 Outdoor Access Point		
	DAP-2695 DAP-3315 DAP-3666	デュアル シングル デュアル	A1, A2 A1 A1	Nuclias Connect AC1750 PoE Access Point Wireless N Exterior Access Point Nuclias Connect AC1200 Wave 2 Outdoor Access Point		

図 9-10 Nuclias Connect について

Nuclias Connect のバージョン情報の下には、サポートされるアクセスポイント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、アクセスポイントのリストを更新できます。新しくアクセスポイントのモデルがサポートされた場合は、リ

ストが更新されます。

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