nuclias connect

ユーザマニュアル

D-Link
Building Networks for People

はじめに

● 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

目次

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。

警告 警告では、設定の組み合わせ、イベントや手順によりネットワークの接続状態やセキュリティなどに悪影響を及ぼす恐れのある事項について説明します。

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

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

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。

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。

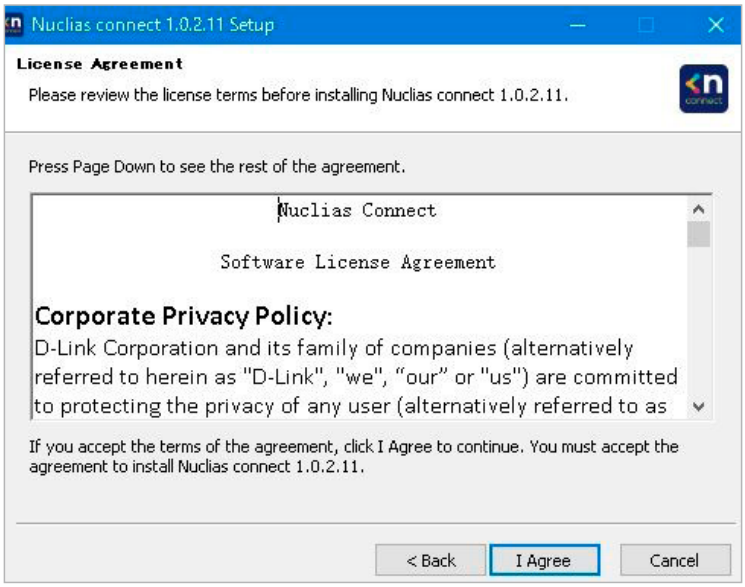

図 2-2　Nuclias Connect - 使用許諾

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。

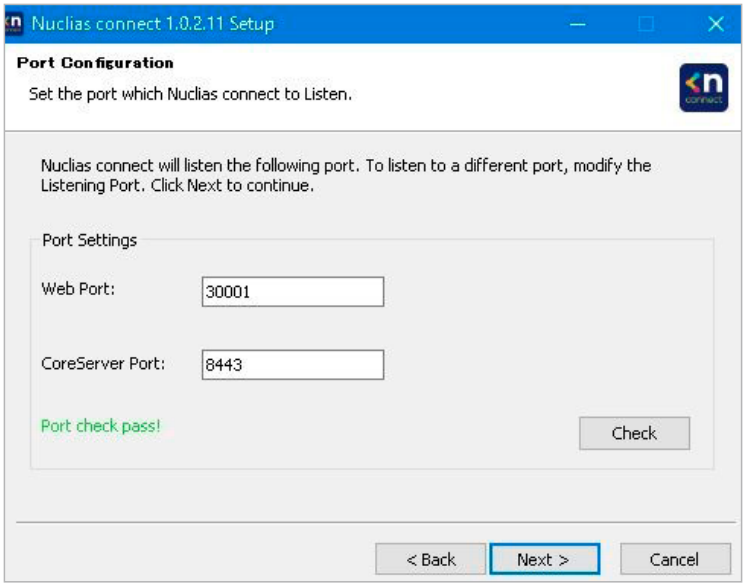

図 2-3　Nuclias Connect - ポート設定

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。

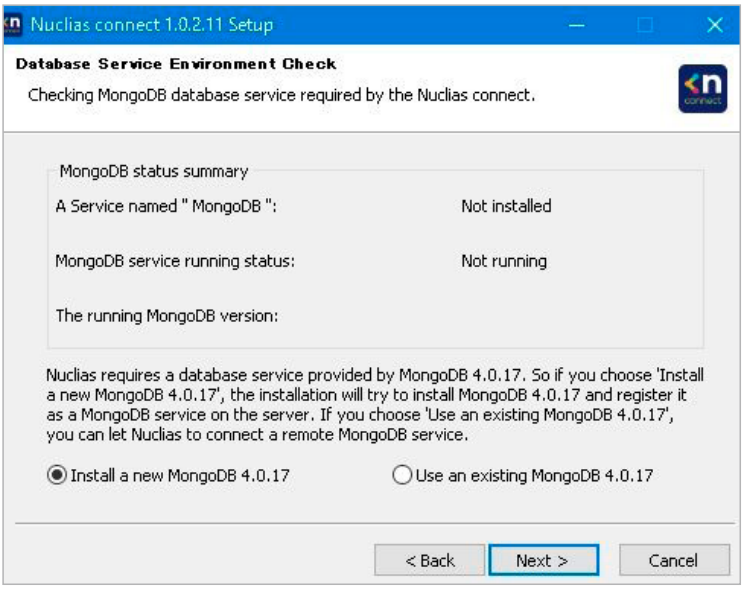

図 2-4　Nuclias Connect - MongoBD サービスステータスのチェック

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。

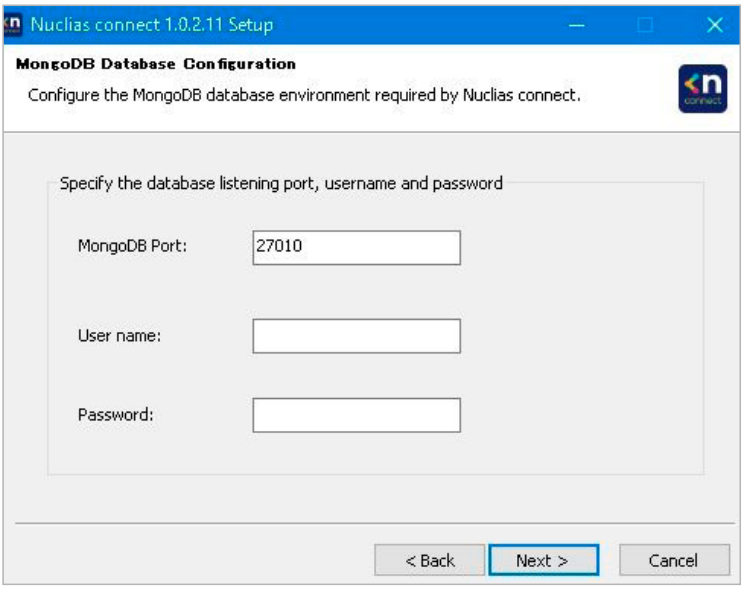

図 2-5　Nuclias Connect - MongoDB データベース設定

7. 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。

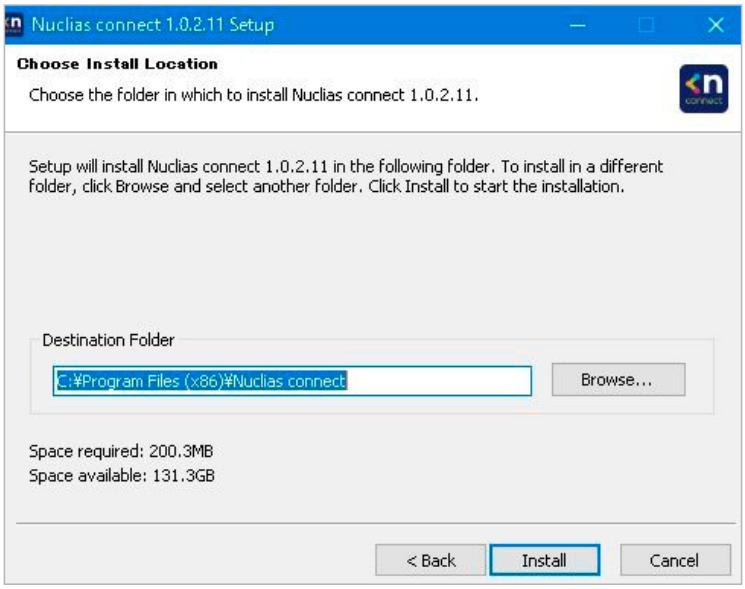

図 2-6　Nuclias Connect - インストールフォルダの指定およびインストールの開始

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。

10. 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。

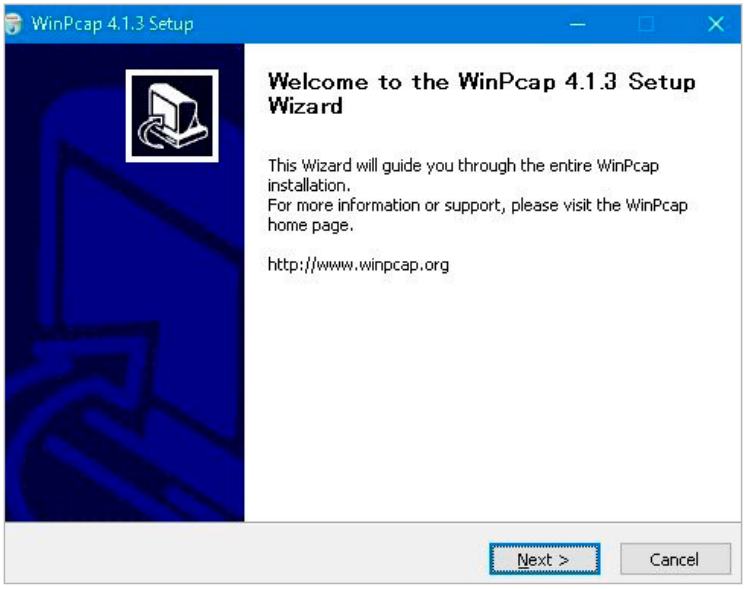

図 2-7　WinPcap - セットアップウィザード

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。

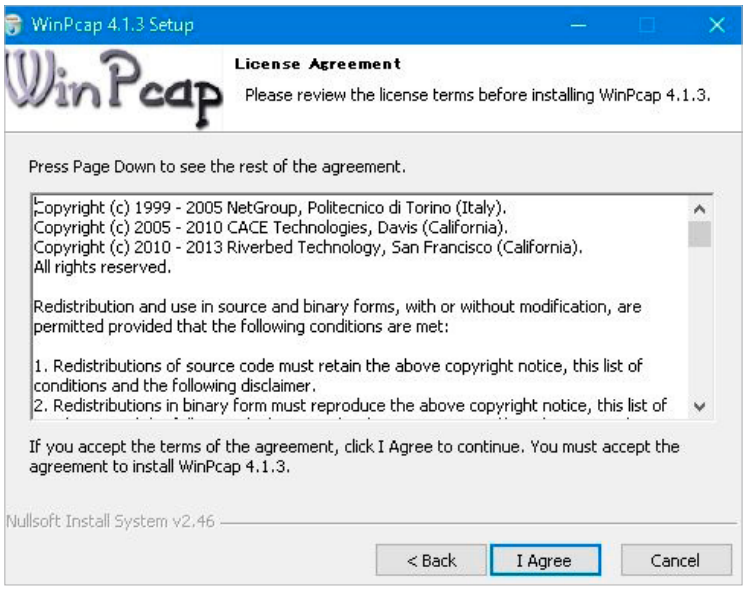

図 2-8　　WinPcap - 使用許諾

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。

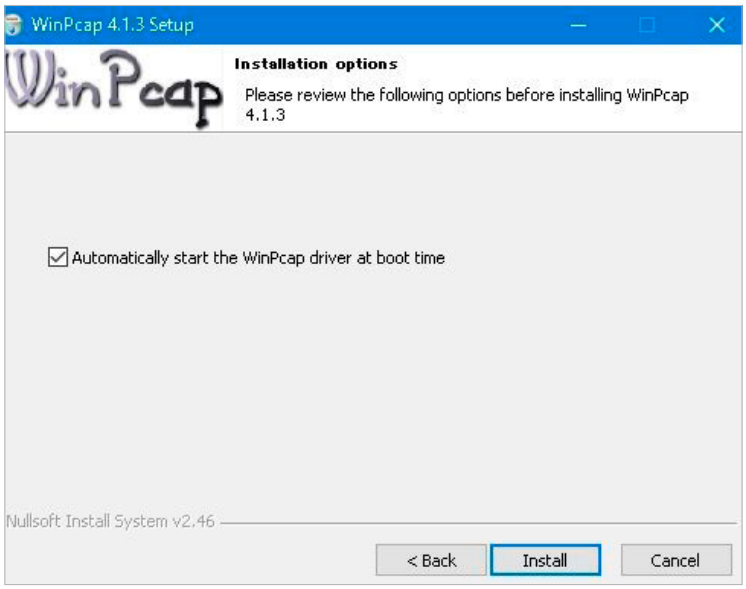

図 2-9　　WinPcap - インストール開始

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。

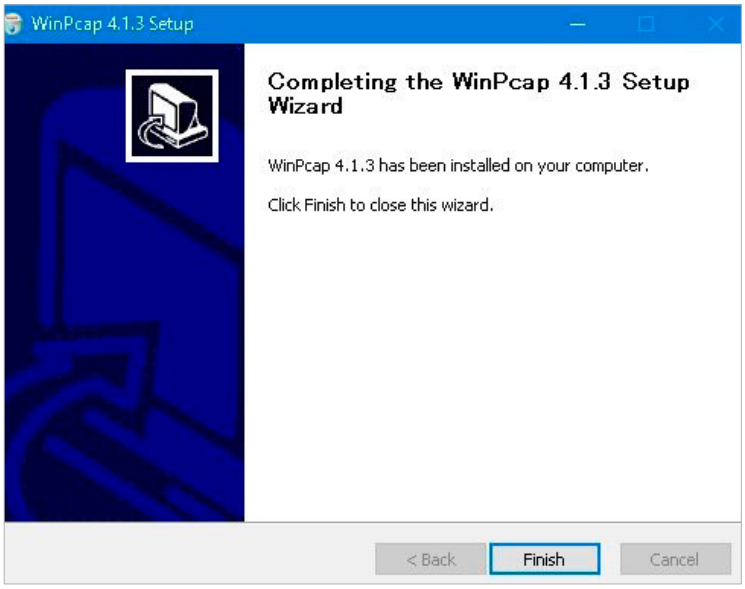

図 2-10　WinPcap - セットアップウィザードの完了

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。

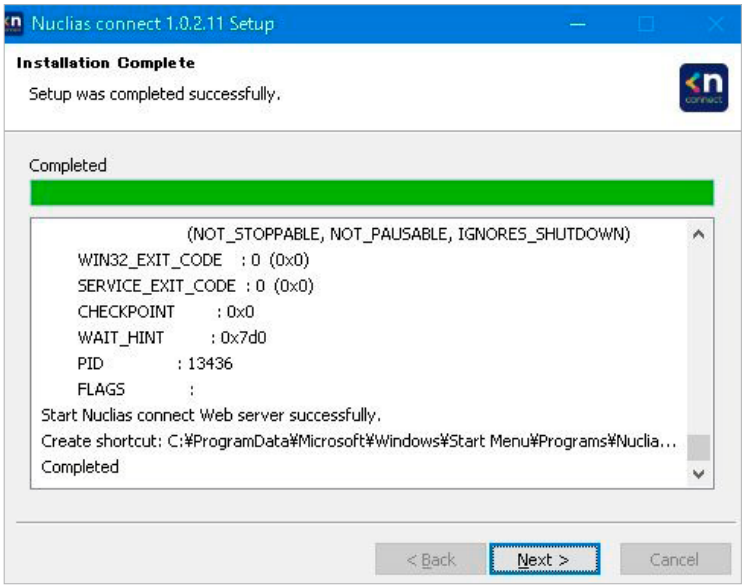

図 2-11　Nuclias Connect - インストール完了

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。

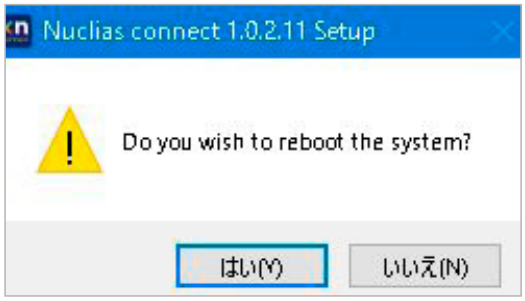

図 2-13　再起動確認メッセージ

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。

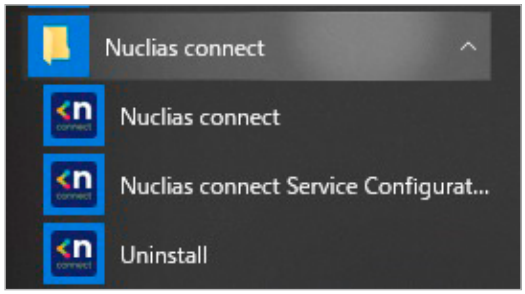

図 2-14　Windows ショートカットメニュー

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。

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

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

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。

図 2-15　Nuclias Connect Setup

■ サービスの有効化 / 無効化

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

■ 管理インタフェースへの接続

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

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

ソフトウェアのインストール

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

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

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

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

■ Nuclias Connect パッケージの展開

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。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。
2. ディレクトリを変更するコマンドを入力します。

```
$ 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
```

4. 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。

```
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 ###########
--
--
--
-e (1/11)---- check your system type ----
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 ----
message: 2
-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
-e (7/11)---- check mongo image ----
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 is 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。

```
User Name: admin
Password: admin
Confirm Password: admin
Creating volume "nuclias_connect_MONGO-DATA" with default driver
Creating mongo ... done
Creating nuclias_connect_core ... done
Creating nuclias_connect_web ... done
-e Nuclias services are running...
-- commands list -----------------------
| |
-e | start: docker-compose up -d |
-e | stop:: docker-compose down |
| |
---------------------------------------
:~/Desktop/nuclias_connect$
```

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。
2. 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_code1 state up group
default qlen 1000
   link/ether 30:65:ec:25:be:3b brd ff: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:ff
4: docker0: <NO-CARRIER,BROADCAST, MULITCAST,UP> mtu 1500 qdisc noqueu state DOWN group
default qlen 1000
   link/ether 02:42:11:ff:39:9f brd ff:ff:ff:ff:ff:ffs
   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。

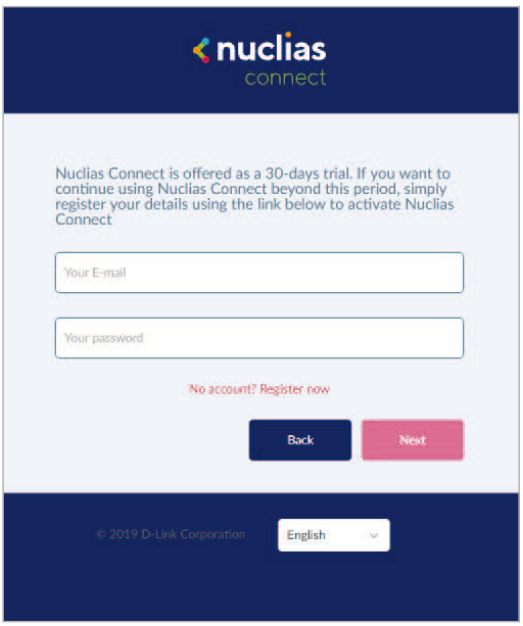

図 2-16　Nuclias Connect 初回ログイン

アカウントの登録

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

1. 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。

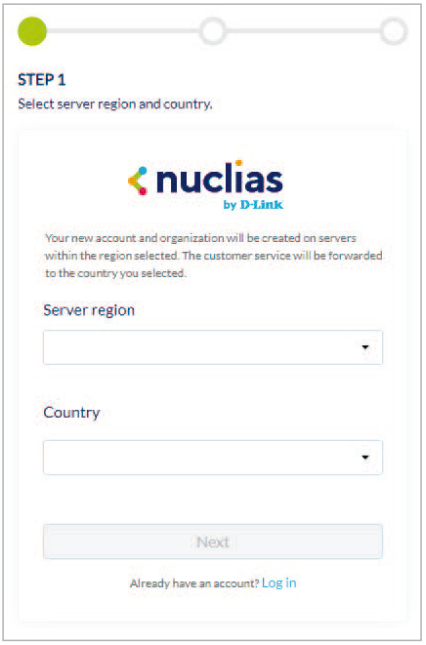

図 2-17　地域 / 国の選択

補足　すでにアカウントをお持ちの場合は、そのアカウントを使用してログインすることができます。新しいアカウントを作成する必要はありません。

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

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。

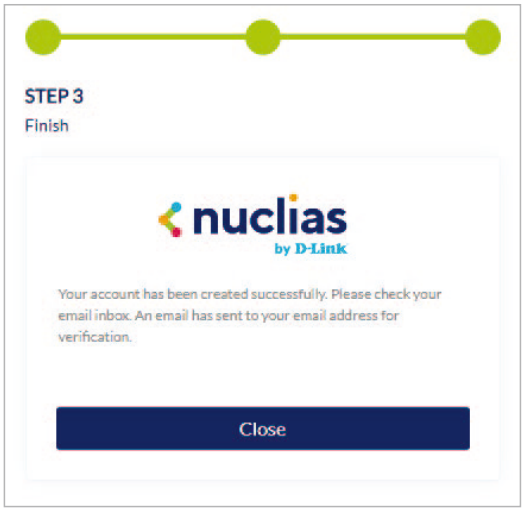

図 2-19　完了画面

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。

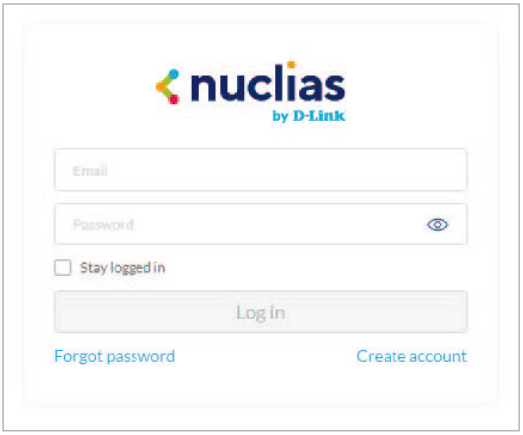

図 2-20　ログイン画面

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://domain-name.com など）を入力します。

補足　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、 

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。

図 2-21　Nuclias Connect Setup 画面

または、次の方法でインタフェースに直接アクセスすることも可能です。

- デスクトップから、**スタート > すべてのプログラム > Nuclias Connect** の順に選択し、 

をクリックしてデフォルトの Web ブラウザを開きます。

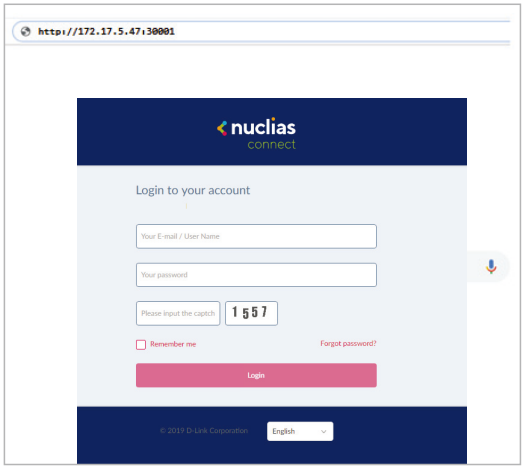

図 2-22　Nuclias Connect ログイン画面

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。

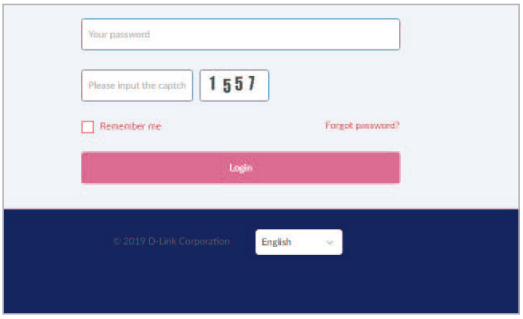

図 2-23　アカウント情報入力オプション

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。

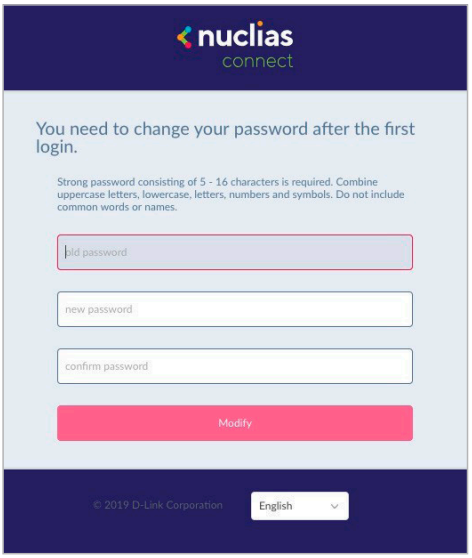

図 2-24　パスワードの変更

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。

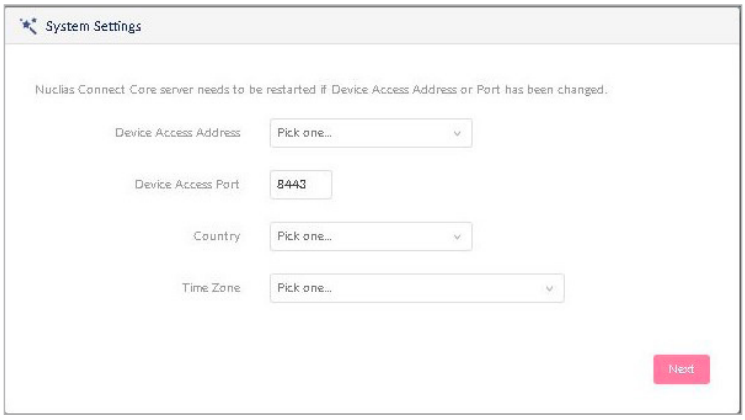

図 2-25　システム設定

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。

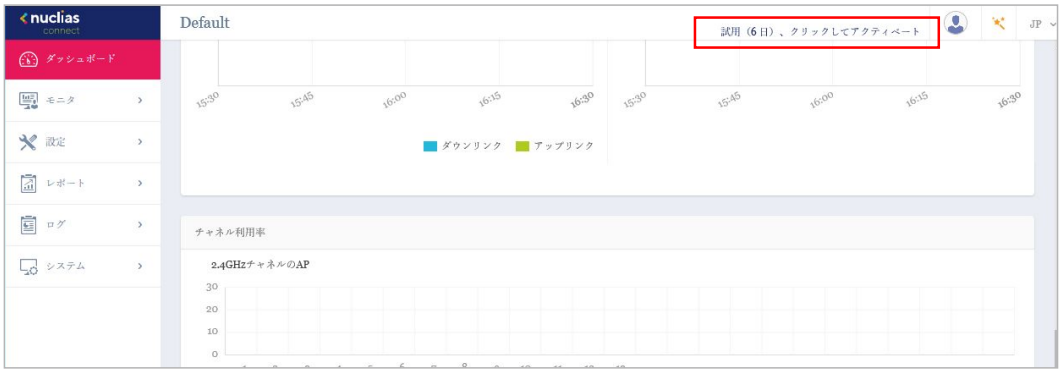

図 2-26　アクティベート

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。

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。

図 2-28　管理情報の入力

項目	説明
どのように Nuclias Connect を使用しますか？	Nuclias Connect の用途を選択します。 • 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 を管理する予定ですか？	管理対象のアクセスポイント数を指定します。 • 選択肢：<20, 20-50, 50-100, 100-500, >500
いくつのサイトを管理する予定ですか？	管理するサイト数を入力します。

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。

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。

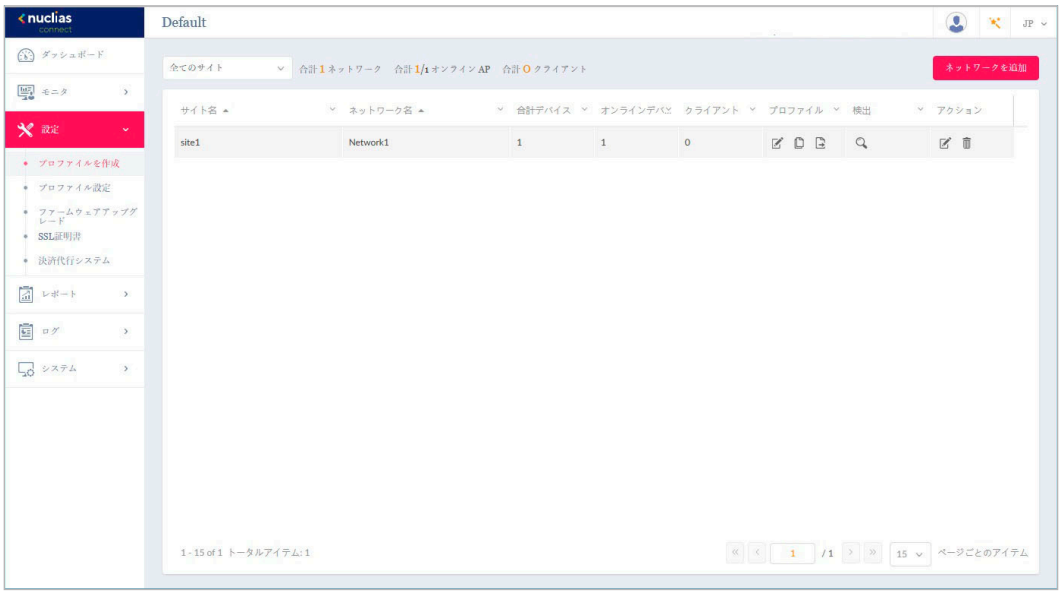

図 2-30　プロファイルを作成

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。

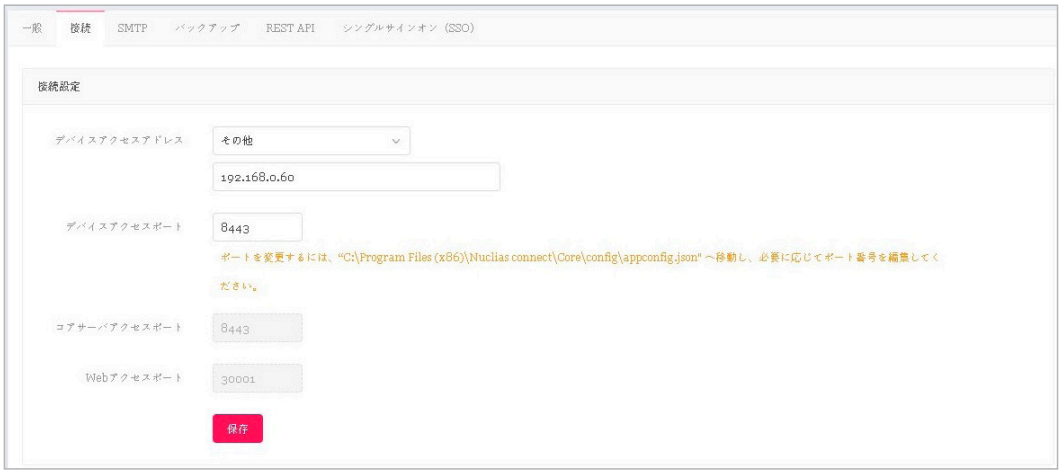

図 2-31　設定 - 接続タブ

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。

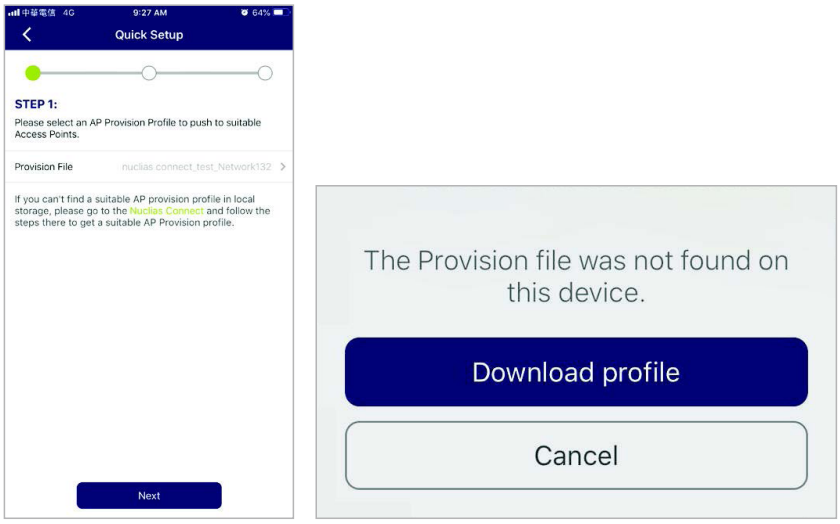

図 2-33　STEP 1 - プロファイルのダウンロード

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。

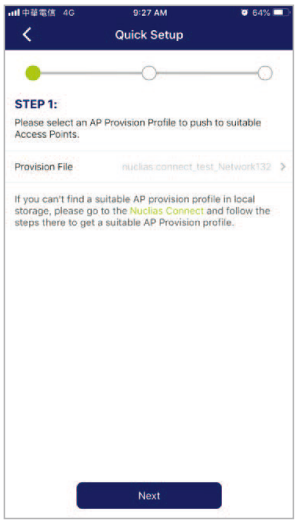

図 2-34　STEP 1 - プロビジョンプロファイルの選択

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。

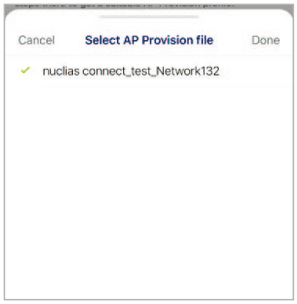

図 2-35　STEP 1 - プロビジョンプロファイルの選択

■ 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。

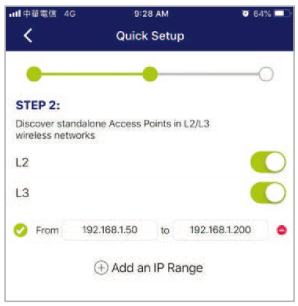

図 2-36　STEP 2 - アクセスポイント検出範囲の定義

■ 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。

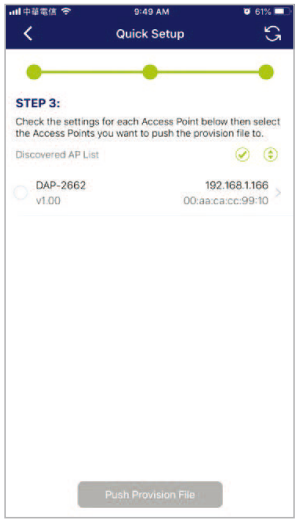

図 2-37　STEP 3 - アクセスポイントの選択

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。

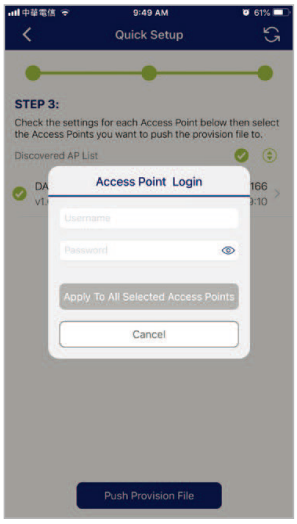

図 2-38　STEP 3 - アクセスポイントへのログイン

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。

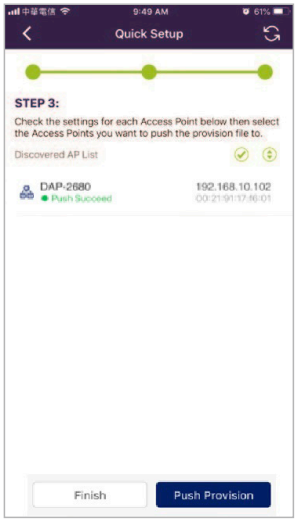

図 2-39　STEP 3 - プロファイルの適用

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

2. 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。

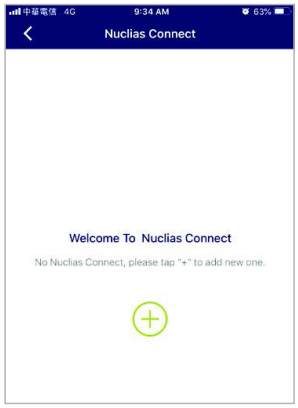

図 2-41　Welcome 画面

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

項目	説明
Specify NuciasConnect URL/IP Address	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。
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　新規サーバへのログイン画面

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

図 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。

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。

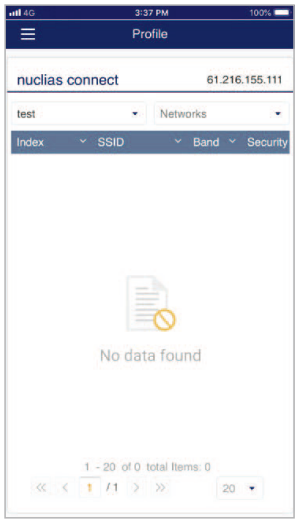

図 2-45　ダッシュボード

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。

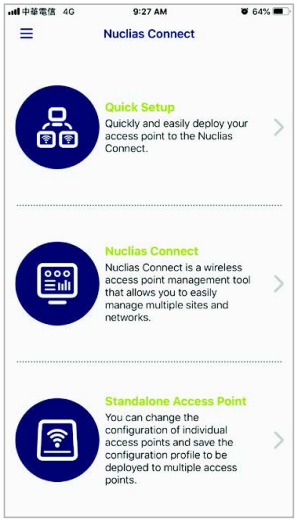

図 2-46　Nuclias Connect アプリ - トップ画面

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。

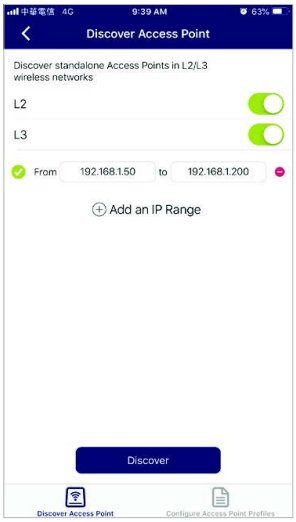

図 2-47　アクセスポイントの検出範囲

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。

図 2-48　プロファイルの配信

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。

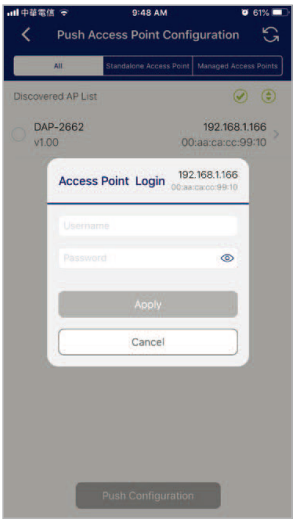

図 2-49　アクセスポイントへのログイン

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。

「IP Info」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。
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。

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。

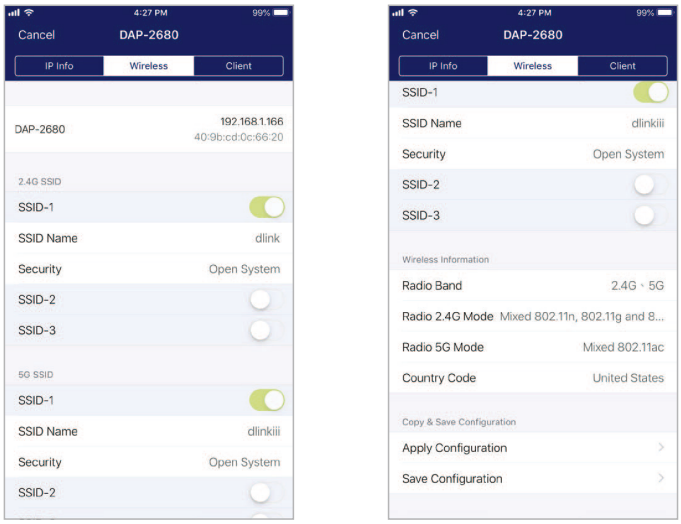

図 2-51　ワイヤレス設定

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。

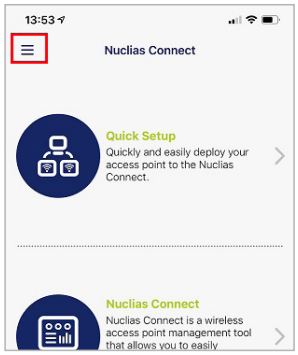

図 2-52　Nuclias Connect アプリ - トップ画面

2. 「AP Provision Profile」を選択します。

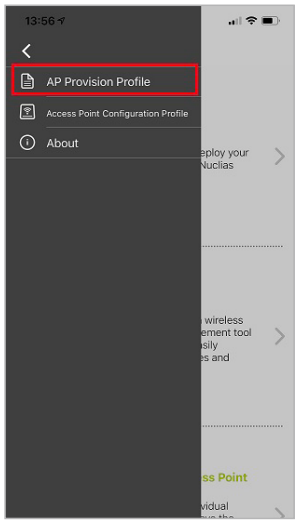

図 2-53　Nuclias Connect アプリ - メニュー項目

3. 対象のプロファイルを選択して削除します。

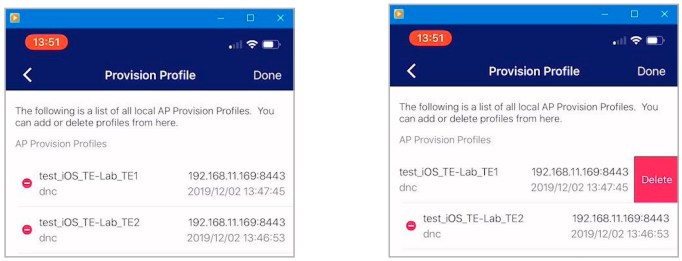

図 2-54　Nuclias Connect アプリ - プロファイル選択

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。

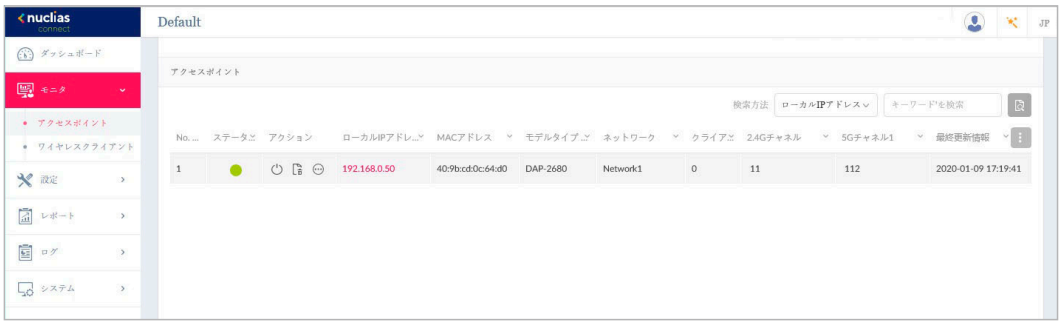

図 2-55　モニタ - アクセスポイント

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。

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

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。

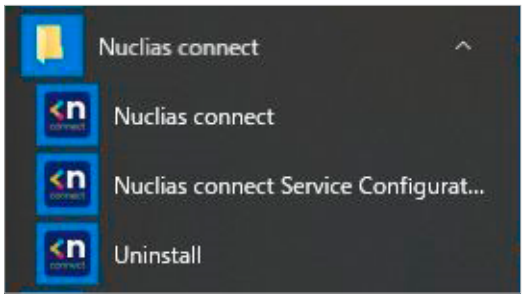

図 3-1　Nuclias Connect アプリケーション

「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。

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。

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。

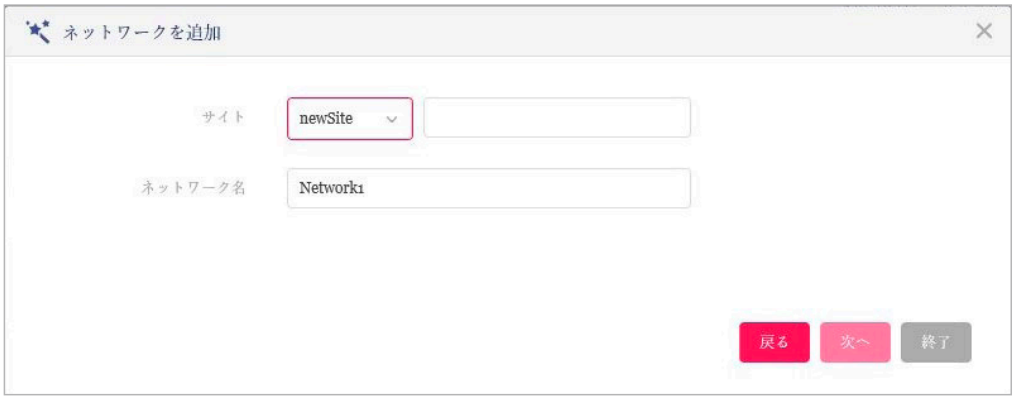

図 3-4　ネットワークを追加

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。

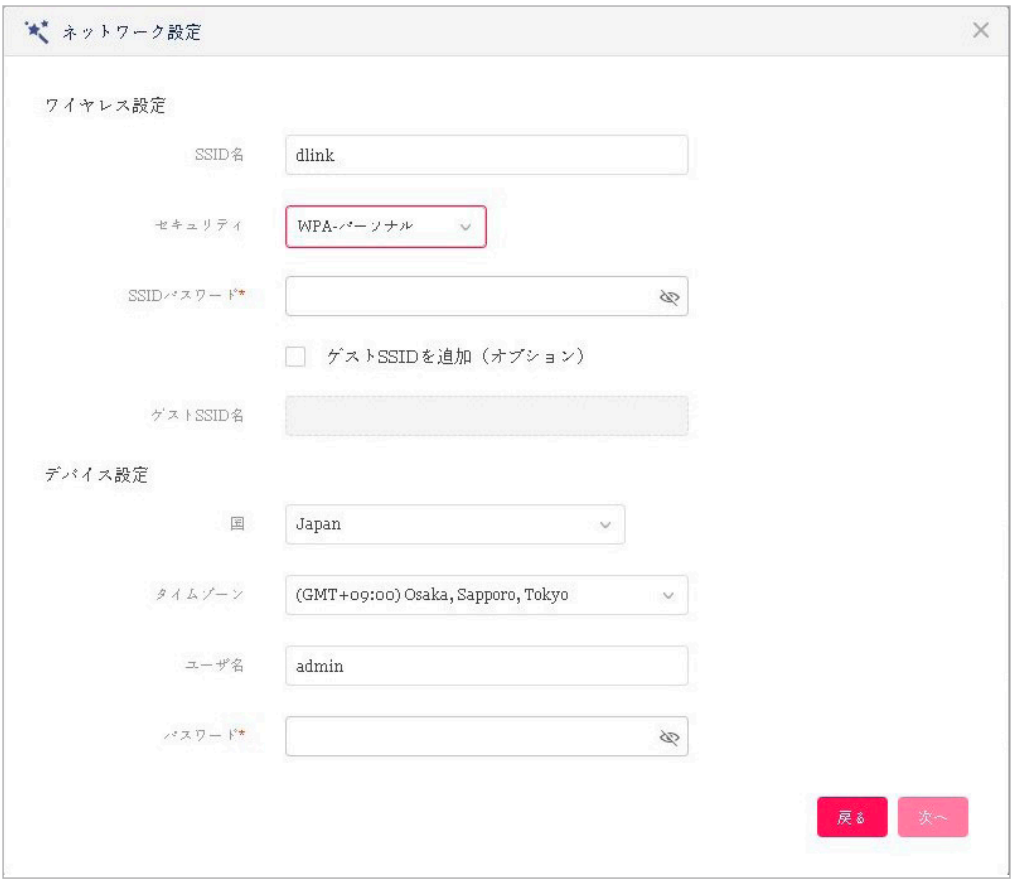

図 3-5　ネットワークの設定

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。

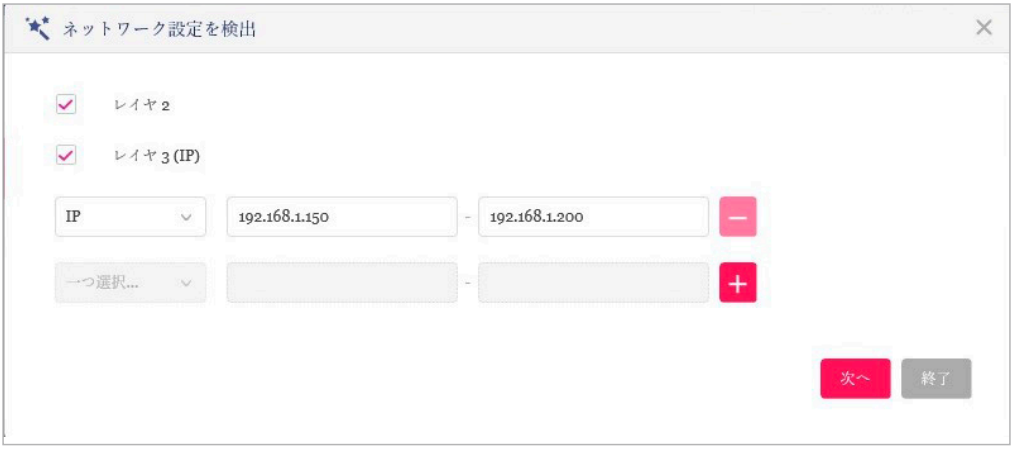

図 3-6　ネットワーク設定を検出

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。

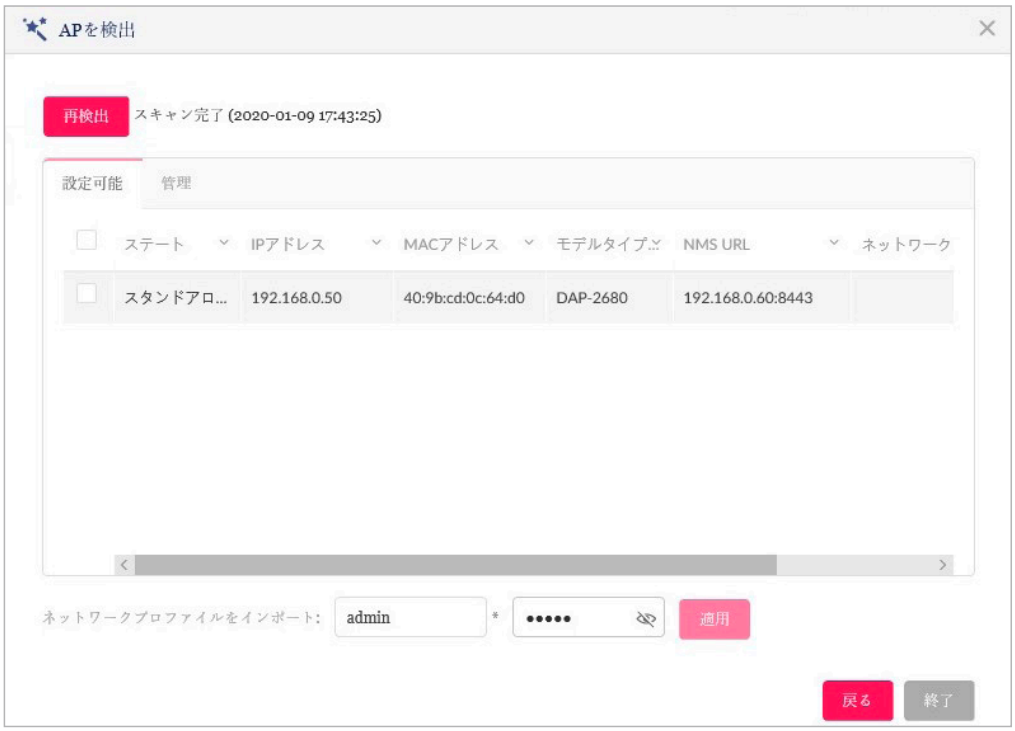

図 3-7　AP を検出

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。

図 3-8　ユーザプロファイル - 個人情報

「設置場所」「電話番号」「説明」を設定し、「更新」をクリックします。

セキュリティ

「セキュリティ」タブを選択すると、以下の画面が表示されます。

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。

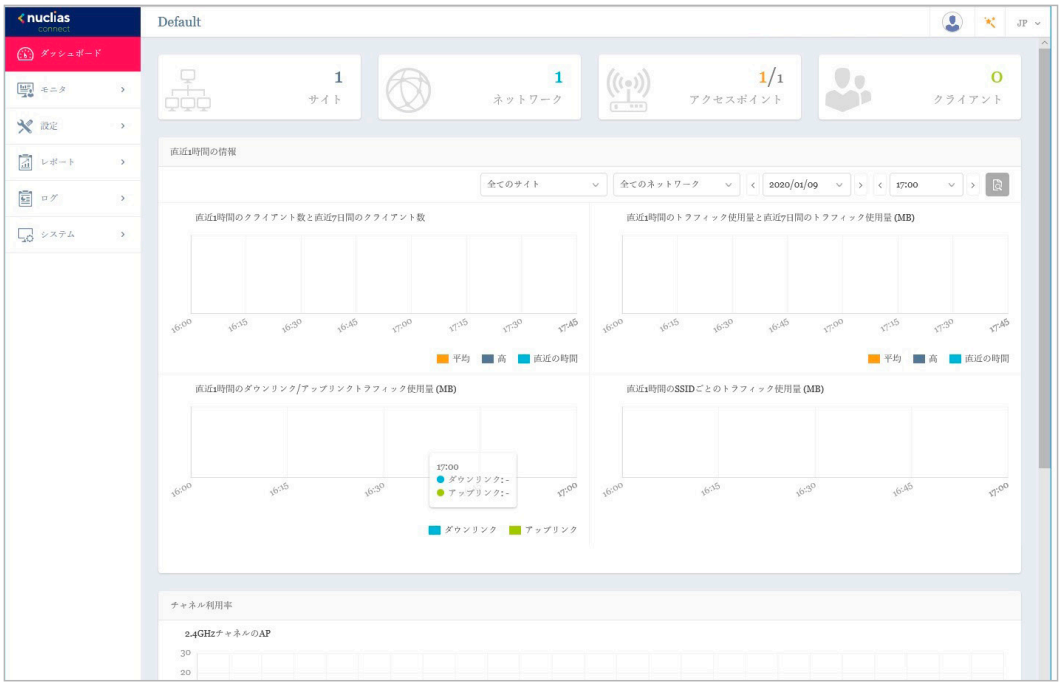

図 4-1　　ダッシュボード

第 5 章　モニタ

アクセスポイント

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。

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。

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

ブロックされたクライアント

左側のパネルから**モニタ > ワイヤレスクライアント**をクリックすると、「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。

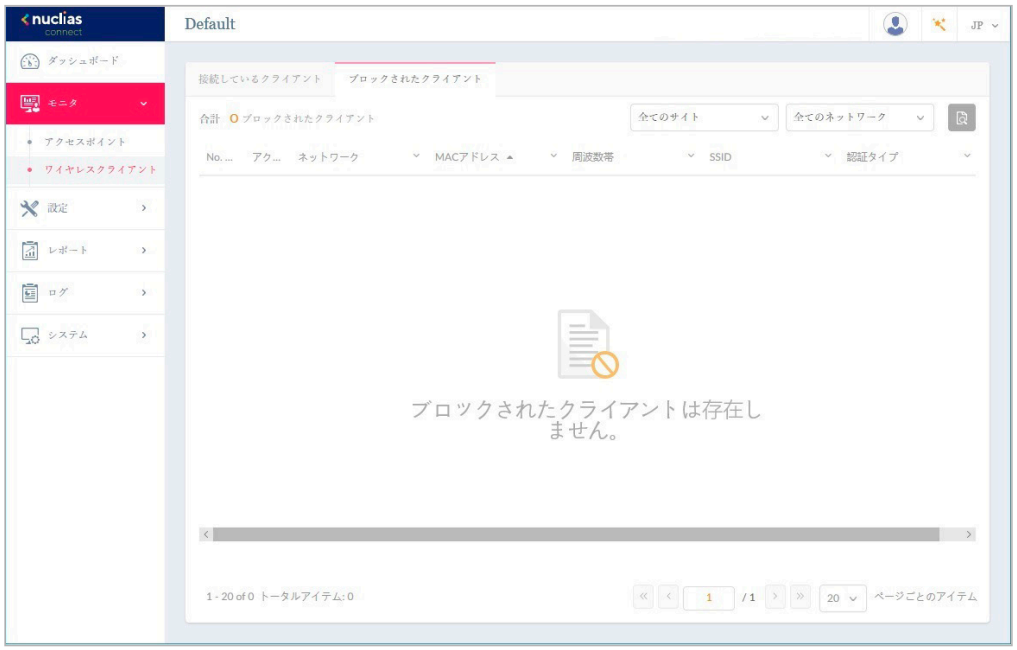

図 5-3　　モニタ - ワイヤレスクライアント（ブロックされたクライアント）

「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。

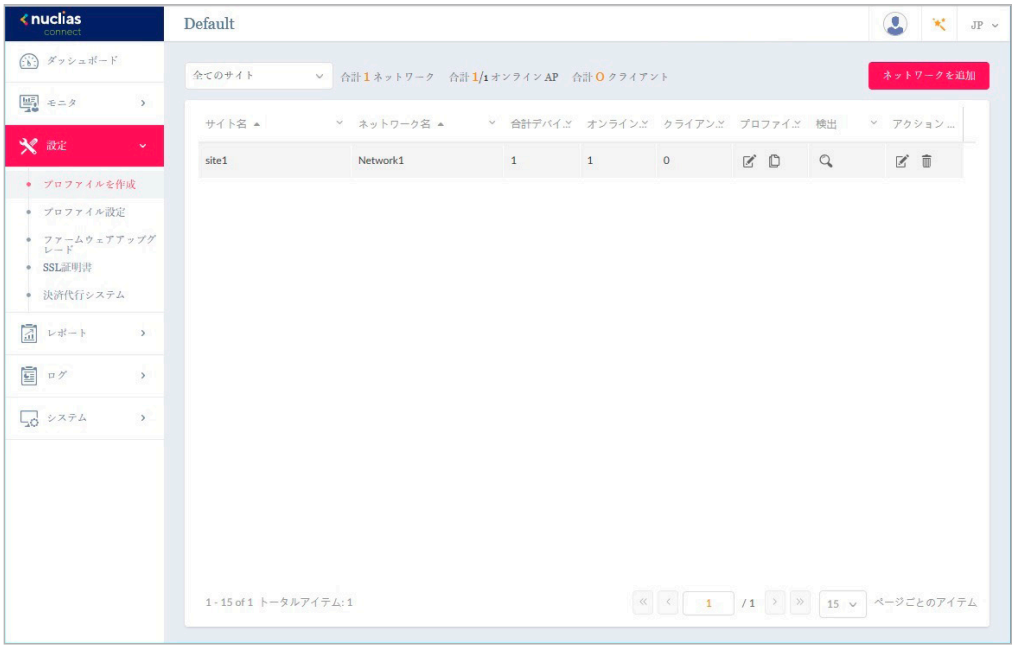

図 6-1　　プロファイルを作成

「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	説明
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ロファイルをコピー	既存のプロファイルを指定したサイトとネットワークにコピーします。
ネットワークプロファイルをエクスポート	選択したプロファイル（*.dat）をローカルディレクトリにエクスポートします。
検出	「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」面面を開きます。この画面から、ネットワーク設定を編集したり、新しいサイトまたは既存のサイトに移行したりすることができます。
ネットワークを削除	選択したネットワーク設定を削除します。

ネットワークの追加

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

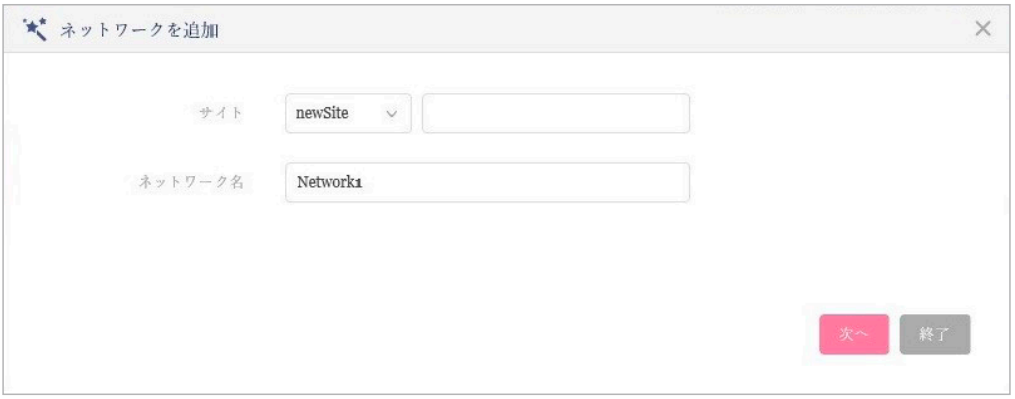

図 6-2　ネットワークを追加

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。

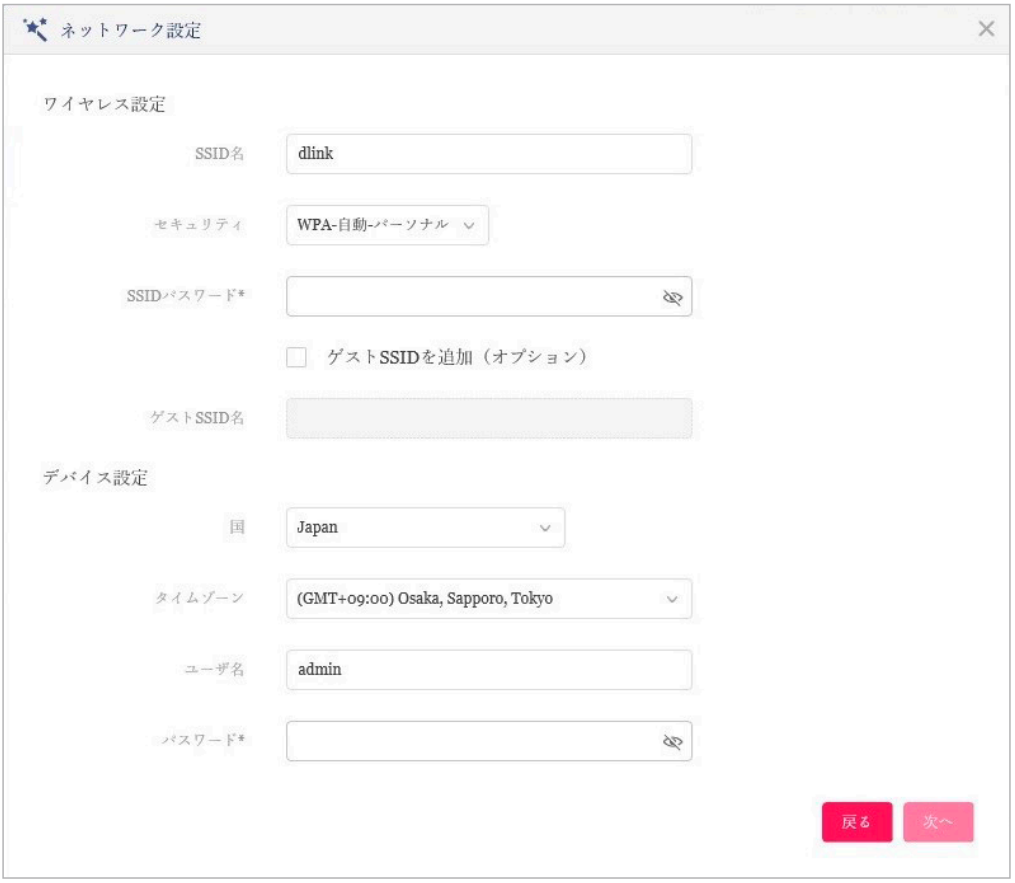

図 6-3　ネットワークの設定

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。

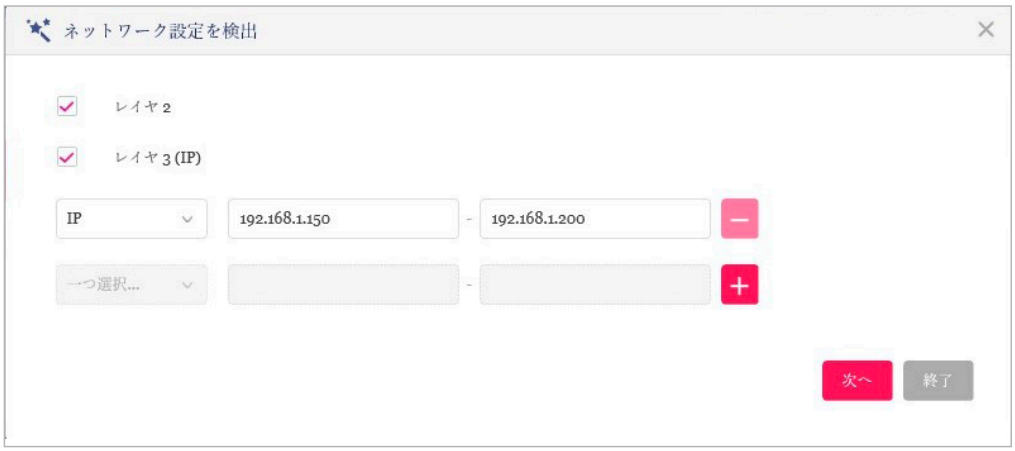

図 6-4　ネットワーク設定を検出

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。

図 6-5　AP を検出

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

プロファイル設定

プロファイル設定機能では、既存のネットワークを管理することができます。

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

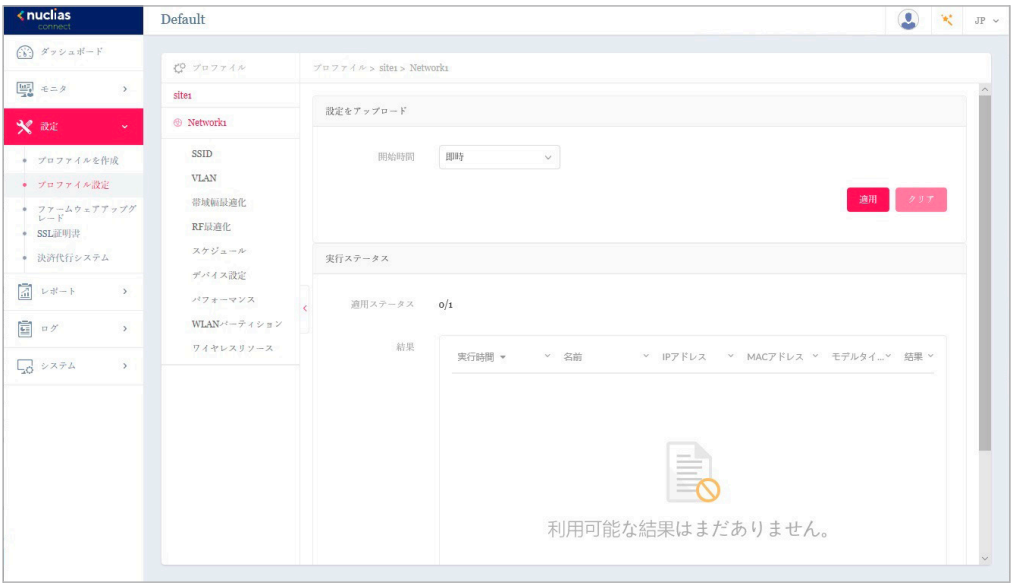

図 6-6　　プロファイル設定

■ 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。

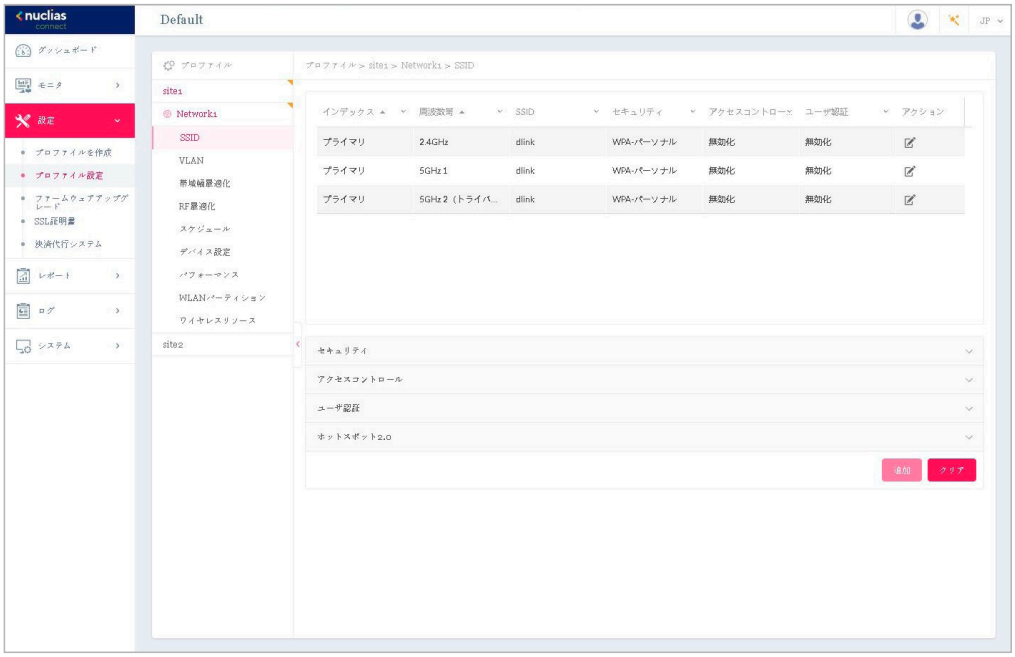

図 6-7　　プロファイル設定 - SSID

セキュリティ

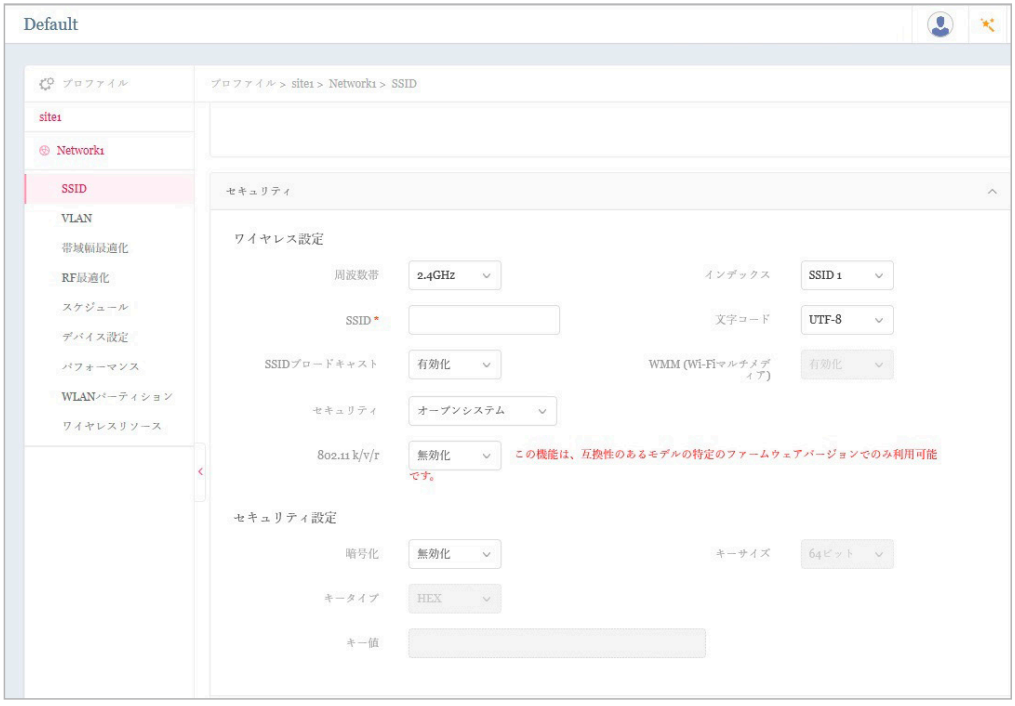

図 6-8　　セキュリティ

「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

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

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

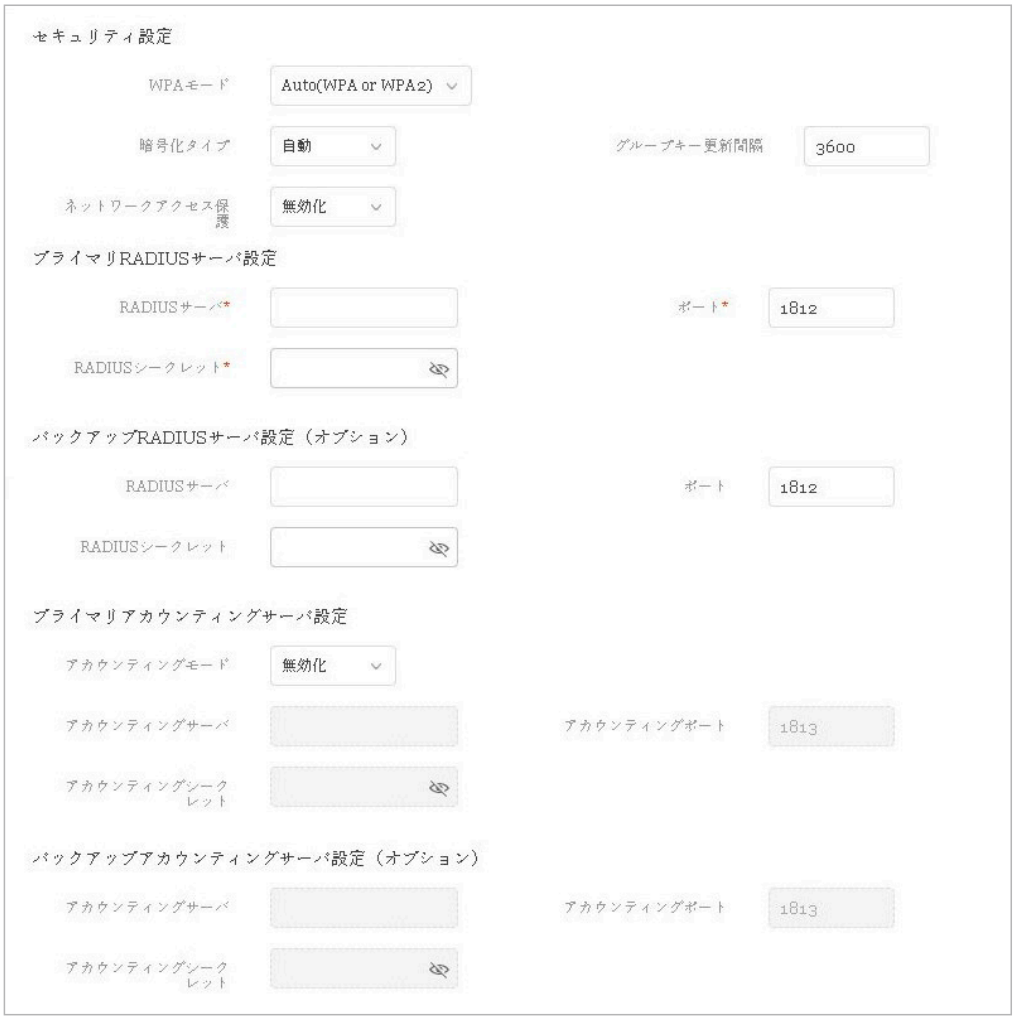

図 6-11　セキュリティ（WPA エンタープライズ）

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

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

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 アドレスリストをアップロード	「ブラウザ ...」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードするには、「ダウンロード」をクリックします。
IP フィルタ設定	
アクション	ドロップダウンメニューをクリックして、IP フィルタ機能を有効または無効にします。
IP アドレス	IP アドレスを入力します。
サブネットマスク	サブネットマスクを入力し、「追加」をクリックします。

ユーザ認証

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」「外部キャプティブポータル」「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（2~1440）	セッションタイムアウト値を入力します。
ホワイトリストを有効化（認証タイプが「Web リダイレクトのみ」以外の場合）	
ホワイトリストを有効化	チェックを入れると、ホワイトリスト機能が有効になります。この機能は、「認証タイプ」が「Web リダイレクトのみ」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 アドレスを入力し、「追加」をクリックしてアドレスをホワイトリストテーブルに追加します。
MAC アドレスリストをアップロード	「ブラウザ ...」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードするには、「ダウンロード」をクリックします。
IP 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 / パスワードファイルをアップロード	「ブラウザ ...」をクリックして、ローカルコンピュータに保存されたユーザ名 / パスワードリストのファイルを選択します。「アップロード」をクリックしてユーザリストを更新します。現在のユーザリストをダウンロードするには、「ダウンロード」をクリックします。
リモート RADIUS（認証タイプが「リモート RADIUS」「MAC アドレス」の場合）	
RADIUS サーバ	RADIUS サーバの IP アドレスを入力します。
RADIUS ポート	RADIUS サーバのポート番号を入力します。
RADIUS シークレット	RADIUS サーバのシークレットを入力します。

項目	説明
リモート RADIUS タイプ	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） • 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。 • 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

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。

項目	説明
ホットスポット	
ホットスポット 2.0	ドロップダウンメニューをクリックして、ホットスポット 2.0 機能を有効または無効にします。
OSEN	ドロップダウンメニューをクリックして、OSEN（OSU Server-Only Authenticated L2 Encryption Network）を有効または無効にします。
クロス接続を許可	ドロップダウンメニューをクリックして、クライアントのクロス接続を有効または無効にします。
P2P を管理	ドロップダウンメニューをクリックして、P2P 管理を有効または無効にします。
DGAF	ドロップダウンメニューをクリックして、DGAF（Downstream Group-Addressed Forwarding）を有効または無効にします。有効にすると、AP はダウンストリームのグループアドレスフレームを転送することができます。
プロキシ ARP	ドロップダウンメニューをクリックして、プロキシ ARP を有効または無効にします。
L2TIF	ドロップダウンメニューをクリックして、L2TIF（Layer 2 Traffic Inspection and Filtering）を有効または無効にします。
インターワーキング	
インターワーキング	ドロップダウンメニューをクリックして、インターワーキングを有効または無効にします。
アクセスネットワークタイプ	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」
ASRA	ドロップダウンメニューをクリックして、ASRA（Additional Steps required for Access）を有効または無効にします。
ESR	ドロップダウンメニューをクリックして、ESR（Emergency services reachable）を有効または無効にします。
USEA	ドロップダウンメニューをクリックして、USEA（Unauthenticated Emergency Service Accessible）を有効または無効にします。
Venue グループ	Venue グループの値を入力します。
Venue タイプ	Venue タイプの値を入力します。
Venue 名	言語を選択し、Venue 名を入力します。
HESSID	Homogenous Extended Service Set（ESS）ID を入力します。サービスプロバイダネットワークを識別するために使用されます。
WAN メトリック	
WAN リンクステータス	アクセスポイントの WAN リンクステータスを選択します。 • 選択肢：「リンクアップ」「リンクダウン」「テストステートでのリンク」

項目	説明
WAN 対称リンク	WAN 対称リンクのステータスを「はい」「いいえ」から選択します。「はい」の場合、アップロード / ダウンロードは同じ速度になります。
WAN 帯域	WAN 帯域のステータスを「はい」「いいえ」から選択します。アクセスポイントやネットワークがキャパシティの上限に達している場合、「はい」を選択します。
WAN メトリックダウンロードスピード（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 メトリックアップリンクスピード（kps）	WAN 接続のアップロードスピードを kbps 単位で入力します。アップロードスピードが不明な場合は 0 を指定します。
リスト	
ネットワーク認証タイプ	接続タイプを選択します。 • 選択肢：「利用規約への同意」「オンライン登録をサポート」「http/https リダイレクション」「DNS リダイレクション」「http/https リダイレクション」「DNS リダイレクション」の場合は、URL を入力する必要があります。
利用可能な IP アドレスタイプ	利用可能な IP アドレスタイプを選択します。ネットワークへの認証後、 ホットスポットのオペレータやモバイルデバイスによってこのアドレスタイプが使用されます。 • 選択肢：「アドレスタイプは利用できません。」「利用可能なグローバル IP アドレス」「利用可能なポート制限された IPv4 アドレス」「利用可能なシングル NAT されたプライベート IPv4 アドレス」「利用可能なダブル NAT されたプライベート IPv4 アドレス」「利用可能なポート制限された IPv4 アドレスとシングル NAT された IPv4 アドレス」「利用可能なポート制限された IPv4 アドレスとダブル NAT された IPv4 アドレス」「アドレスタイプの IPv4 可用性は不明です。」「利用可能な IPv6 アドレスタイプ」「アドレスタイプの IPv6 可用性は不明です。」
ドメイン名リスト	
ドメイン名	アクセスポイントの実行エンティティのドメイン名を入力し、「追加」をクリックします。
ローミングコンソーシアム	
ローミングコンソーシアム	サービスプロバイダや、ローミングパートナーのグループを入力し、「追加」をクリックします。ネットワークに接続する際に、それらのセキュリティ認証が使用されます。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 レルム	＋をクリックして NAI レルムを入力します。BSS で利用可能な全ての 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、－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」をクリックします。 • 設定可能範囲：00-999
接続機能	
IP プロトコル	IP プロトコルを選択します。 • 選択肢：「ICMP」「TCP」「UDP」
ポート番号	ポート番号を入力します。
ステータス	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リー名	言語を選択し、オペレータフレンドリー名を入力します。Hotspot Venue オペレータの識別名です。
OSU（Onlin Sign-Up）	
OSU SSID	OSU SSID を入力します。
OSU サーバ URI	OSU サーバ URI を入力します。
OSU 方式リスト	
OSU 方式	言語を選択し、OSU 方式を入力します。
OSU コンフィグ	OSU コンフィグ選択します。 • 選択肢：「コンフィグ 1」「コンフィグ 2」
OSU 言語コード	OSU 言語コードを選択します。
OSU フレンドリー名	言語を選択し、OSU フレンドリー名を入力します。
OSU Nai	OSU NAI を入力します。
OSU サービス説明	OSU サービス説明を入力します。

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

■ 新規 SSID の追加

新し 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。

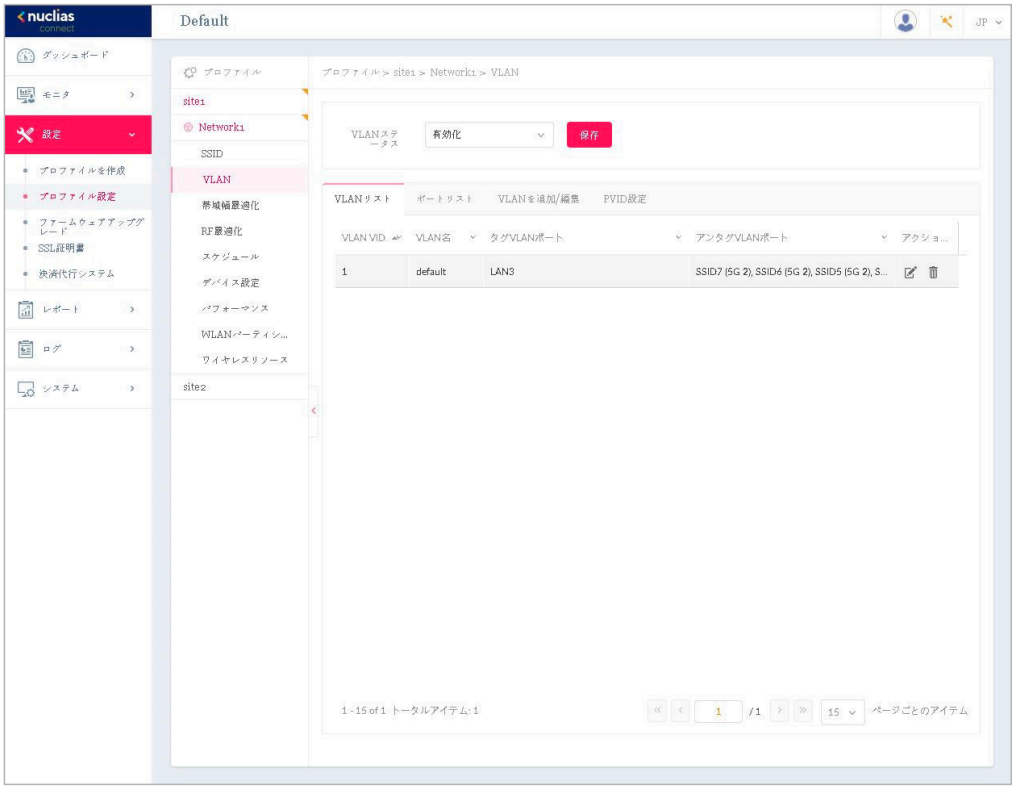

図 6-16　プロファイル設定 - VLAN

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。

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。

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。

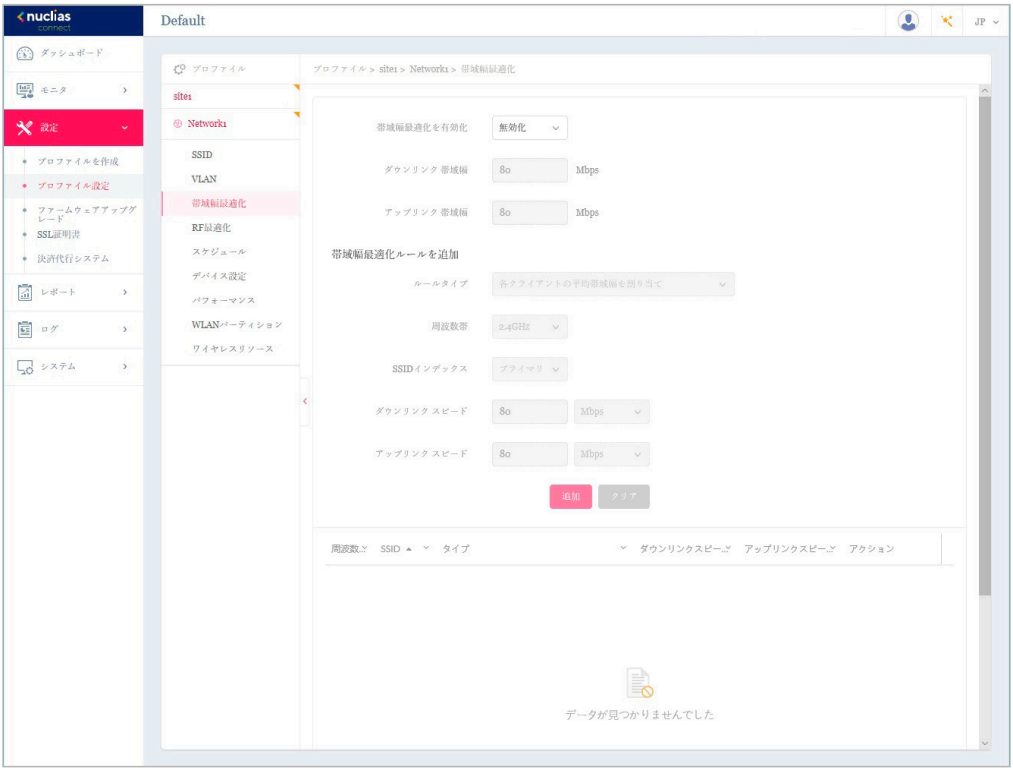

図 6-17　プロファイル設定 - 帯域幅設定

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 をクリックします。設定完了後、「保存」をクリックしてルールを保存します。

ルールを削除する場合は、対象ルールの をクリックします。

「クリア」をクリックすると、設定中のパラメータが初期値に戻ります。

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

RF 最適化

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

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

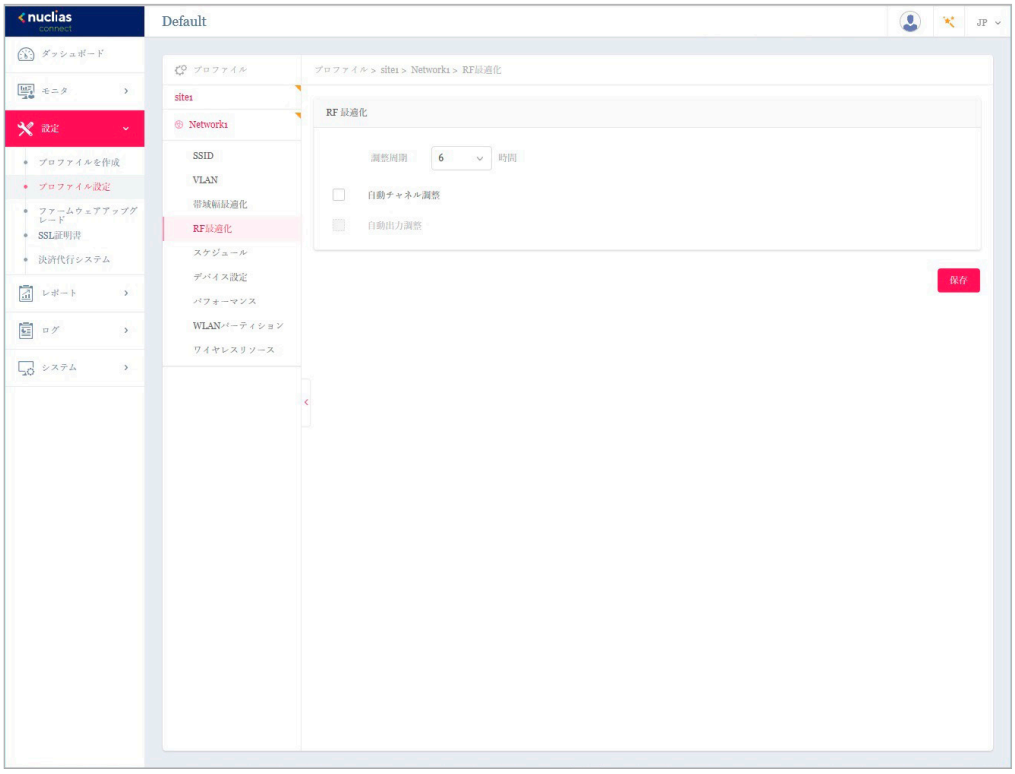

図 6-18　プロファイル設定 - RF 設定

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。

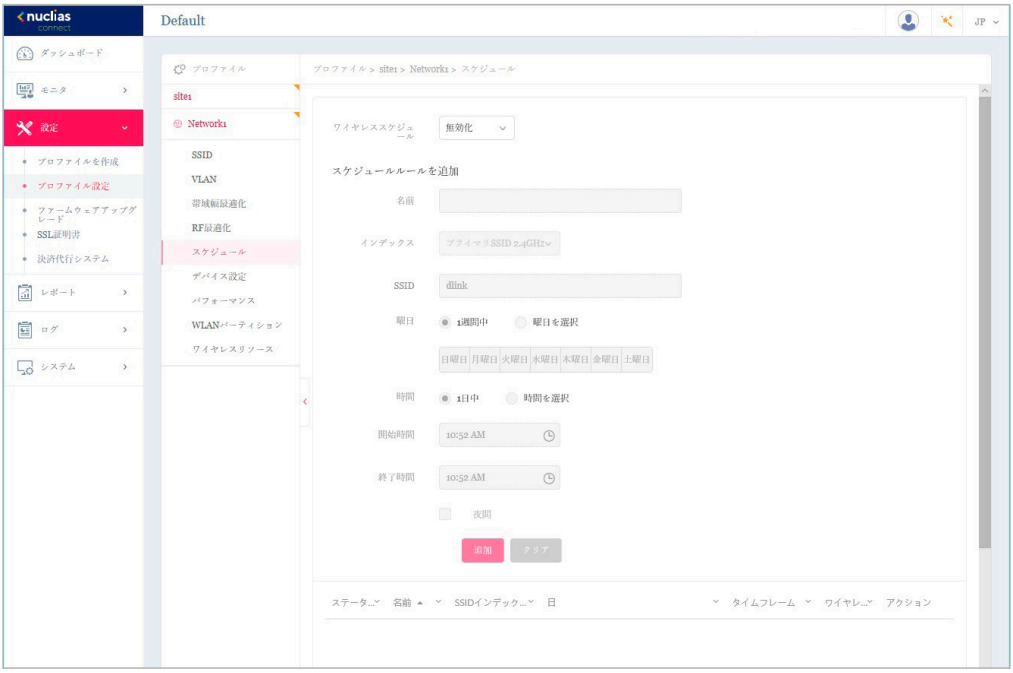

図 6-19　プロファイル設定 - スケジュール

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 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。

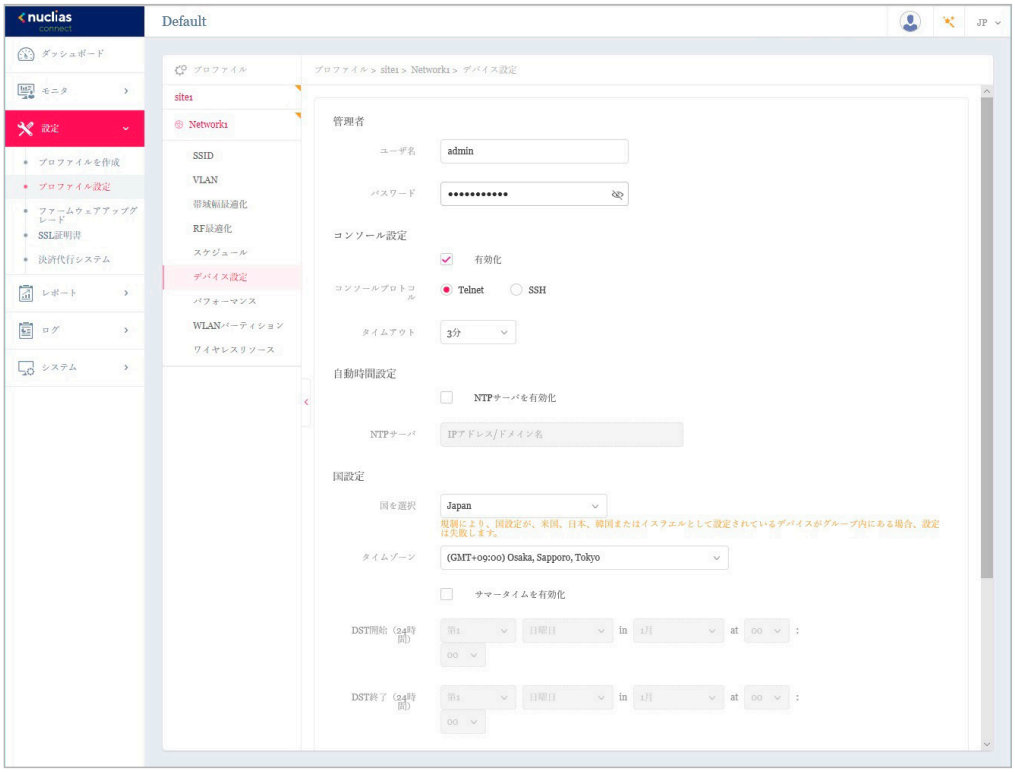

図 6-20　プロファイル設定 - デバイス設定

以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

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

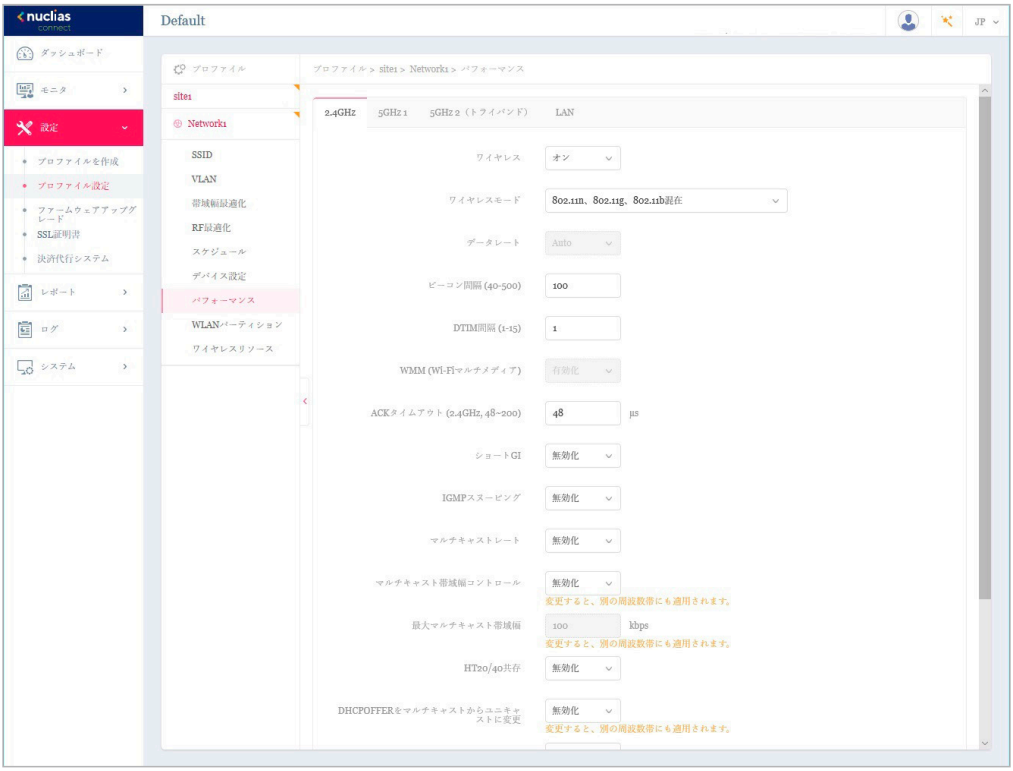

図 6-21　プロファイル設定 - パフォーマンス設定

「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 マルチメディア）	ドロップダウンメニューをクリックして、Wi-Fi マルチメディア（WMM）機能を有効または無効にします。
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コントロール	ドロップダウンメニューをクリックして、マルチキャスト帯域コントロール機能を有効または無効にします。
最大マルチキャスト帯域幅	マルチキャスト帯域幅の最大値を入力します。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 をマルチキャストからユニキャストに変更	ドロップダウンメニューをクリックして、ユニキャストへの DHCP オファー転送を許可または拒否します。
RTS 長	RTS の長さの値を入力します。 • 初期値：2346

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

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。

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/ マルチ SSID1-7	ラジオボタンをクリックして、WLAN パーティションへの SSID のメンバーシップを有効または無効にします。この SSID がゲストとしてこの WLAN パーティションにアクセスできるようにするには、「ゲストモード」を選択します。

「保存」をクリックして設定を保存します。

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

リンクインテグリティ

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

「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

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

「保存」をクリックして設定を保存します。

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

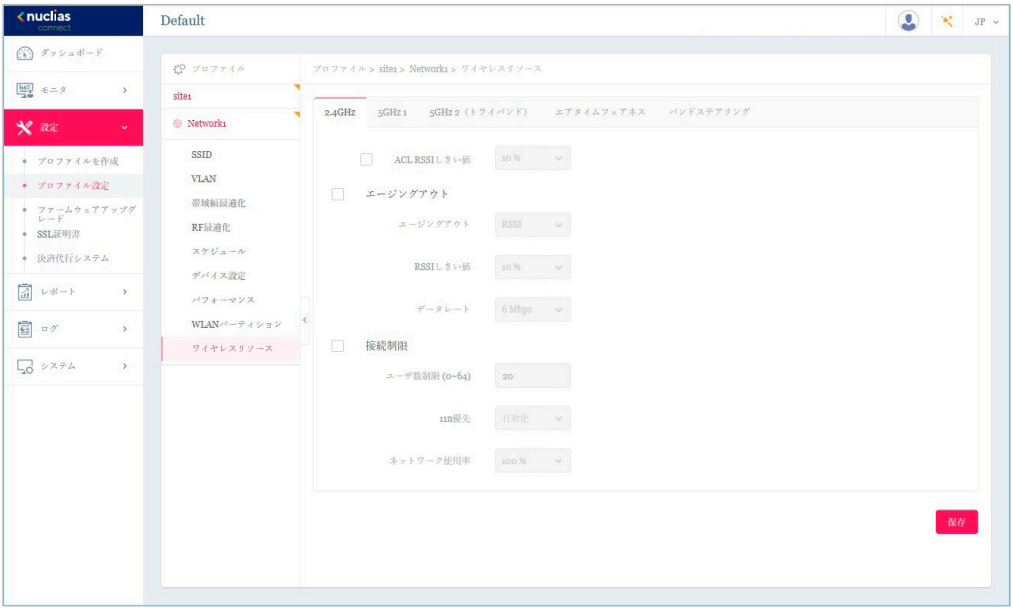

図 6-26　プロファイル設定 - ワイヤレスリソース

「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。

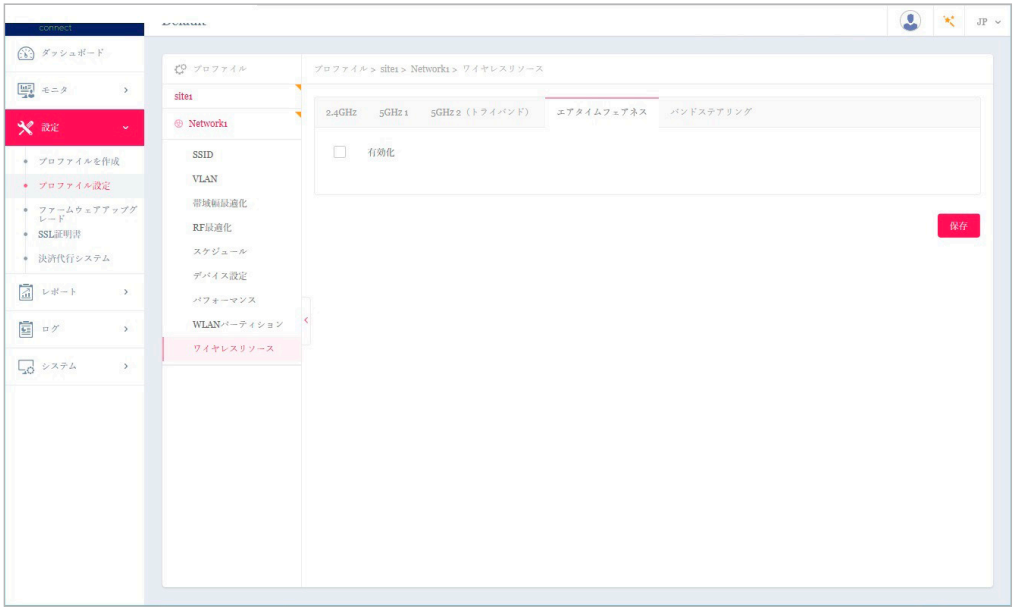

図 6-27　プロファイル設定 - エアタイムフェアネス

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。

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。

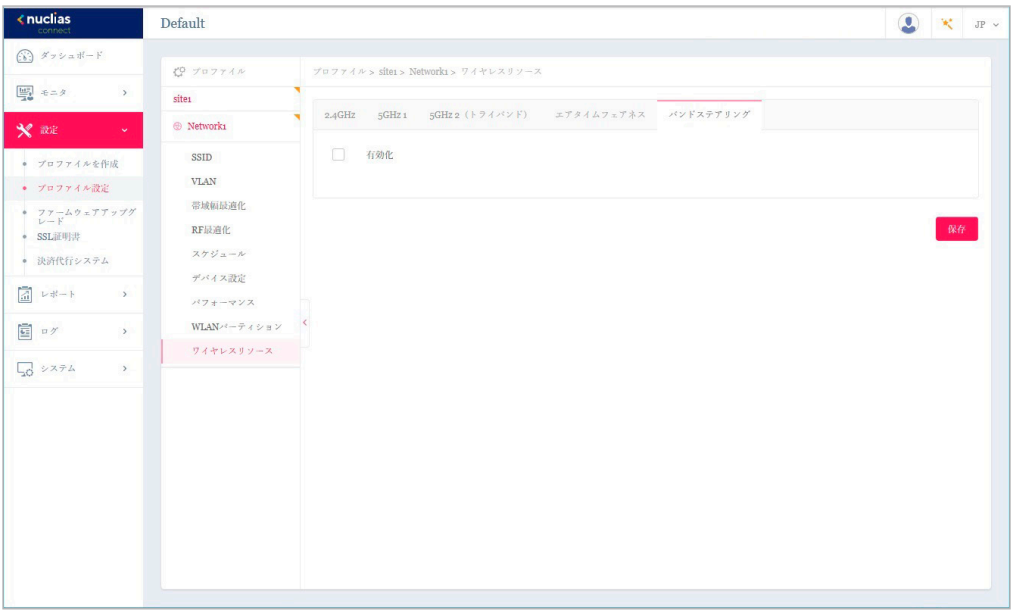

図 6-28　プロファイル設定 - バンドステアリング

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レード > サイト > ネットワーク の順に移動します。

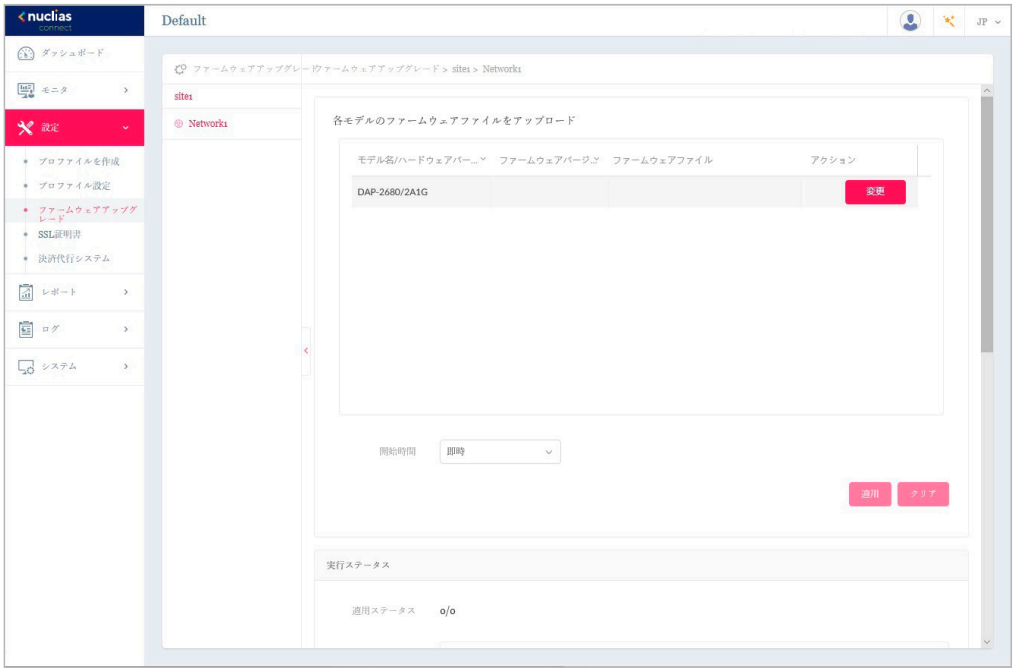

図 6-29　ファームウェアアップグレード

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。

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。

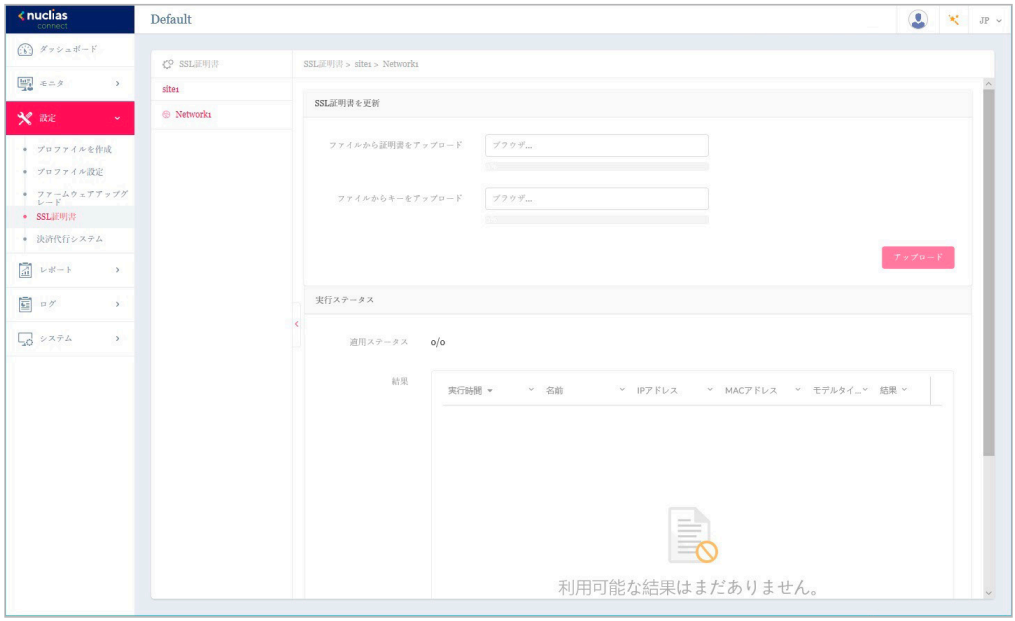

図 6-31　SSL 証明書

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

「アップロード」をクリックして、ファイルのアップロードを開始します。アップロードのステータスと結果が画面下部の「実行ステータス」に表示されます。

決済代行システム　※本項目は日本ではサポート対象外となります。

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

設定 > 決済代行システムに移動します。

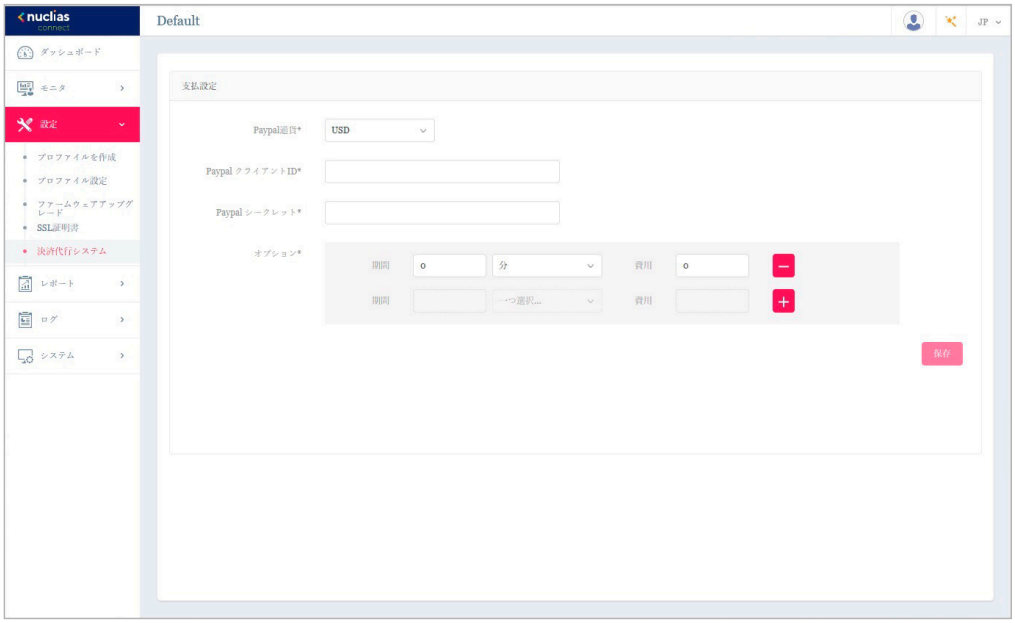

図 6-32　決済代行システム

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。

「保存」をクリックして設定を保存します。

第 7 章　レポート

ピークネットワークアクティビティ

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。

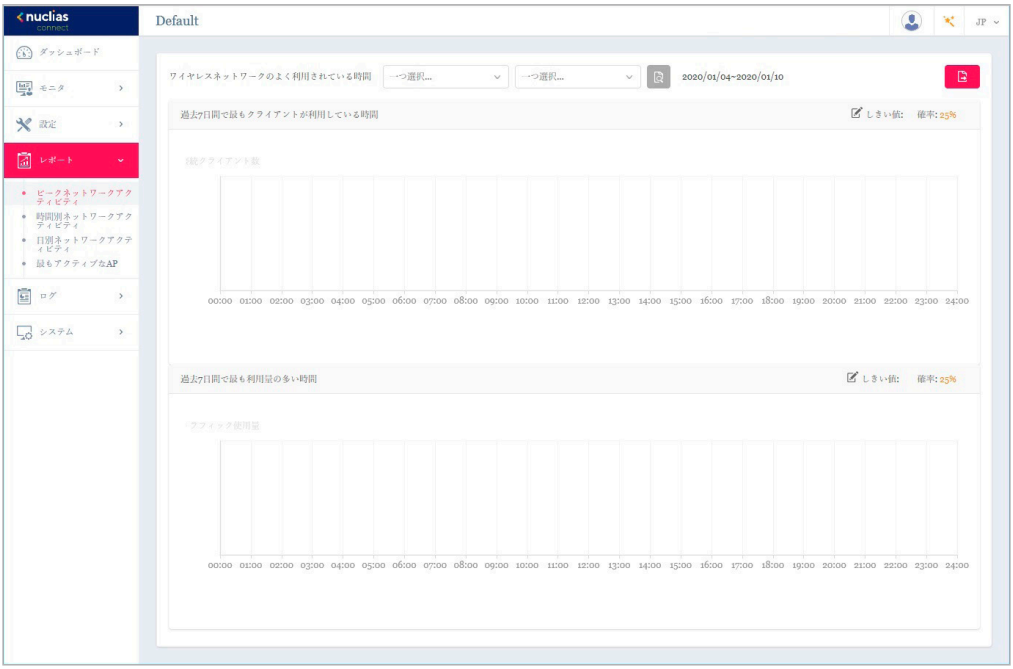

図 7-1　　ピークネットワークアクティビティ

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

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。

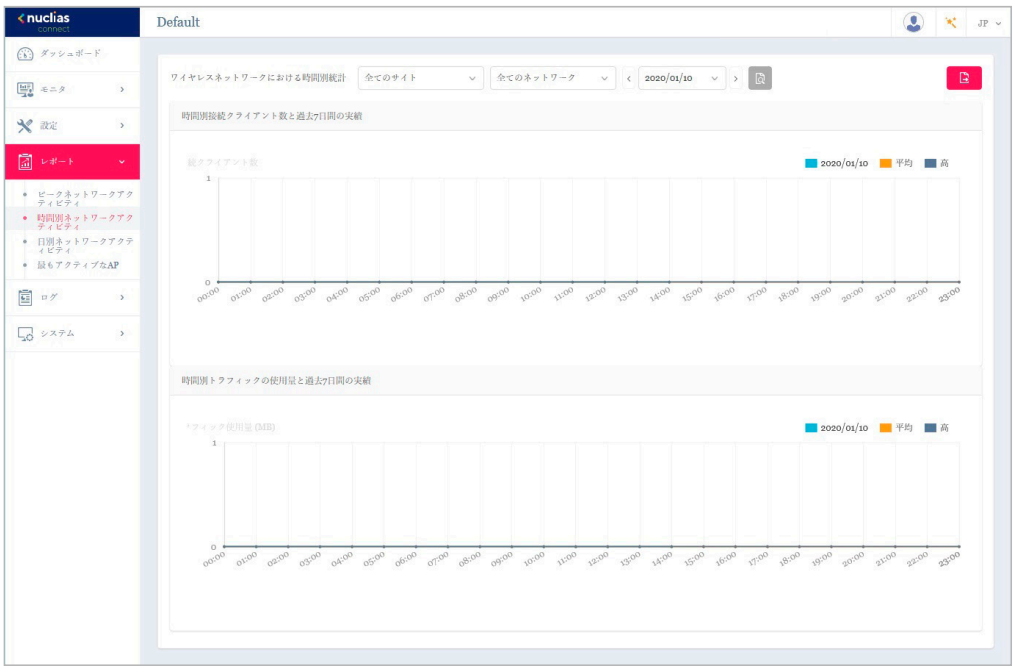

図 7-2　　時間単位のネットワークアクティビティ

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

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。

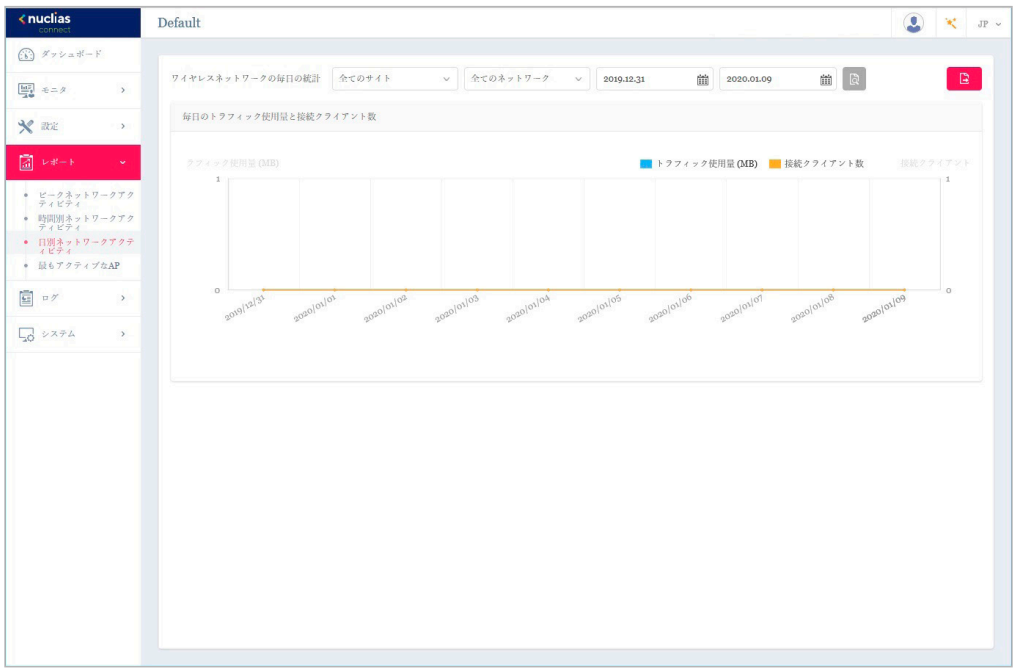

図 7-3　　日別ネットワークアクティビティ

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

以下のレポートが表示されます。

- 毎日のトラフィック使用量と接続クライアント数

最もアクティブな AP

特定のアクセスポイントのトラフィック使用量を表示します。

レポート > 最もアクティブな AP に移動して、レポートを表示します。

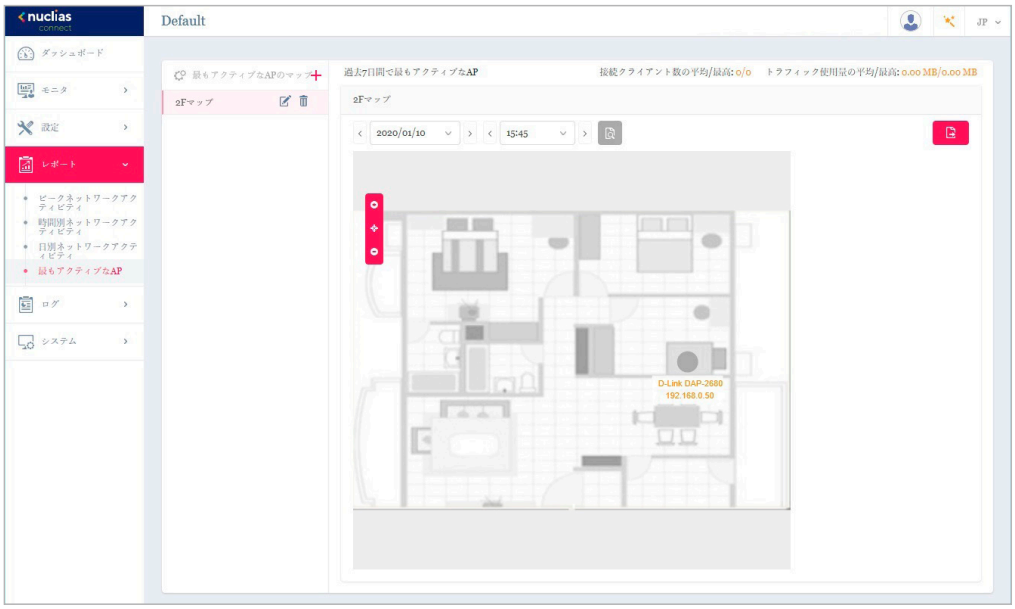

図 7-4　　最もアクティブな AP

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

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。

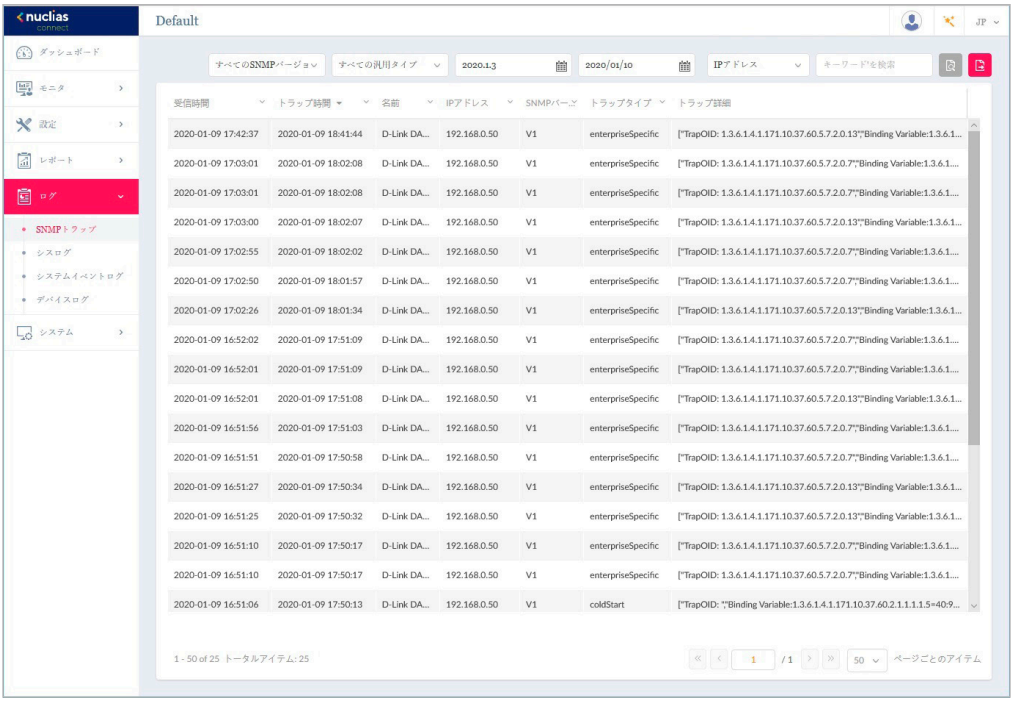

図 8-1　　SNMP トラップ

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。 をクリックしてフィルタを適用します。

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

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

シスログ

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

ログ > シスログに移動して、ログ情報を表示します。

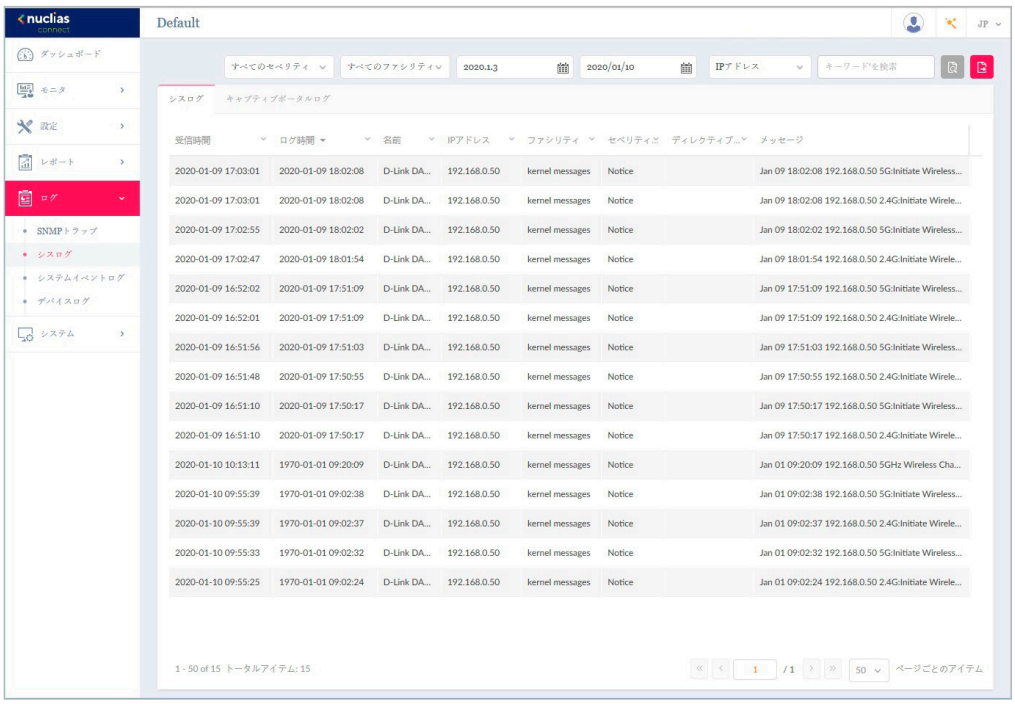

図 8-2　　シスログ

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。 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。

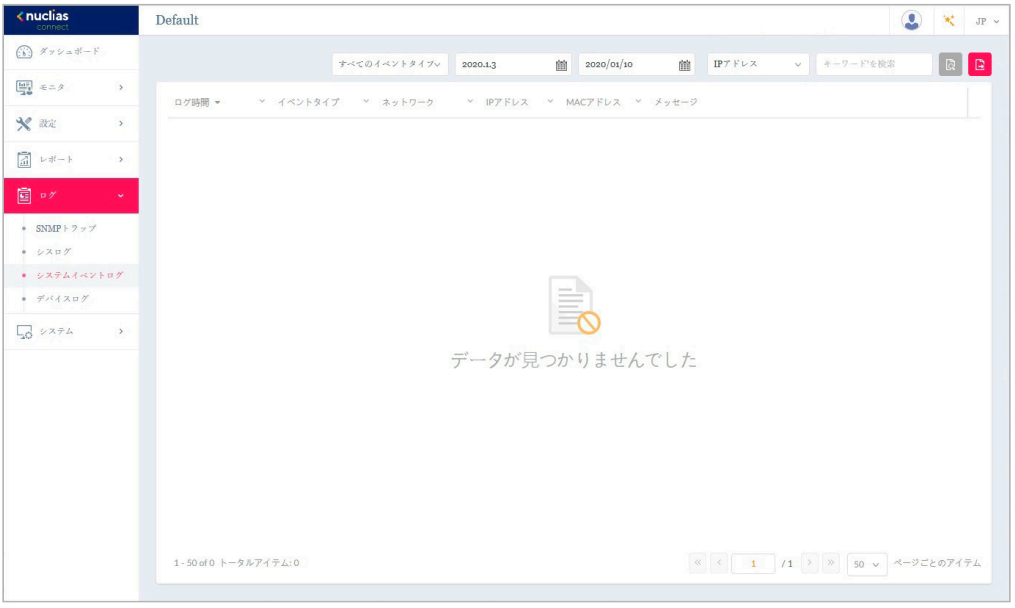

図 8-3　　システムイベントログ

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。 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。

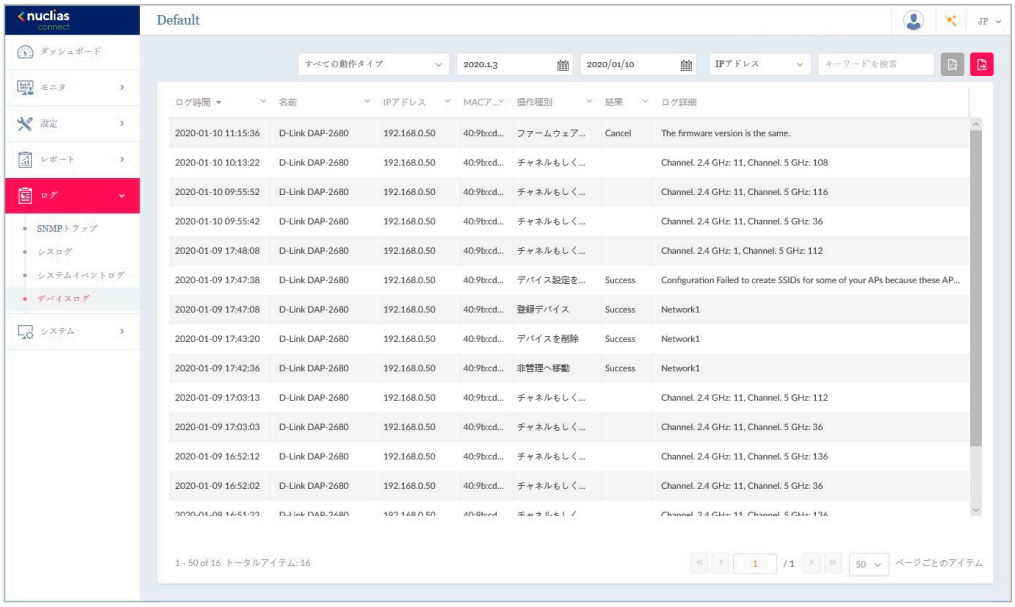

図 8-4　　デバイスログ

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

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

システム > デバイス管理に移動します。

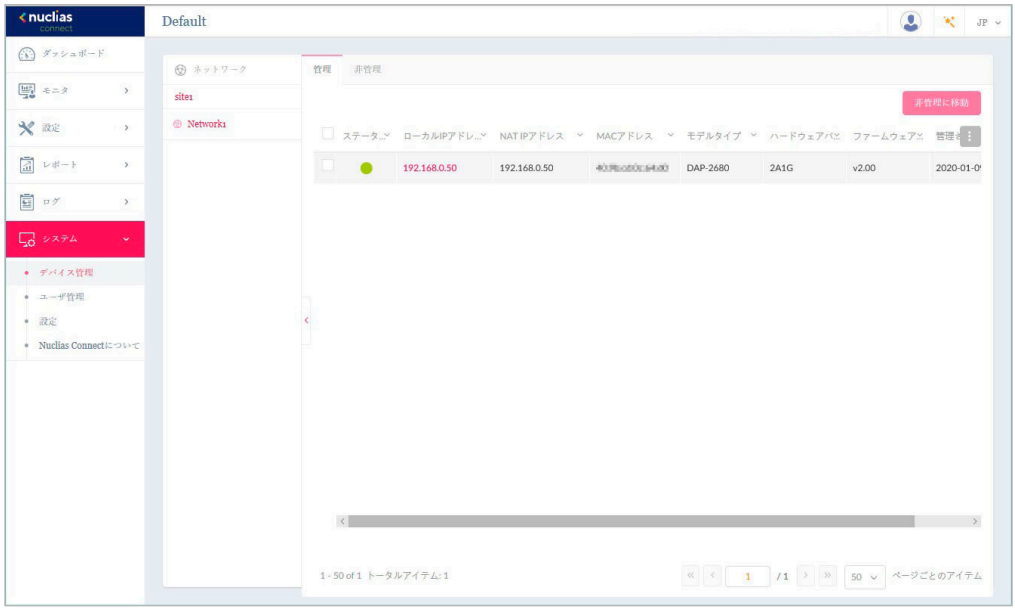

図 9-1　　デバイス管理 - 管理デバイス

「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。

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 をクリックし、「ユーザの編集」面画を表示します。「ユーザ名」、「パスワード」、「メールアドレス」、「権限」、「権限ステータス」、「設置場所」、「電話番号」、「説明」は、変更ページから編集できます。管理者アカウントは削除できません。また、管理者アカウントのユーザ名と権限の設定を変更することもできません。
ユーザ設定が完了したら、「保存」をクリックして確認するか、「キャンセル」をクリックして前のメニューに戻ります。

使用可能なユーザプロファイルは以下の通りです。

- 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。

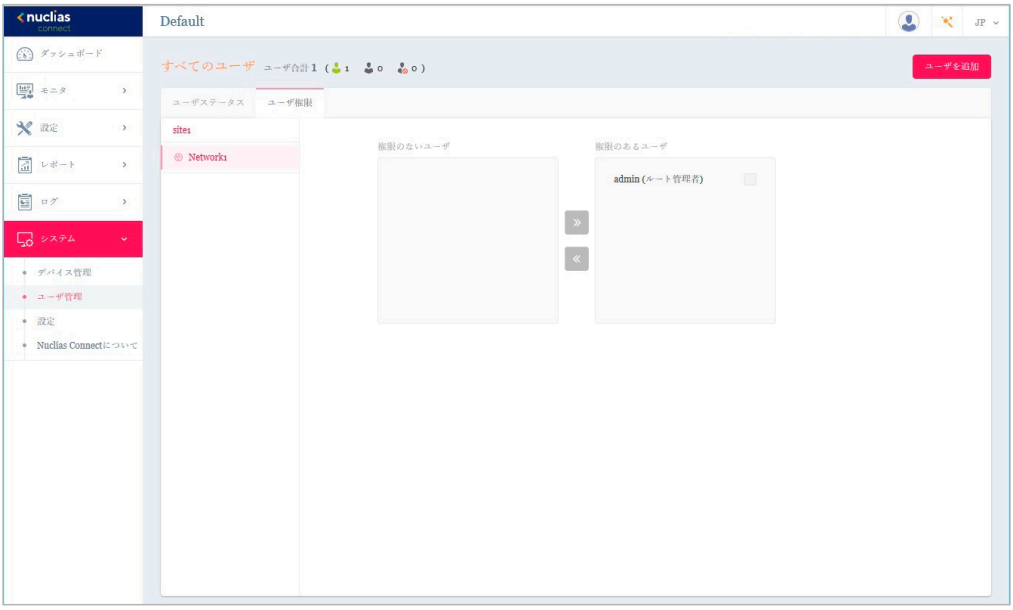

図 9-3　　ユーザ管理 - ユーザ権限

■ 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。

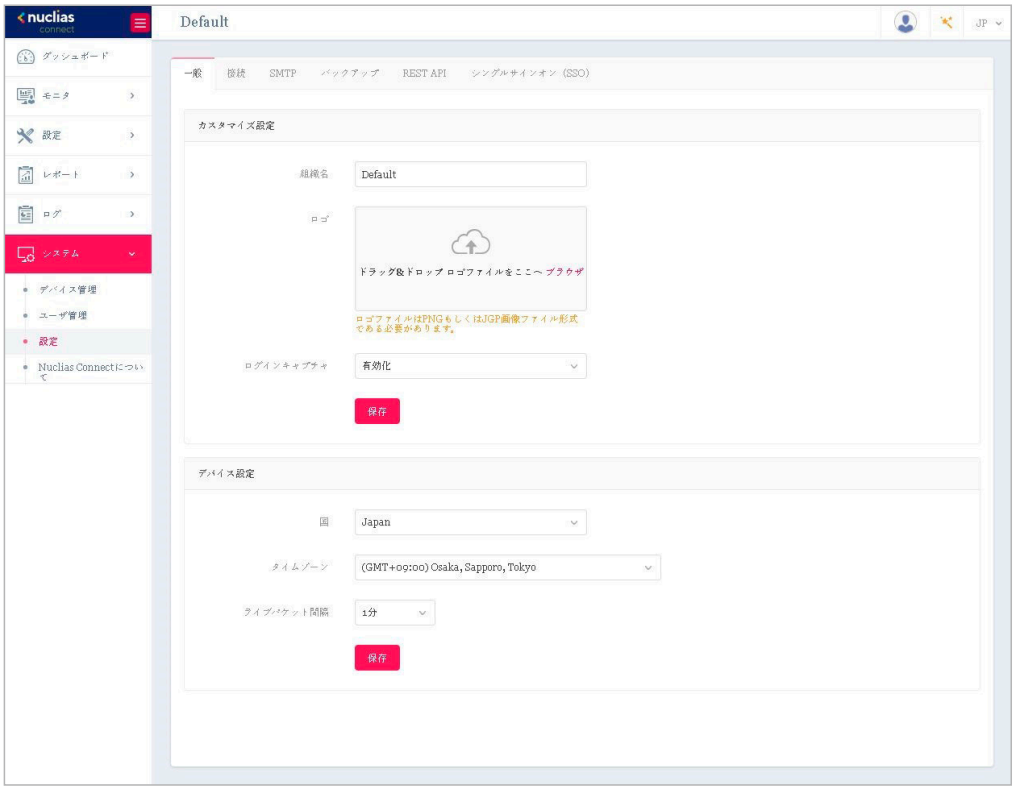

図 9-4　　システム - 一般

「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。
ロゴ	「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」

「保存」をクリックして設定を保存します。

接続

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

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

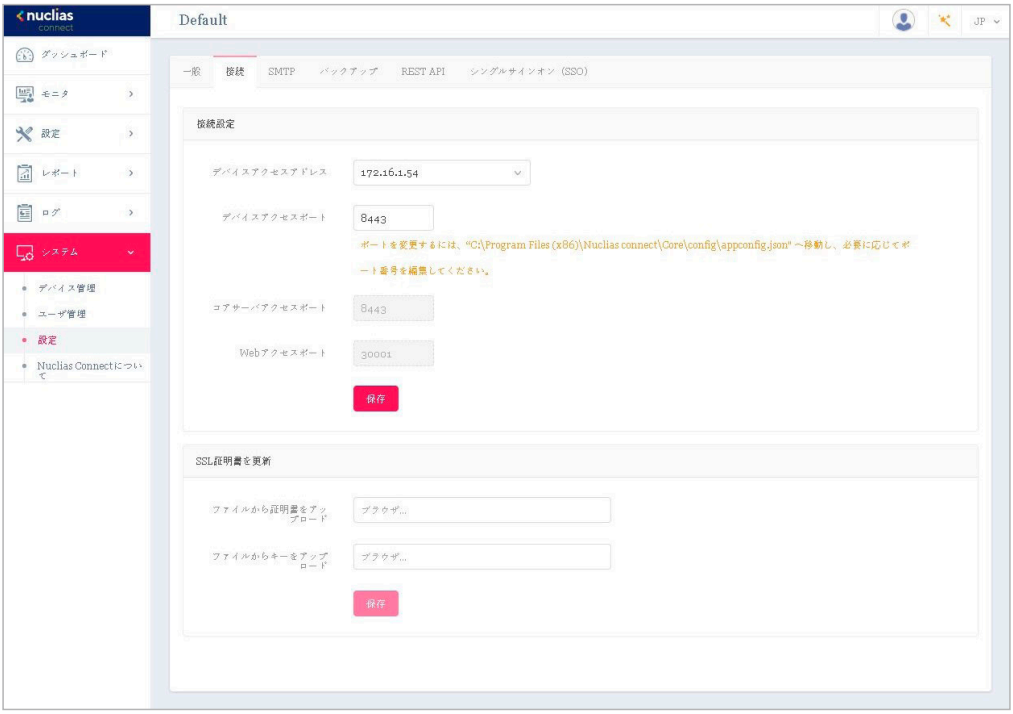

図 9-5　　システム - 接続

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

「保存」をクリックして設定を保存します。

SMTP

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

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

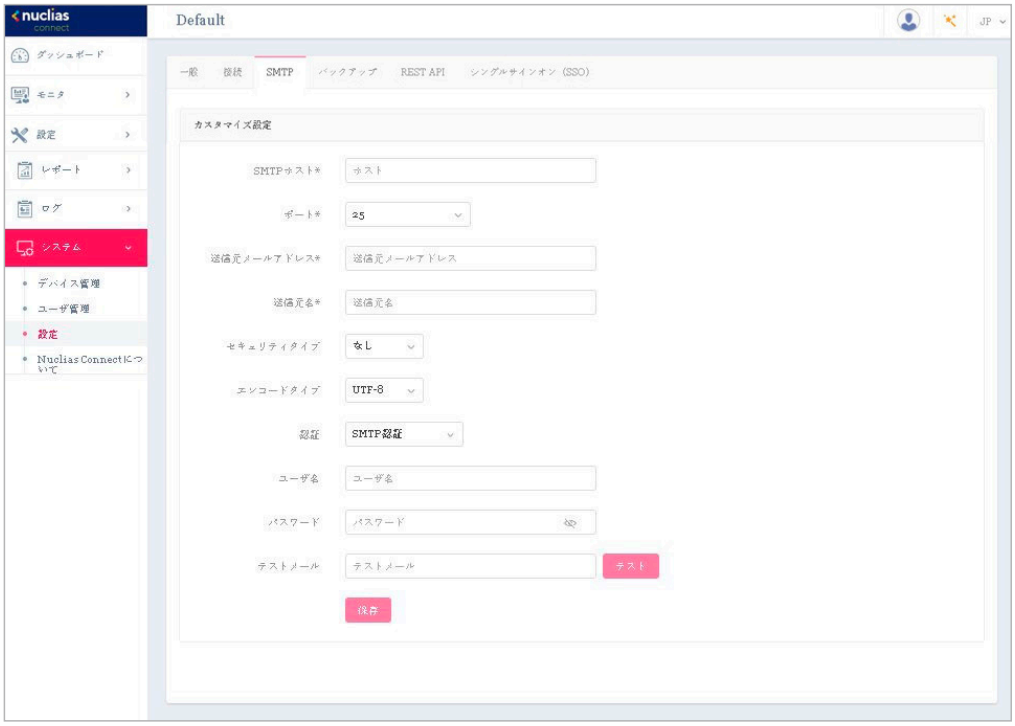

図 9-6　　システム - SMTP

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。

「保存」をクリックして設定を保存します。

バックアップ

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

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

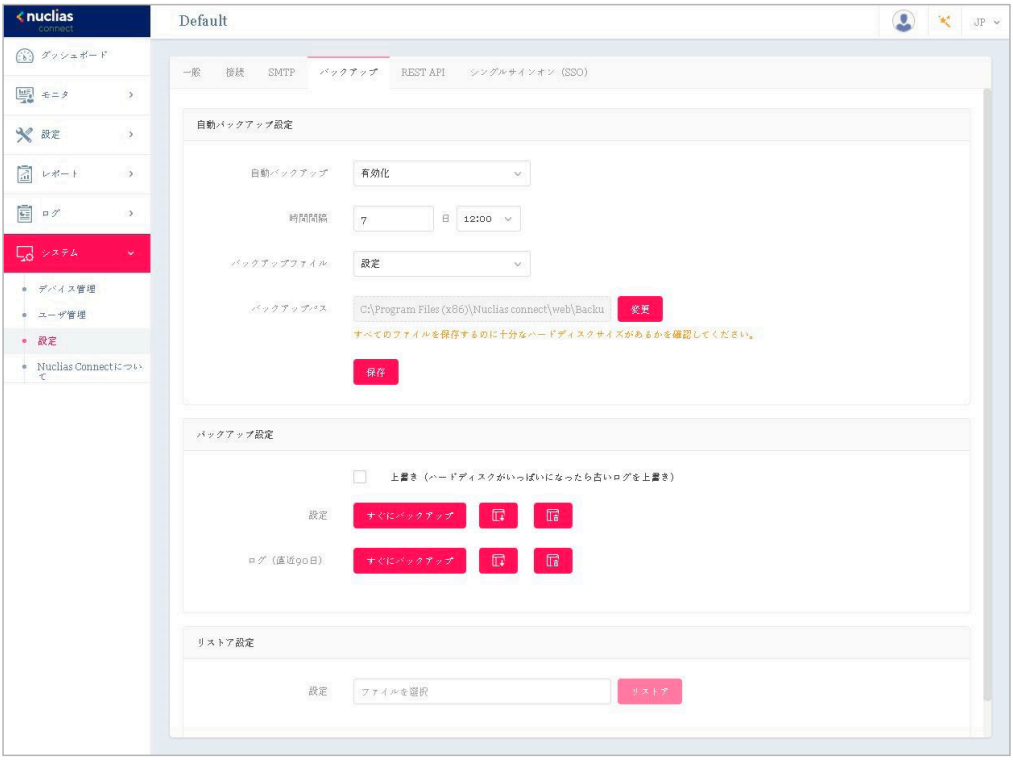

図 9-7　　システム - バックアップ

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。

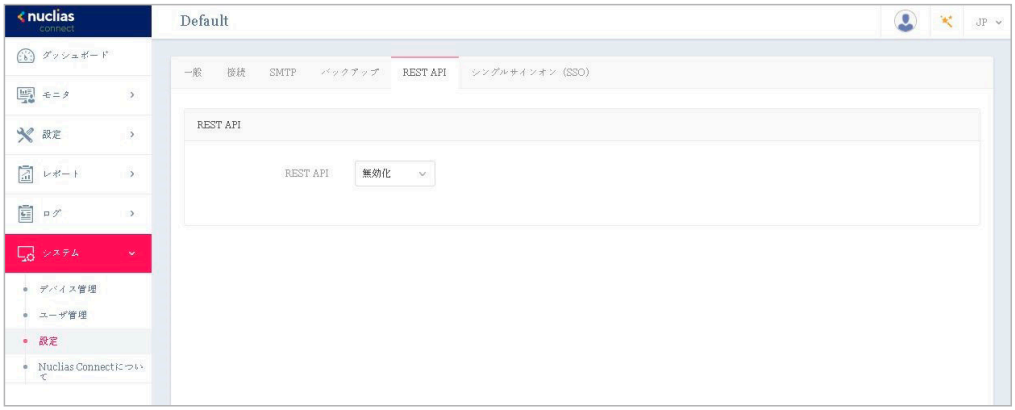

図 9-8　システム - REST API

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。

「コピー」をクリックして REST 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。

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

「保存」をクリックして設定を保存します。

Nuclias Connect 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。

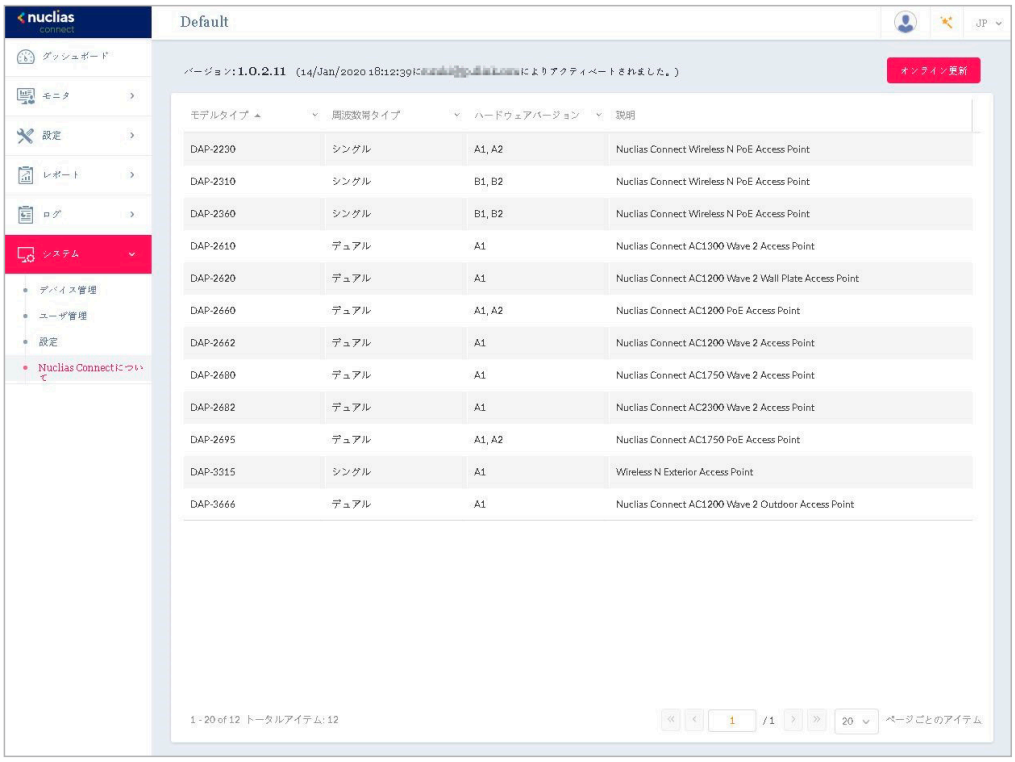

図 9-10　Nuclias Connect について

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）