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 のサポート
- 最大 1500AP 管理 / サーバ
- https エージェントを使用した NAT パススルー（NAT デバイスの後方にある複数の AP を管理可能）
- AP と Nuclias Connect 間のすべてのトラフィックを暗号化
- 日本語 GUI のサポート
- コンフィグレーション / ログのバックアップと復元
- スケジューリングによるプロファイル / ファームウェア更新
- Web による管理（HTTPS）
- Syslog サーバ※ 1
- 外部 Syslog サーバ※ 2
- 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 本機が管理しているデバイスから送信されるログを受信する Syslog サーバとしての機能となります。
※ 2 キャプティブポータルログのみ対応

ビジネス Wi-Fi 機能

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

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

推奨システム要件

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

項目	大規模環境	小規模環境
最大管理アクセスポイント数	1500 台	100 台
推奨 CPU	12 世代 Intel® Core ™ i7 プロセッサ以上	12 世代 Intel® Core ™ i5 プロセッサ以上
推奨 RAM	32G DDR3 以上	16G DDR3 以上
推奨ストレージ容量	4TB 以上	2TB 以上
イーサネット NIC	ギガビットイーサネットカード	ギガビットイーサネットカード
モニタ解像度	1080p	1080p
プラットフォーム（Windows）	Windows Server 2019（64-bit）	Windows 11 Professional（64-bit）
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

Nuclias Connect 対応機器

Nuclias Connect では以下の機器をサポートしています。

製品名	品番	ファームウェアバージョンの最小要件※
DAP-X2850	DAP-X2850/A1	R1.10r027
DAP-X2810	DAP-X2810/A1	R1.20r032
DAP-2680※1	DAP-2680/A1	R2.00B08r051
DAP-2610※1	DAP-2610/A1	R2.01B05r073
DAP-3666	DAP-3666/A1	R1.10b08r068

※ Nuclias Connect に対応したファームウェアバージョンにおいて CWM は利用できません。
※ 1 既にソフトウェアサポートは終了しています。

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）」および「第 3 章　Nuclias Connect の管理インタフェース（p.34）」を参照してください。
- **Nuclias Connect アプリケーション**：スタンドアロンの D-Link AP 製品への簡単な設定および展開、また、複数のサイトやネットワークの管理を可能にする無線アクセスポイント管理ツールです。詳細については、「Nuclias Connect アプリのセットアップ（p.22）」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、Nuclias Connect 関連コンポーネント全てアンインストールし、新規に Nuclias Connect をインストールする手順を推奨します。

Nuclias Connect のインストール

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。

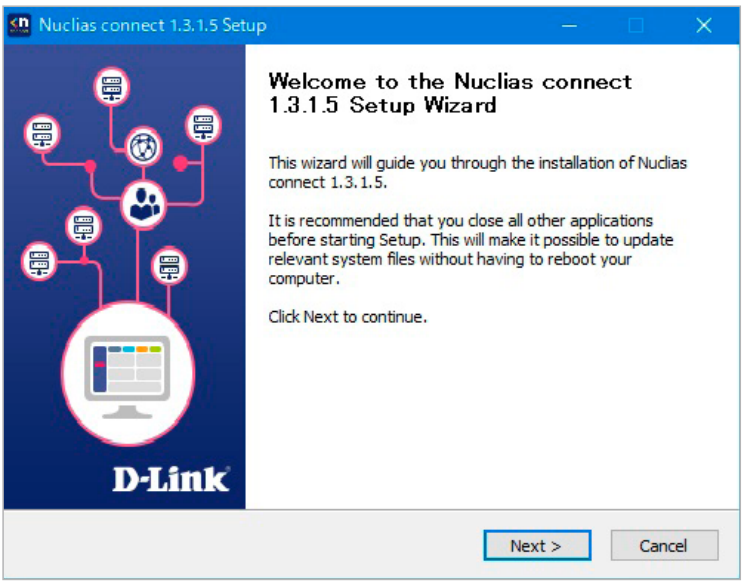


図 2-1　Nuclias Connect - セットアップウィザード

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。

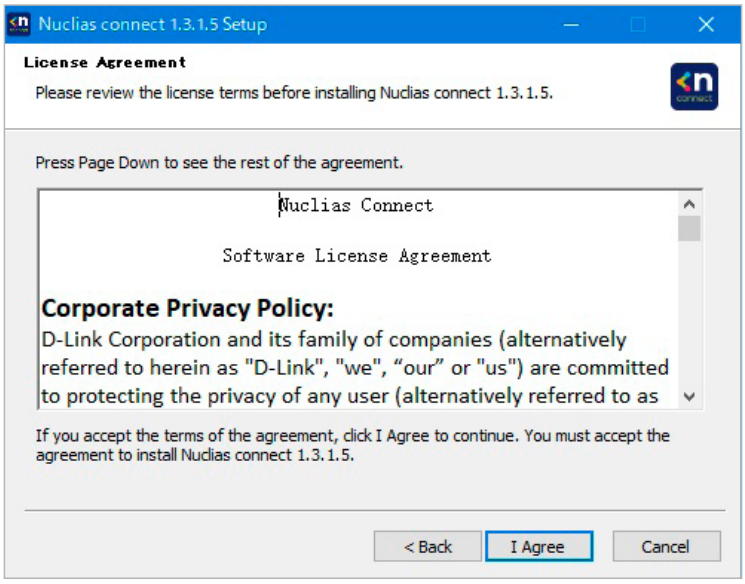


図 2-2　Nuclias Connect - 使用許諾

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

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

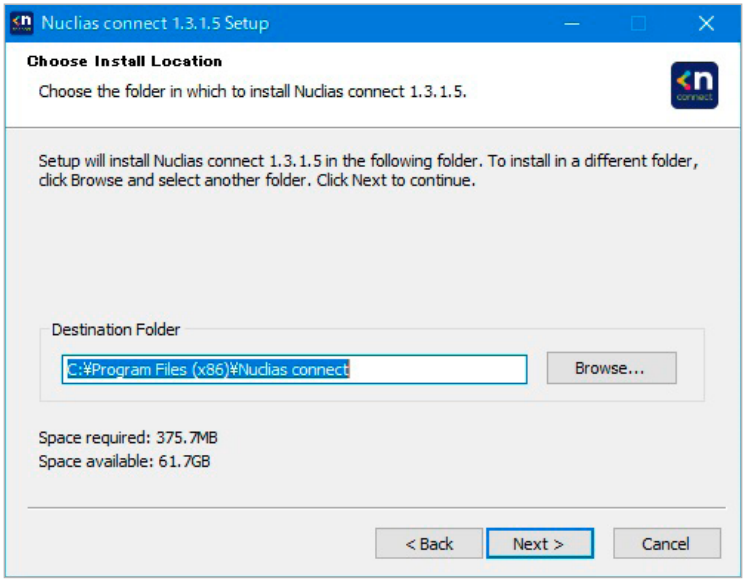


図 2-3　Nuclias Connect - インストールフォルダの指定

5. 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。

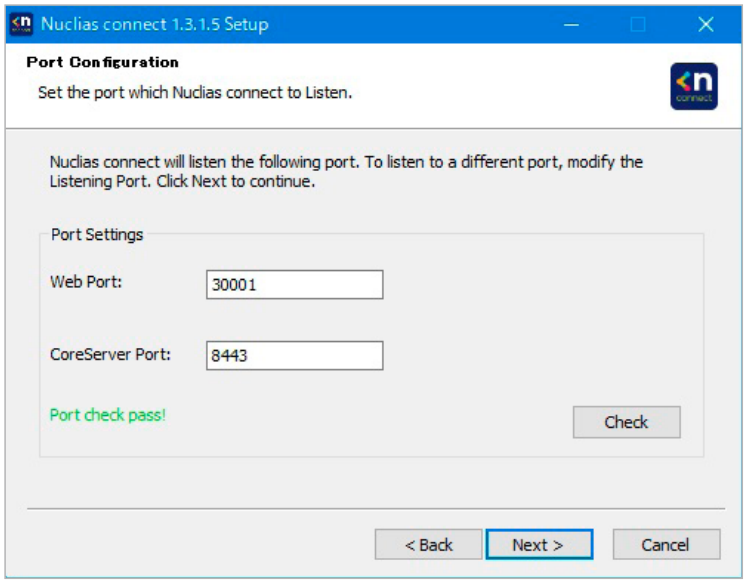


図 2-4　Nuclias Connect - ポート設定

6. 「Database Service Environment Check」画面が表示されます。ここでは、必要な PostgreSQL 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。「PostgreSQL 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、PostgreSQL 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 PostgreSQL を利用する場合は、「Use an existing PostgreSQL」、新規のサービスをインストールする場合は「Install a new PostgreSQL」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。

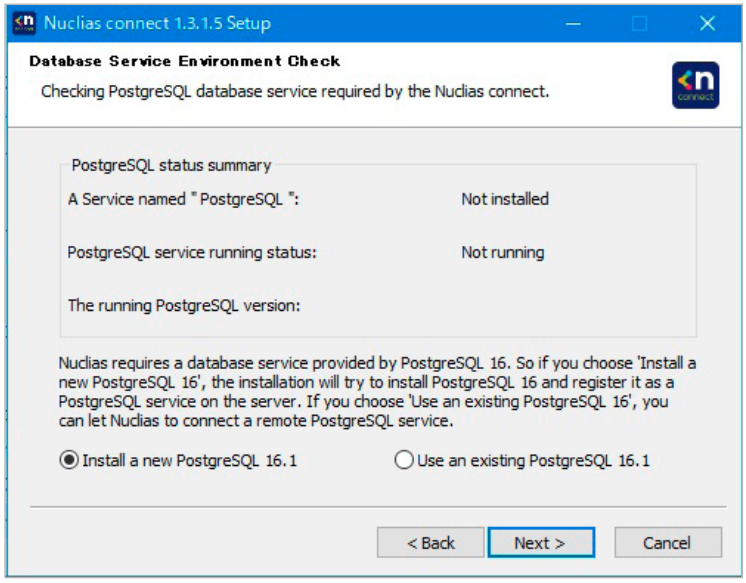


図 2-5　Nuclias Connect - PostgreSQL サービスステータスのチェック

7. 「PostgreSQL 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 PostgreSQL リスニングポート（デフォルト：5432）、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。

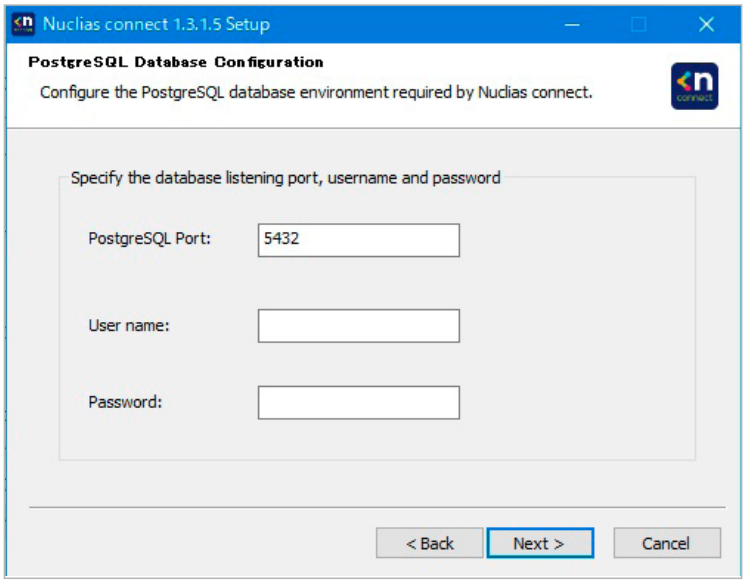


図 2-6　Nuclias Connect - PostgreSQL データベース設定

8. 「Warning messages」画面が表示されます。Npcap 利用に関する説明とライセンス条項を確認し、チェックボックスにチェックを入れます。
   ※ Nuclias Connect v1.3.1.5 では、Npcap v1.75 以上をインストールする必要があります。

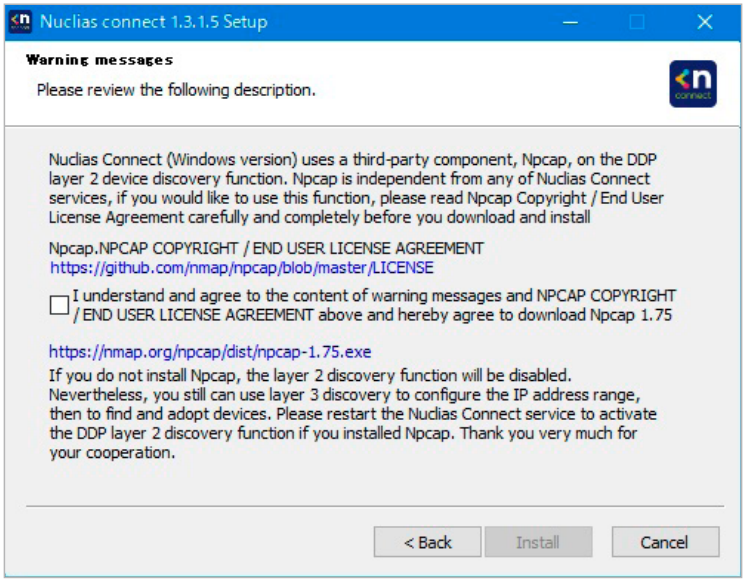


図 2-7　Nuclias Connect - Npcap に関するメッセージ

9. Npcap v1.75 ダウンロードリンク（https://nmap.org/npcap/dist/npcap-1.75.exe）から Nmap v1.75 のインストーラをダウンロードし、インストーラを実行します。

■ Npcap のインストール

10. Npcap セットアップウィザードが開始します。「I Agree」をクリックし、使用許諾に同意します。

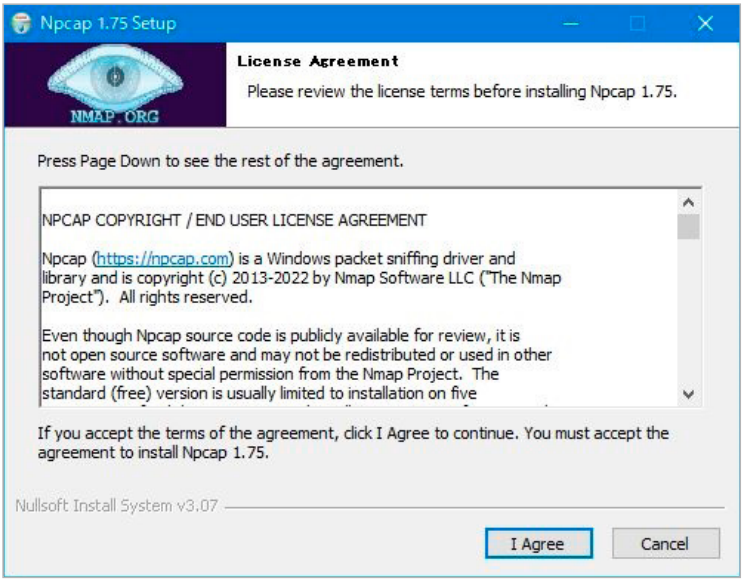


図 2-8　　Npcap - 使用許諾

11. デフォルトオプションのまま「Install」をクリックします。

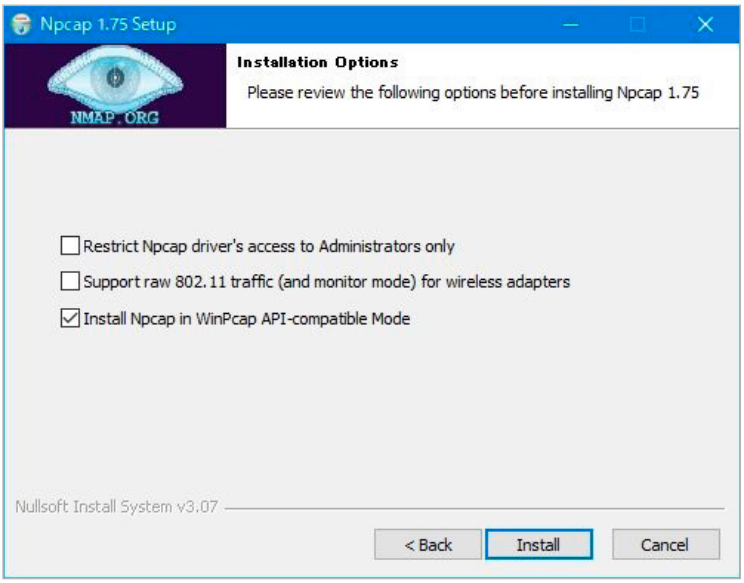


図 2-9　　Npcap - インストールオプション

12. インストール完了後、「Next」をクリックします。

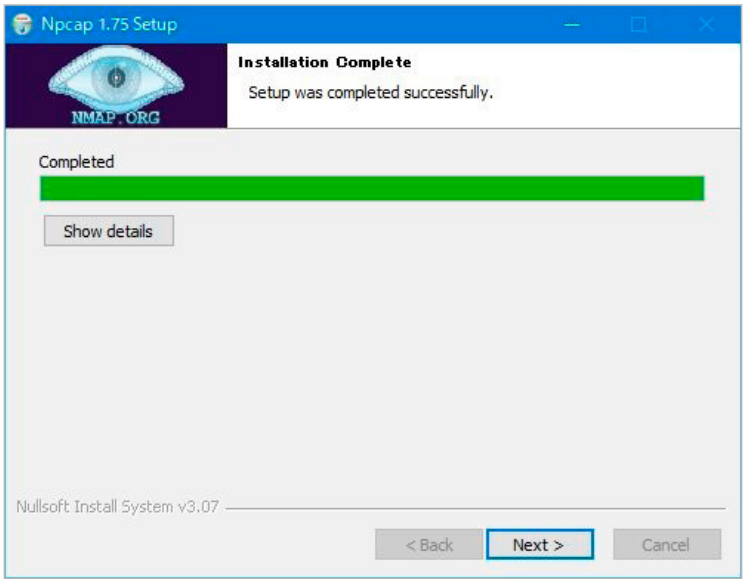


図 2-10　Npcap - インストール完了

13. 「Finish」をクリックしてウィザードを終了します

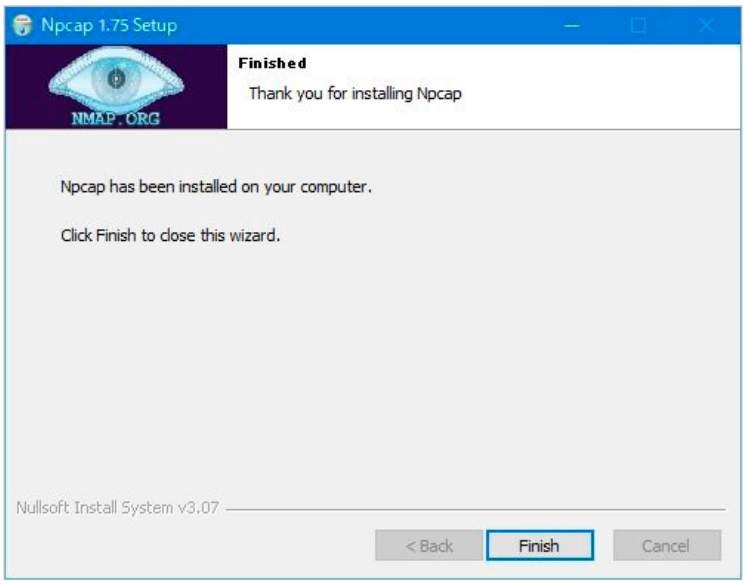


図 2-11　Npcap - ウィザード完了

14. Nuclias Connect セットアップウィザードに戻り、「Install」をクリックします。

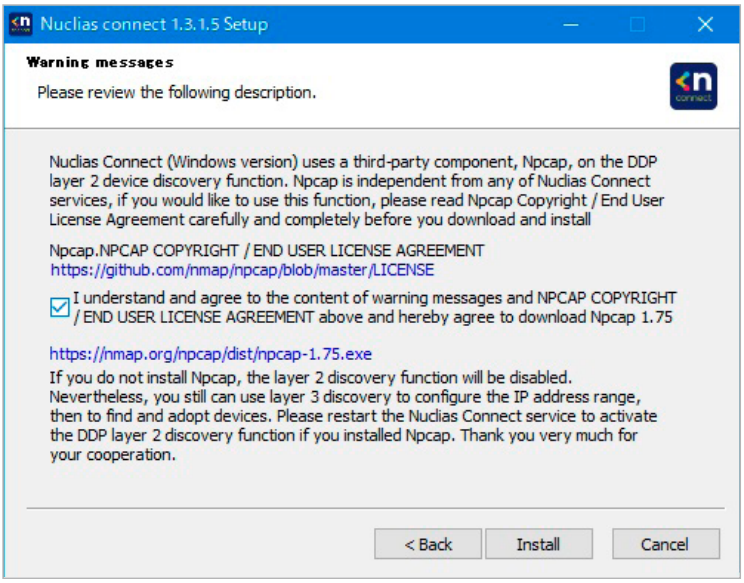


図 2-12　Nuclias Connect - Npcap に関するメッセージ

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

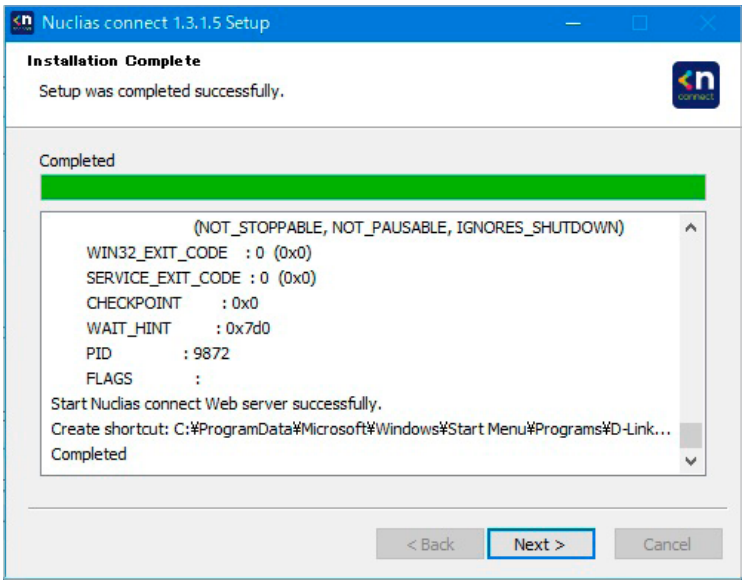


図 2-13　Nuclias Connect - インストール完了

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

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

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。「Finish」をクリックします。

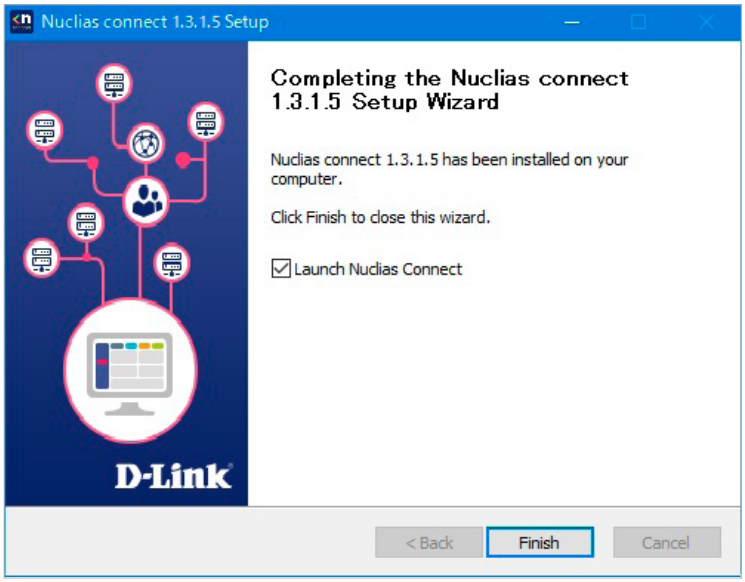


図 2-14　Nuclias Connect - セットアップウィザードの完了

17. 既定のブラウザで Nuclias Connect に接続されます。

図 2-15　Nuclias Connect への接続

参照 ソフトウェアインストール後の Nuclias Connect セットアップやログイン手順については、「Nuclias Connect オンライン登録への初回ログイン（p.16 ）」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。

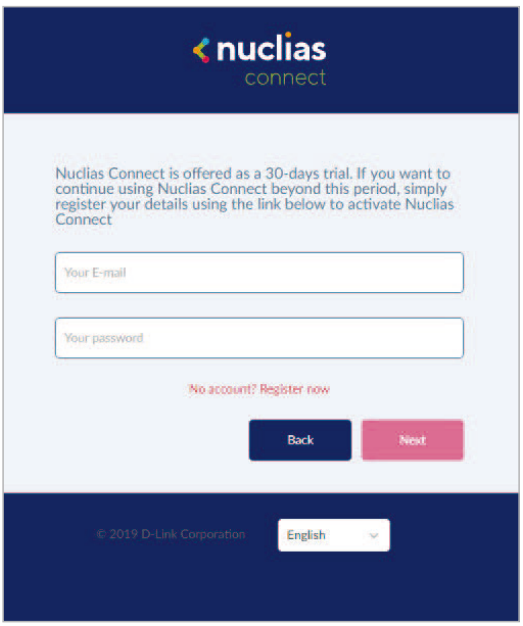


図 2-16　Nuclias Connect 初回ログイン

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

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ポリシーに同意します。アカウント作成ボタンが有効になります。

図 2-18　アカウント情報の入力

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

図 2-19　ログイン画面

Nuclias Connect へのログイン

1.　以下の方法で Nuclias Connect にアクセスします。

Web ブラウザから直接接続する方法

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

ソフトウェアから起動する方法

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。

Windows のスタートメニューから、**「D-Link Nuclias Connect」をクリックします。**

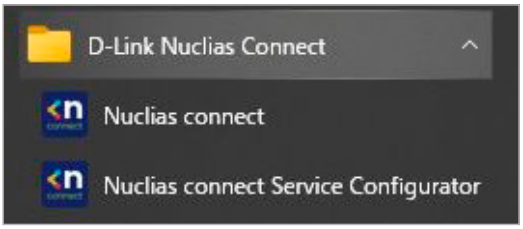


図 2-20　Windows ショートカットメニュー

- Nuclias connect をクリックして既定の Web ブラウザで Nuclias Connect インタフェースを開きます。
- または、Nuclias connect Service Configurator をクリックして Nuclias Connect Setup 画面を起動し、「Launch a Browser to Manage the Network」をクリックします。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。

注意　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。

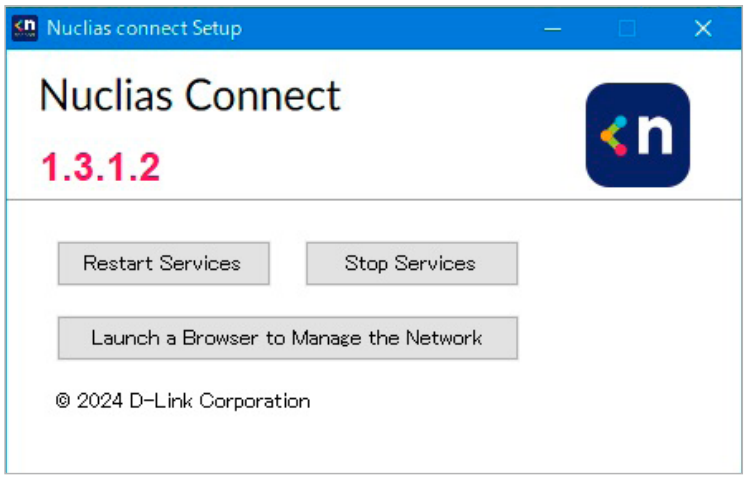


図 2-21　Nuclias connect Setup

■　サービスの有効化 / 無効化

Nuclias Connectを管理するには、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。

2. ログイン画面でユーザ名とパスワードを入力します。また、画面に表示されている CAPTCHA コードを入力します。

図 2-22　アカウント情報入力

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

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

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

図 2-23　パスワードの変更

注意　一般的な単語や名前は使用しないでください。

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

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を変更した場合は、Nuclias Connect Core サーバを再起動する必要があります。

図 2-24　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。

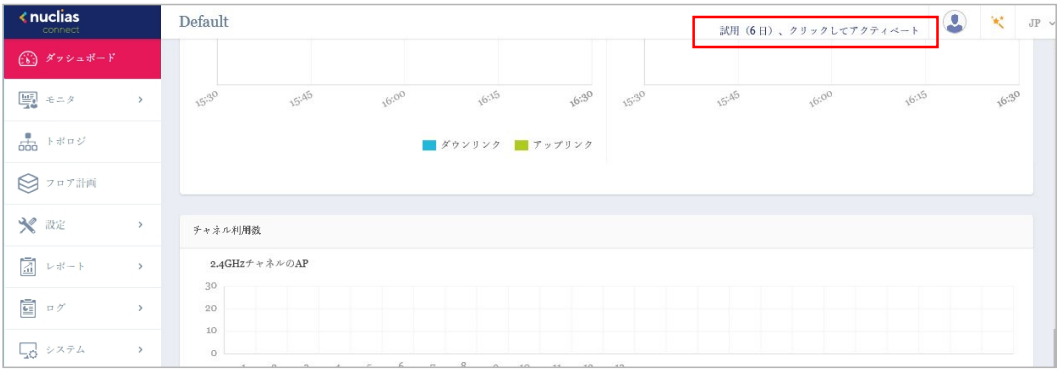


図 2-25　アクティベート

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

図 2-26　アカウント情報の入力

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

図 2-27　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 2-28　アクティベーションの完了

Nuclias Connect アプリのセットアップ

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

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

ネットワークプロファイルのエクスポート

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

参照 Nuclias Connect 管理インタフェースから同一セグメント内のデバイスを検出する場合、本手順は不要です。ネットワークおよびデバイスの検出手順については、「ネットワークの追加（p.71 ）」を参照してください。

1. **設定 > プロファイルを作成**の順にクリックします。
2. 「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。

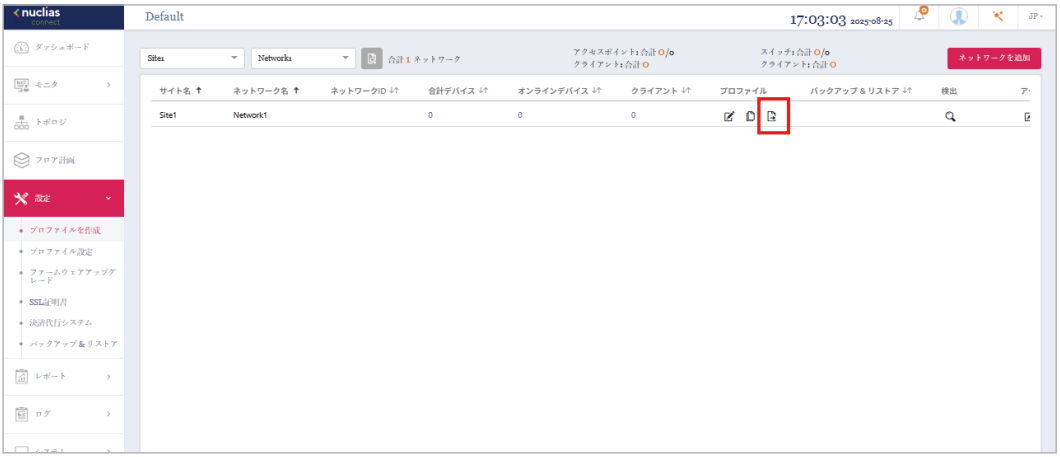


図 2-29　設定 - プロファイルを作成

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

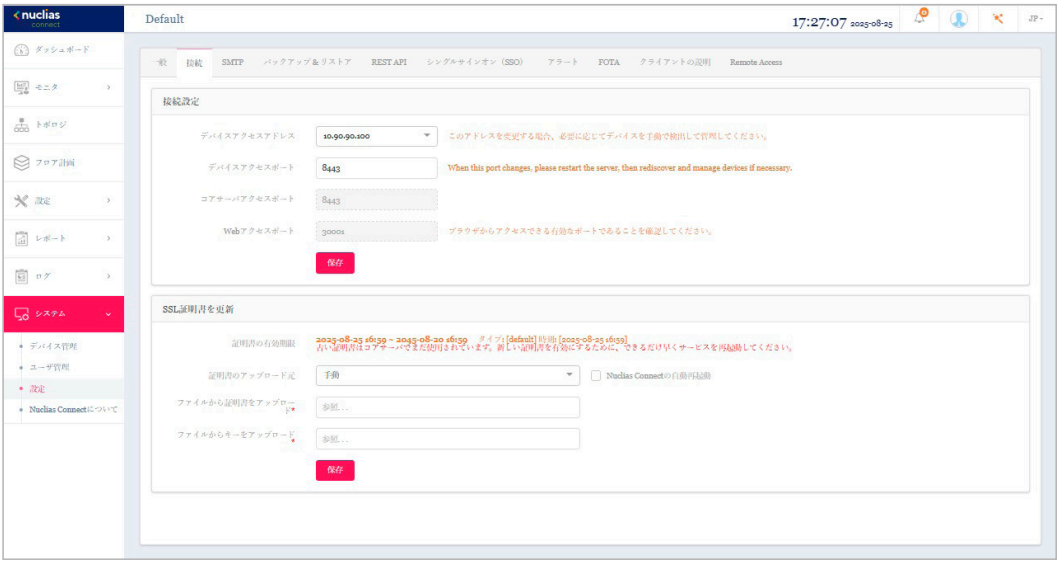


図 2-30　システム - 設定 - 接続タブ

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

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

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

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

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

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

クイックセットアップ

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

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

図 2-31　Nuclias Connect アプリ（iOS）

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

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

ステップ 1：プロビジョニングプロファイルの選択

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

図 2-32　ステップ 1 - プロファイルのダウンロード

4. ⊕「＋」アイコンをクリックし、Nuclias Connect サーバへの接続情報を入力してログインします。接続に必要な入力項目については、27 ページの「Nuclias Connect サーバへの接続」を参照してください。
5. サイトとネットワークを選択し、「ダウンロード」をタップしてプロファイルをダウンロードします。
6. 「ダウンロードを続ける」または「戻る」をタップし、「ステップ 1」の画面に戻ります。
7. プロビジョニングプロファイルが選択されている状態で「次へ」をタップします。

図 2-33　ステップ 1 - プロビジョンプロファイルの選択

■ ステップ 2：アクセスポイント検出範囲の定義

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

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

図 2-34　アクセスポイント検出範囲の定義

■ ステップ 3：アクセスポイントへのプロファイル適用

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

図 2-35　アクセスポイントの選択

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

図 2-36　アクセスポイントへのログイン

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

図 2-37　プロファイルの適用

Nuclias Connect サーバへの接続

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

1. 「Nuclias Connect」をタップします。

図 2-38　Nuclias Connect アプリ - トップ画面

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

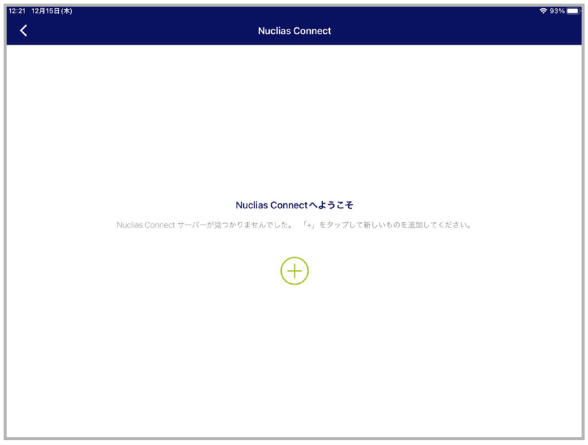


図 2-39　Nuclias Connect へようこそ画面

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

図 2-40　新規サーバへのログイン画面

以下の項目が表示されます。

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

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

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

図 2-41　ダッシュボード

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

図 2-42　Nuclias Connect サーバのリスト

スタンドアロンアクセスポイントの検出と設定

■ アクセスポイントの検出

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

1. 「スタンドアロンアクセスポイント」をタップします。

図 2-43　Nuclias Connect アプリ - トップ画面

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

図 2-44　アクセスポイントの検出範囲

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

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

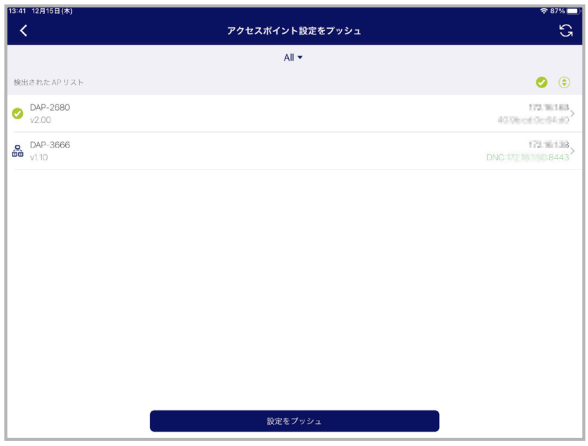


図 2-45　プロファイルの配信

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

図 2-46　アクセスポイントへのログイン

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

「IP 情報」タブには以下の項目が表示されます。

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

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

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

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

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

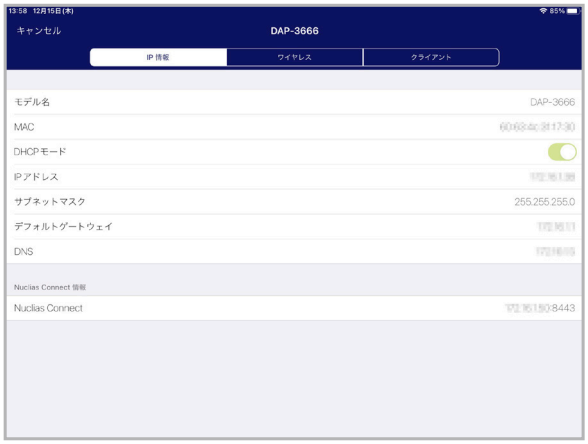


図 2-47　IP 情報の設定

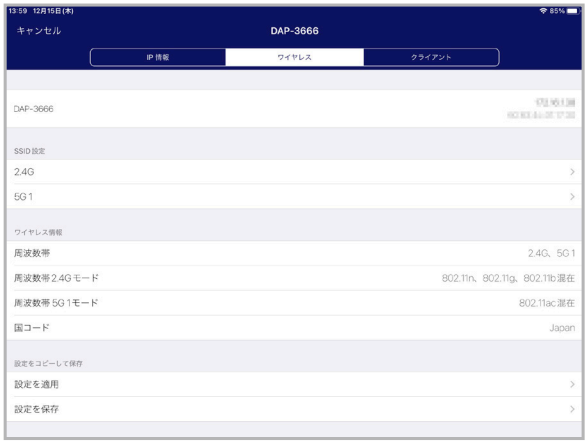


図 2-48　ワイヤレス設定

ネットワークプロファイルの削除

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

1. 左上のメニューをタップします。

図 2-49　Nuclias Connect アプリ - トップ画面

2. 「AP プロビジョニングプロファイル」を選択します。

図 2-50　Nuclias Connect アプリ - メニュー項目

3. 右上の削除ボタン（⊖）をタップします。

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

図 2-51　Nuclias Connect アプリ - プロファイル選択

管理対象アクセスポイントの確認

アクセスポイント接続を確認するには、以下の手順を実行します。

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

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

図 2-52　モニタ - アクセスポイント - アクセスポイント

ファームウェアのアップロード

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

1. **設定 > ファームウェアアップグレード**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 AP モデルを表示します。
2. 「ファームウェアの手動アップグレード」タブをクリックします。
3. 対象デバイスの「アクション」欄で「変更」ボタンをクリックし、アップロードするファームウェアを選択します。

図 2-53　設定 - ファームウェアアップグレード - ファームウェアの手動アップグレード

4. 以下のいずれかの手順でファームウェアを適用します。

即時適用：

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

指定日時に適用：

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

第 3 章　Nuclias Connect の管理インタフェース

Nuclias Connect への接続

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。

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

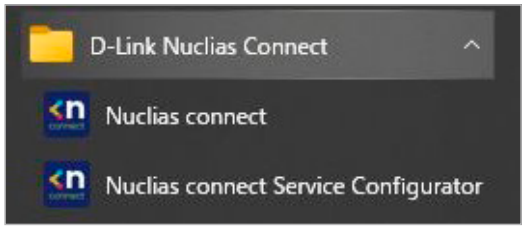


図 3-1　Nuclias Connect アプリケーション

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

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

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

図 3-2　Nuclias Connect へのログイン

注意　デフォルトでは、ユーザ名とパスワードは admin です。日本語を含む複数の言語がサポートされています。

ウィザード

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

1. 画面右上の をクリックして、ウィザードを開始します。

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

図 3-3　ウィザード - システム設定

2. 「ネットワークを追加」画面が表示されます。

図 3-4　ウィザード - ネットワークを追加

3. 「サイト」ドロップダウンメニューから既存のサイトを選択するか、「新しいサイト」を選択し、空のフィールドにサイトの名前を入力します。
4. 「ネットワーク」フィールドに新しいネットワークを識別する名前を入力し、「次へ」をクリックします。前の画面に戻るには「戻る」をクリック、ウィザードを中止するには「キャンセル」をクリックします。

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

補足　スイッチ製品は未サポートです。

図 3-5　ウィザード - ネットワークの設定

図 3-6　ウィザード - ネットワークの設定（アクセスポイント）

6. 「デバイスを検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを検出・表示します。

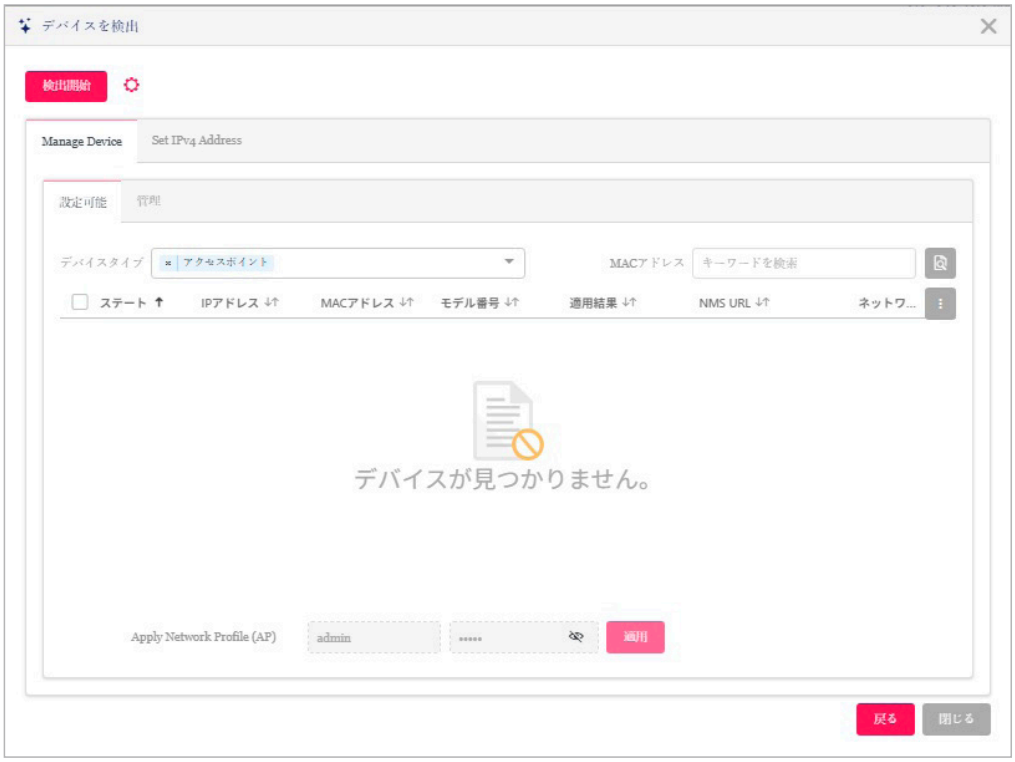


図 3-7　ウィザード - デバイスを検出

検出範囲を指定する場合は、 アイコンをクリックし、「ネットワーク検出設定」画面で検出範囲を設定します。

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。

図 3-8　ウィザード - ネットワーク検出設定

7. 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」タブでは、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ができます。

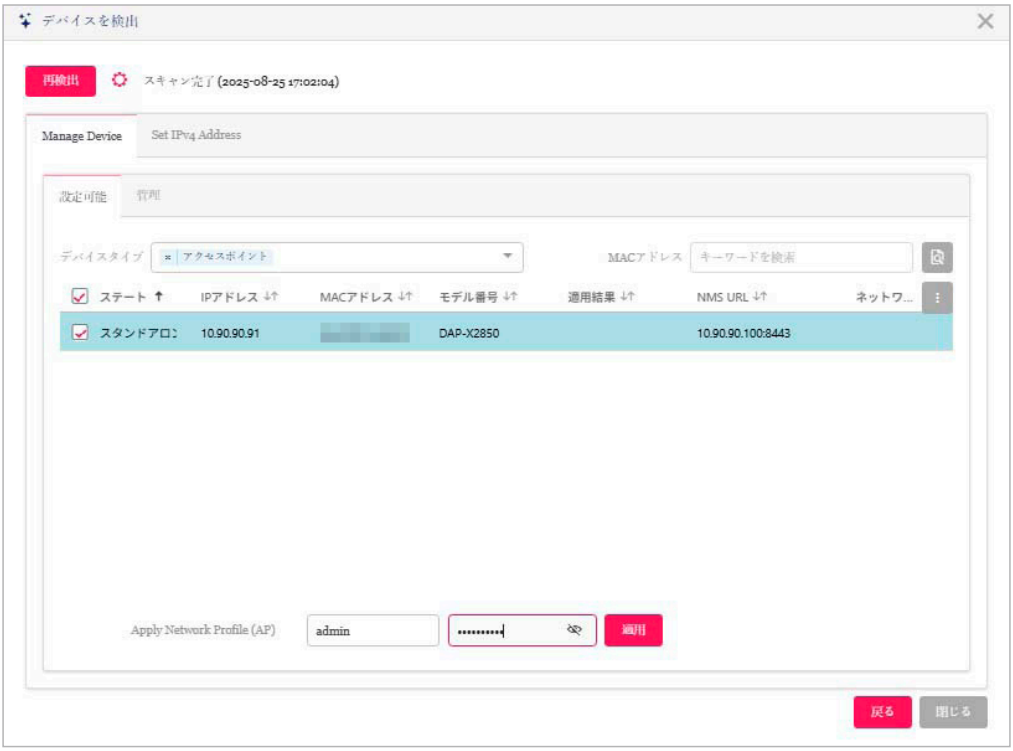


図 3-9　ウィザード - デバイスを検出

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

補足 「Set IPv4 Address」設定は未サポートです。

8. 右上の「×」または「閉じる」ボタンをクリックして画面を閉じます。

ユーザプロファイル

管理者のアカウント情報を設定します。

個人情報

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

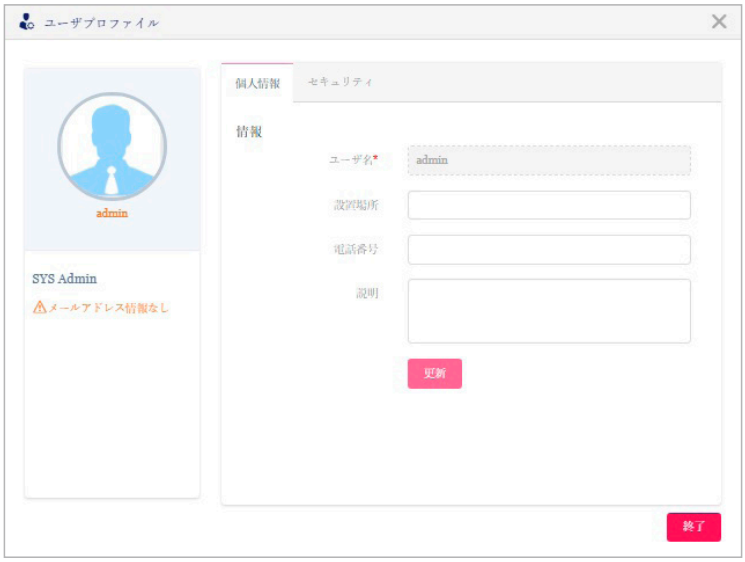


図 3-10　ユーザプロファイル - 個人情報

「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 3-11　ユーザプロファイル - セキュリティ

パスワードおよびメールアドレスを設定・変更することができます。
パスワードを変更する場合は、「パスワード」に現在のパスワードを入力し、「新しいパスワード」「パスワード確認」に新しいパスワードを入力します。

管理インタフェースからのログアウト

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

第 4 章　ダッシュボード

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

補足　スイッチは未サポートです。

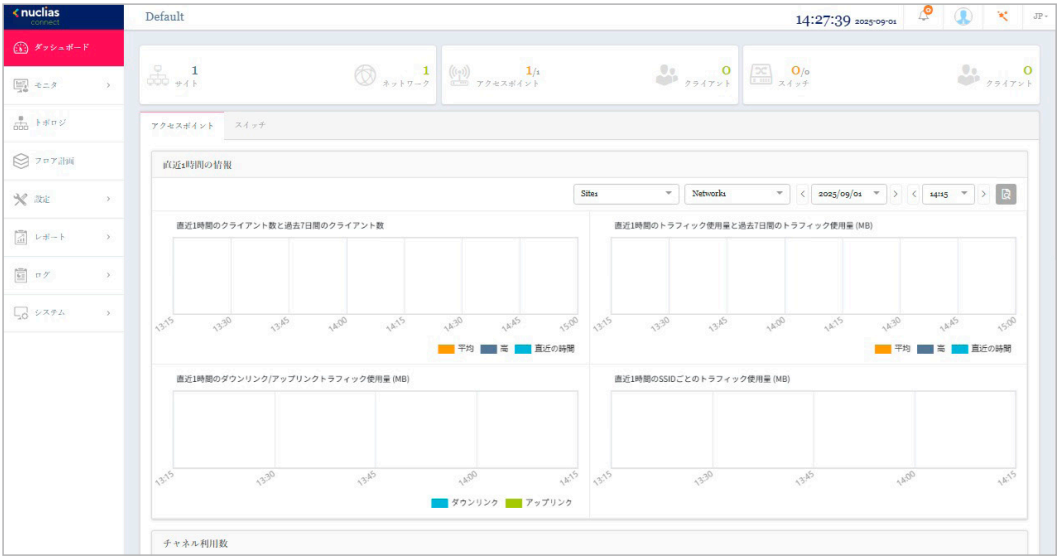


図 4-1　　ダッシュボード

画面上部の統計情報には以下の項目が表示されます。

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

「アクセスポイント」タブには以下の項目が表示されます。

項目	説明
直近 1 時間の情報	以下の履歴情報を表示します。表示するサイト / ネットワークおよび期間を指定することができます。 • 直近 1 時間のクライアント数と過去 7 日間のクライアント数 • 直近 1 時間のトラフィック使用量と過去 7 日間のトラフィック使用量（MB） • 直近 1 時間のダウンリンク / アップリンクトラフィック使用量（MB） • 直近 1 時間の SSID ごとのトラフィック使用量（MB）
チャネル利用数	2.4GHz/5GHz/6GHz 帯域のチャネルごとのアクセスポイントの台数を表示します。
直近のイベント	最新イベントの簡易的なログを表示します。 表示するサイト / ネットワークを指定することができます。

「スイッチ」タブには以下の項目が表示されます。

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

第 5 章　モニタ

補足　スイッチ製品は未サポートです。

アクセスポイント

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

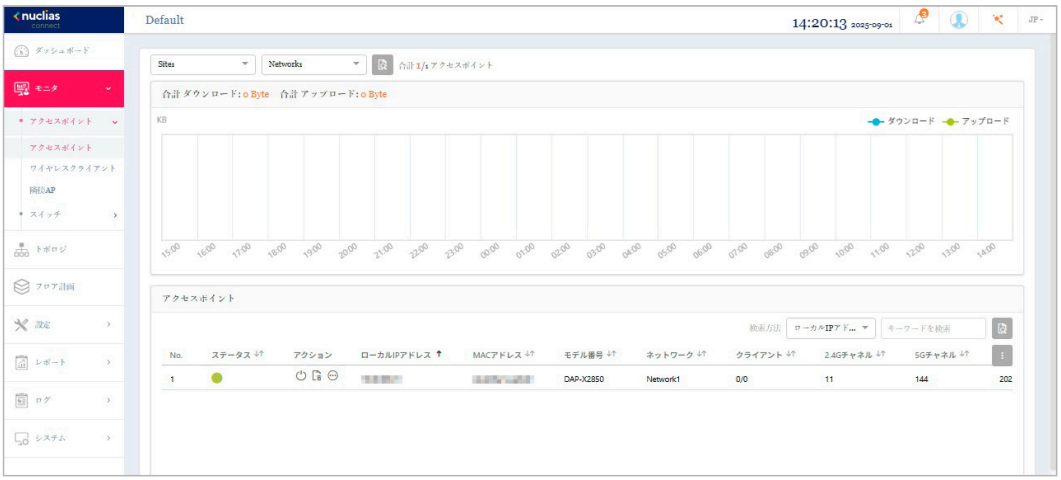


図 5-1　モニタ - アクセスポイント - アクセスポイント

■ 対象範囲の指定 / デバイスの検索

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

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

■ レポート項目

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

- ステータス
- ローカル IP アドレス
- ローカル IPv6 アドレス
- NAT IP アドレス
- MAC アドレス
- モデル番号
- ファームウェアバージョン
- ハードウェアバージョン
- 名前
- 設置場所
- サイト
- ネットワーク
- ネットワーク ID
- クライアント
- 2.4G チャネル
- 5G チャネル
- 6G チャネル
- 2.4G 出力
- 5G 出力
- 6G 出力
- ダウンロード
- アップロード
- トラフィック使用量
- トラフィック使用率（%）
- CPU 使用率（%）
- メモリ使用率（%）
- 最終更新情報
- 稼働時間

アクセスポイント - デバイス詳細

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

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

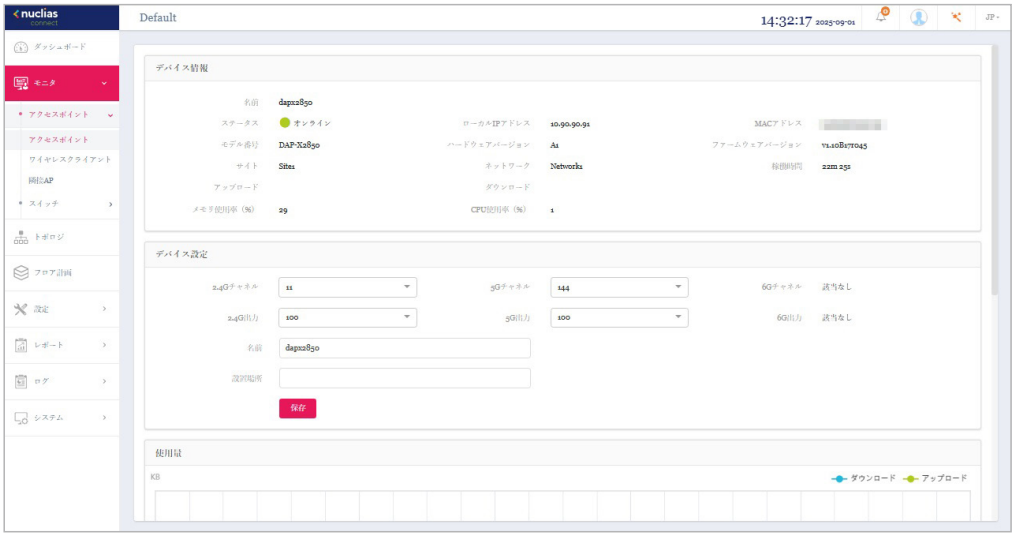


図 5-2　モニタ - アクセスポイント - アクセスポイント - デバイス詳細

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

アクセスポイント - ワイヤレスクライアント

接続しているクライアント

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

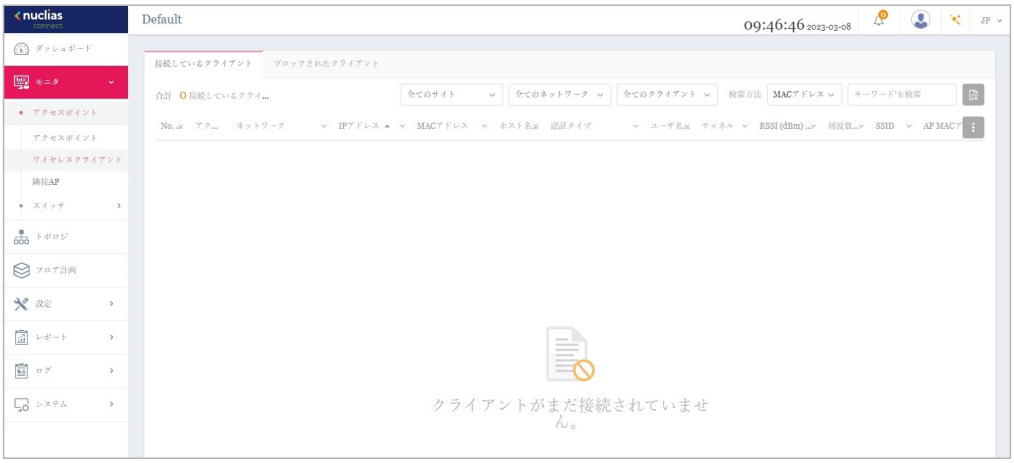


図 5-3　　モニタ - アクセスポイント - ワイヤレスクライアント（接続しているクライアント）

■ 対象範囲の指定 / デバイスの検索

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

- をクリックしてクライアントをブロックします。

■ レポート項目

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

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

ブロックされたクライアント

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

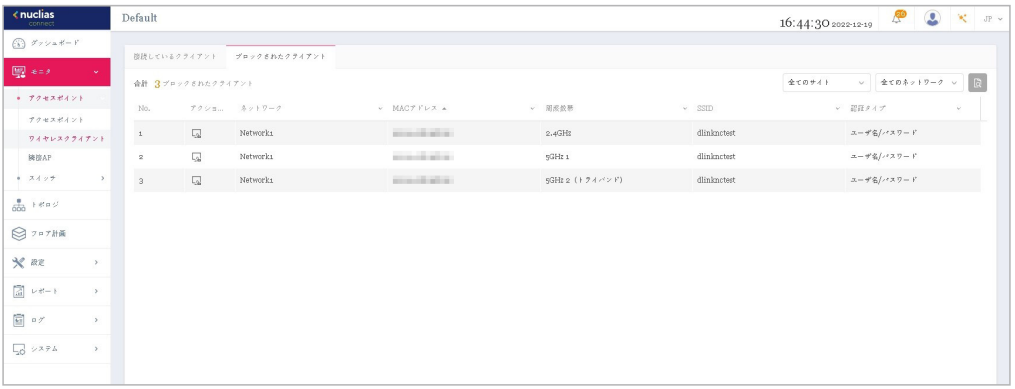


図 5-4　　モニタ - アクセスポイント - ワイヤレスクライアント（ブロックされたクライアント）

■ 対象範囲の指定

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

- をクリックしてクライアントのブロックを解除します。

■ レポート項目

ブロックされた各無線クライアントについて、以下の項目が表示されます。

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

アクセスポイント - 隣接 AP

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

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

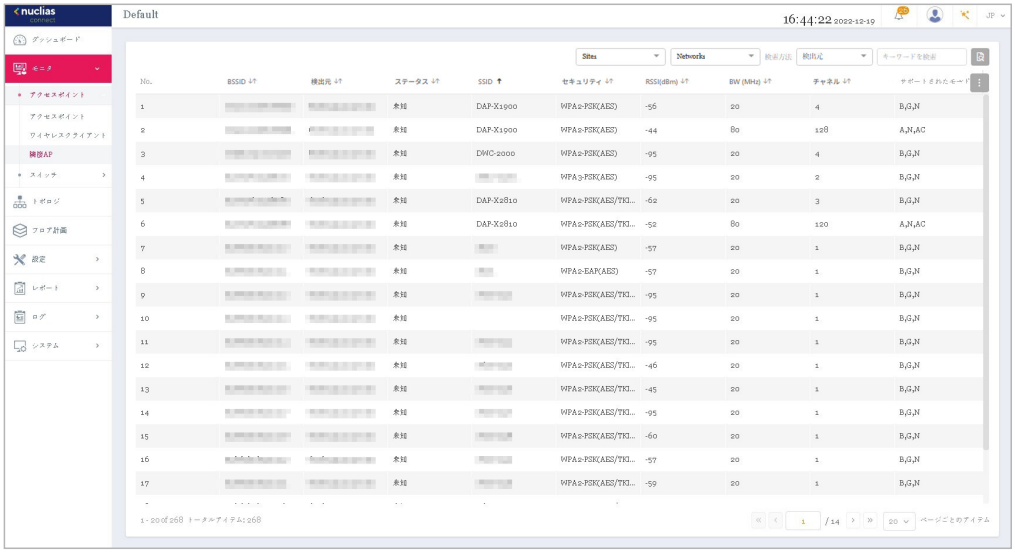


図 5-5　モニタ - アクセスポイント - 隣接 AP

■ 対象範囲の指定 / デバイスの検索

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

以下の項目が表示されます。表示項目を変更するには、をクリックします。

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

補足　「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140 ）」をご確認ください。

スイッチ

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

補足　スイッチ製品は未サポートです。

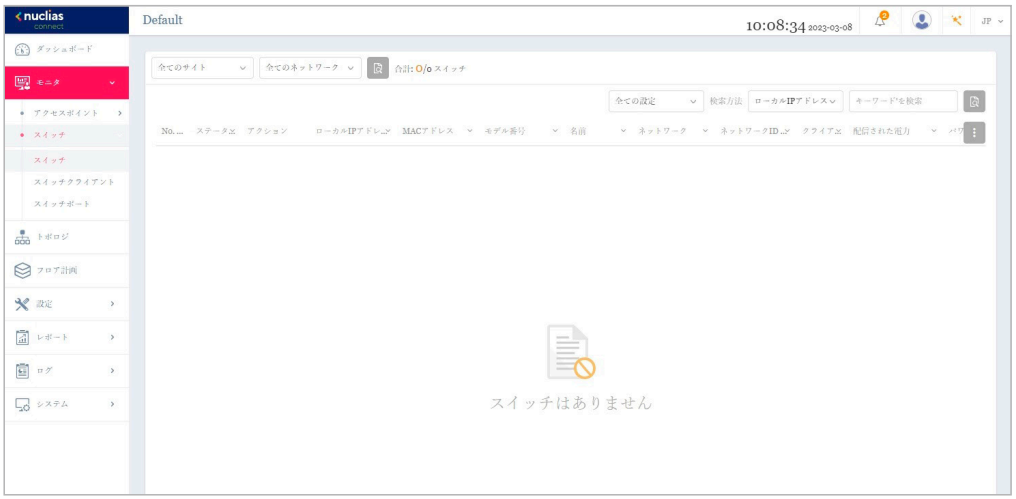


図 5-6　モニタ - スイッチ - スイッチ

■ 対象範囲の指定 / デバイスの検索

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

■ デバイスに対する操作

アクション欄で以下の操作を実行できます。

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

■ レポート項目

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

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

主要な項目の説明は以下の通りです。

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

項目	説明
ポート	スイッチのポートの総数を表示します。 ポートの数をクリックすると、「スイッチポート」画面に遷移します。
使用中の設定	設定モード（プロファイル / スタンドアロン）を表示します。 • プロファイル：プロファイルモードのデバイスは、プロファイル内の同じ設定を共有します。 • スタンドアロン：デバイス個別の設定があり、プロファイルの影響を受けることはありません。
最終更新情報	スイッチが最後に接続された時刻を表示します。
稼働時間	スイッチが再起動してから経過した起動時間を表示します。

スイッチ - デバイス詳細

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

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

基本タブ

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

補足　スイッチ製品は未サポートです。

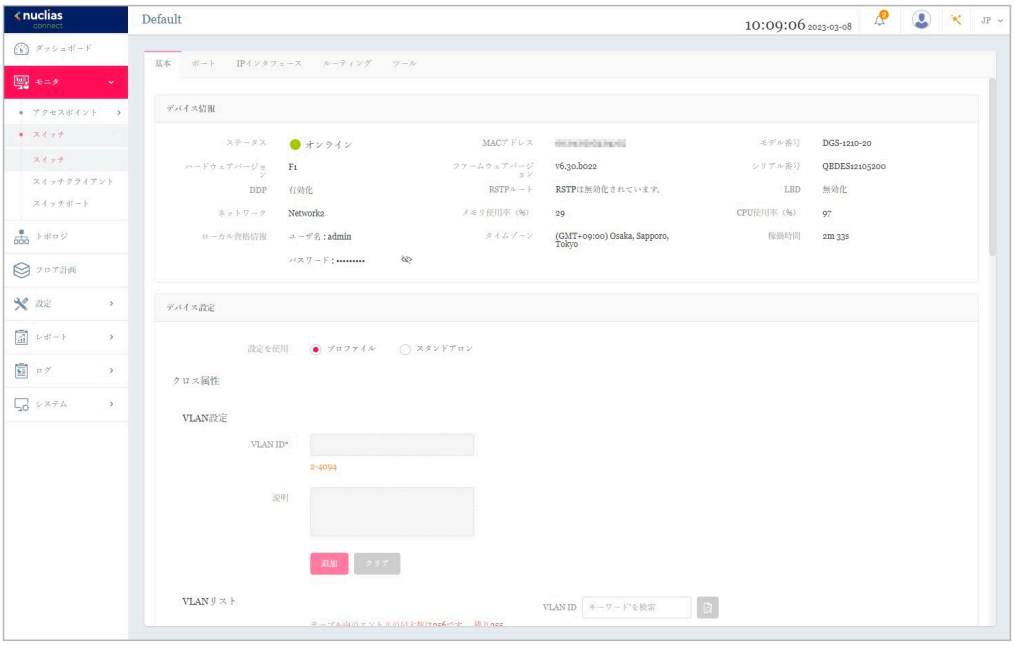


図 5-7　モニタ - スイッチ - スイッチ - デバイス詳細 - 基本タブ

デバイス情報

「デバイス情報」セクションには、以下の項目が表示されます。

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

スイッチの機能に関する項目は、以下の通りです。

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

デバイス設定

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

■ VLAN 設定

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

図 5-8　VLAN 設定

VLAN を作成する場合、以下の手順を実行します。

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

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

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

■ IGMP スヌーピング

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

図 5-9　IGMP スヌーピング設定

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

■ **アンクロス属性**

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

図 5-10　アンクロス属性

(1)　「名前」「設置場所」を入力します。

(2)　ドロップダウンメニューから「STP ブリッジプライオリティ」を選択します。

■ **設定の適用**

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

IP 接続

「IP 接続」セクションでは、プライマリ接続を設定できます。

図 5-11　IP 接続

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

CPU 使用率

「CPU 使用率」セクションには、CPU 使用率のグラフが表示されます。

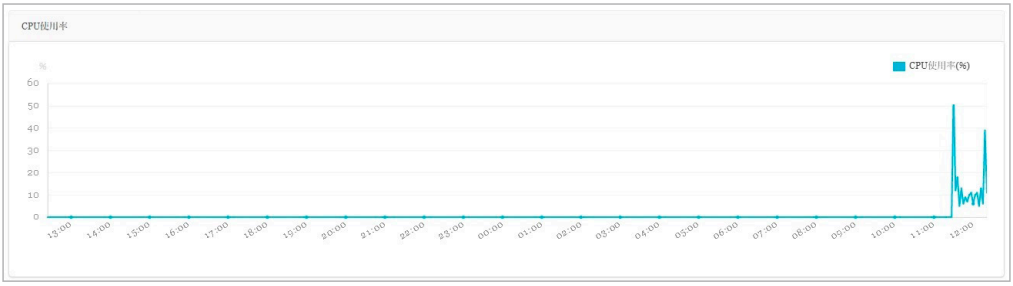


図 5-12　CPU 使用率

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

ポートタブ

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

補足　スイッチ製品は未サポートです。

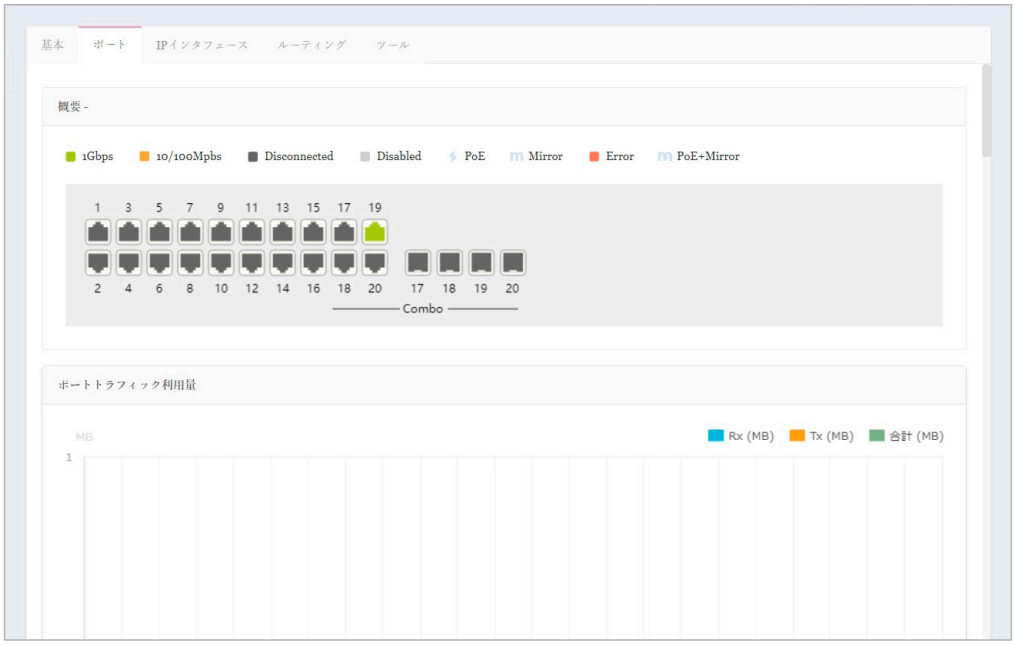


図 5-13　デバイス詳細 - ポートタブ

概要

ポートの色とアイコンが示すステータスは以下の通りです。

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

ポートトラフィック利用量

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

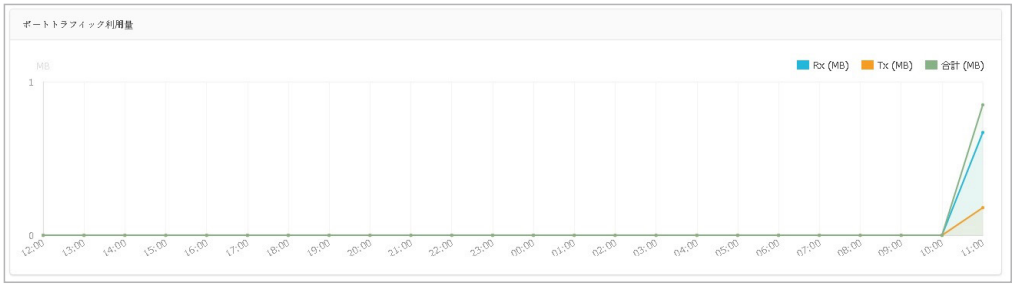


図 5-14　ポートトラフィック利用量

ポート情報

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

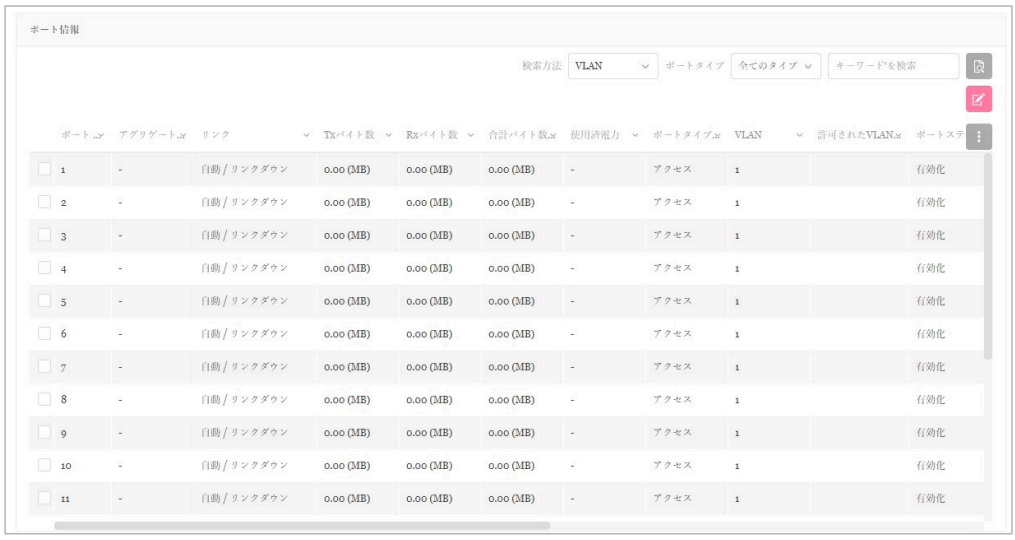


図 5-15　ポート情報

テーブルには以下の項目が表示されます。

- 「ポート（番号）」「アグリゲート」「リンク」「Tx/Rx/ 合計バイト数」「使用済電力」「ポートタイプ」「VLAN」「許可された VLAN」「ポートステート」「RSTP」「LBD」「DDP」「ポートシャットダウンスケジュール」「ミラー」「アクセスポリシー」「LLDP」「ポート名」

  - 「アグリゲート」では、ポートチャネル ID と集約タイプ（スタティック /LACP）を表示します。
  - 「VLAN」では、トランクモードのネイティブ VLAN ID またはアクセスモードの VLAN ID を表示します。 また、音声 VLAN ID に所属する場合、音声 VLAN ID を表示します。
  - 「許可された VLAN」は、ポートタイプが「トランク」の場合、許可された VLAN ID を表示します。

■ ポートの検索

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

■ ポートの変更

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

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

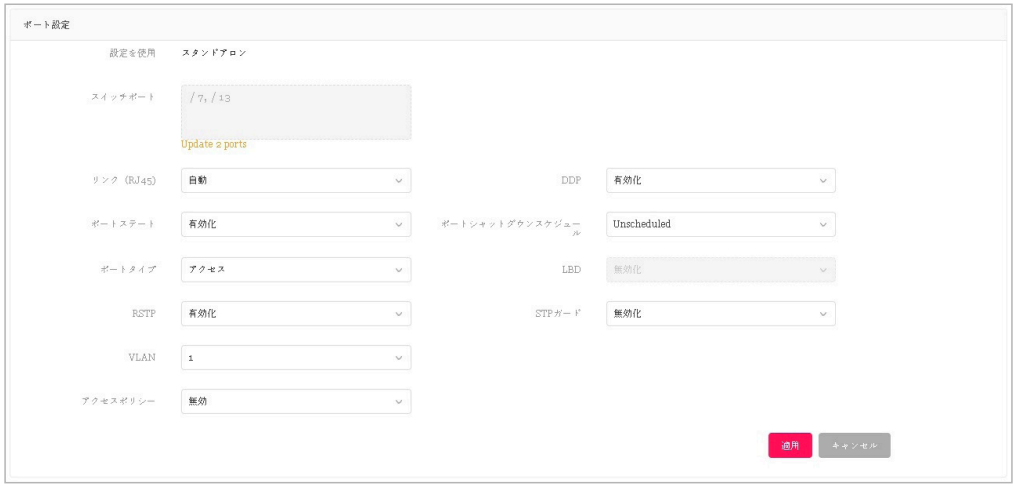


図 5-16　ポート設定

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

項目	説明
ポートタイプ	スイッチポートは、次の 2 つのタイプのいずれに設定できます。 • 「トランク」: トランクポートでは、選択したポートが 802.1Q のタグ付きトラフィックを受け入れ / パスすることができます。 - 「ネイティブ VLAN」:すべてのアンタグトラフィックがこの VLAN に配置されます。1-4094 の範囲で指定します。 - 「許可された VLAN」: 選択された VLAN のみがこのリンクを通過できます。all（すべて）または 1-4094 の範囲で指定します。 • 「アクセス」: アクセスポートは、すべてのトラフィックを定義された VLAN に配置します。 - 「VLAN」: すべてのトラフィックがこの VLAN に配置されます。1-4094 の範囲で指定します。 - 「アクセスポリシー」: このポートに制限ポリシーを適用します。 -「無効」: すべてのデバイスがこのポートにアクセスできます。 -「スタティック MAC ホワイトリスト」: このリストで指定された MAC アドレスを持つデバイスのみがこのポートにアクセスできます。 -「ポートセキュリティ delete-on-time モード」: エントリがエージアウトした場合、またはユーザがこれらのエントリを手動で削除した場合に、学習されたすべての MAC アドレスが消去されます。「ダイナミックホワイトリストサイズ制限」の設定により、動的に学習されたエントリの数を制限できます。「ダイナミックホワイトリスト MAC」の総数が「ダイナミックホワイトリストサイズ制限」の値を超えると、後続のすべての MAC アドレスがこのポートへのアクセスを拒否されます。 -「ユーザ定義のアクセスポリシー」:「アクセスポリシー」画面で定義したポリシー名を適用します。

3. 設定を変更後、「適用」をクリックしてスイッチに設定を適用します。

アグリゲート管理

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

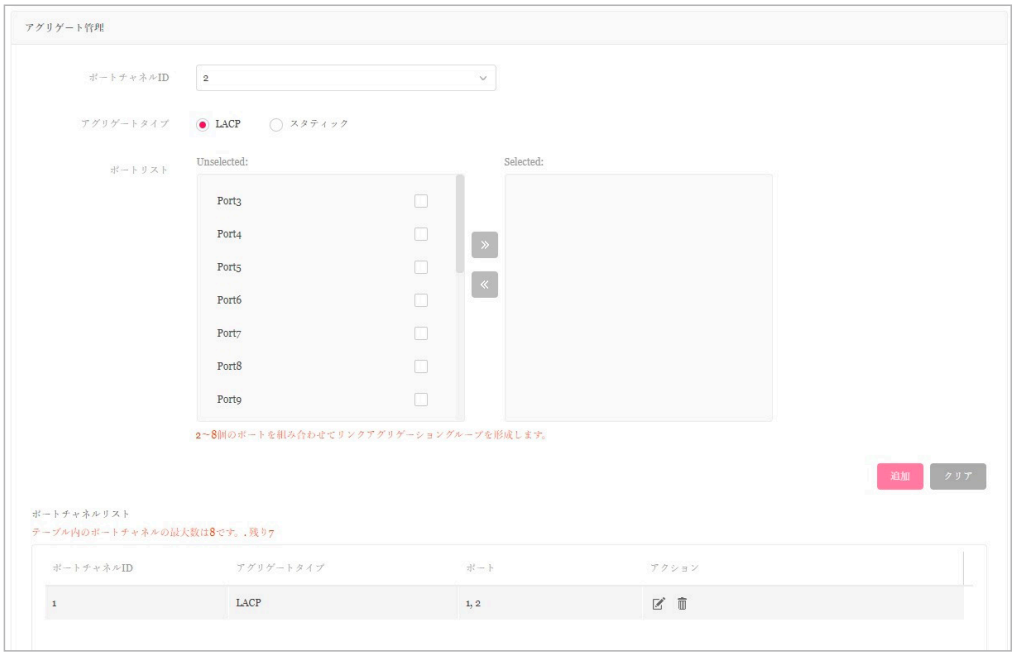


図 5-17　アグリゲート管理

■ アグリゲーショングループの作成

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

■ ポートチャネルリスト

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

■ アグリゲーショングループの編集・削除

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

「適用」をクリックして設定をスイッチに適用します。

ミラー管理

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

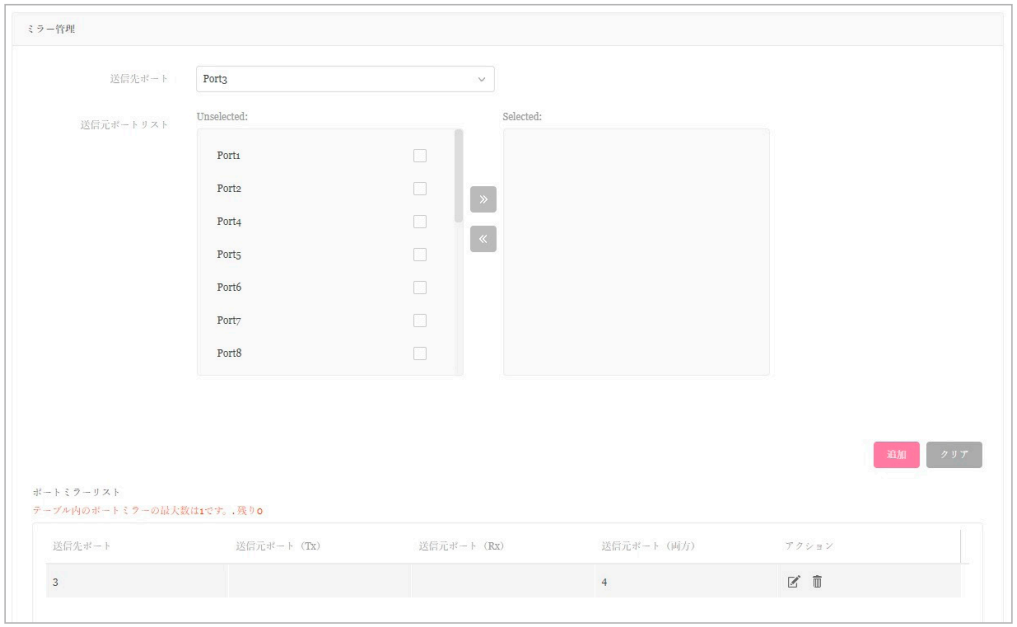


図 5-18　ミラー管理

■ ミラーリングの作成

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

■ ポートミラーリスト

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

■ ミラーリングの編集・削除

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

「適用」をクリックして設定をスイッチに適用します。

クライアント情報

「クライアント情報」セクションに、クライアント情報の概要が表示されます。

図 5-19　クライアント情報

■ クライアント情報の表示・検索

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

以下の項目が表示可能です。表示項目を変更するには、をクリックします。

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

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

IP インタフェースタブ

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

補足　スイッチ製品は未サポートです。

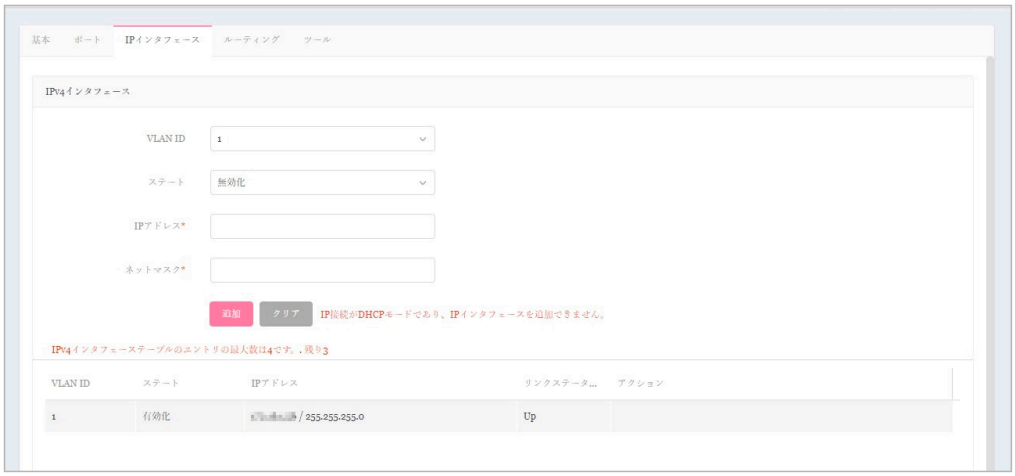


図 5-20　デバイス詳細 - IP インタフェースタブ

■ IPv4 インタフェースの作成

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

■ IPv4 インタフェーステーブル

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

■ インタフェースの編集・削除

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

インタフェースを削除する場合は、対象インタフェースの をクリックします。

「適用」をクリックして、設定をスイッチに適用します。

ルーティングタブ

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

補足　スイッチ製品は未サポートです。

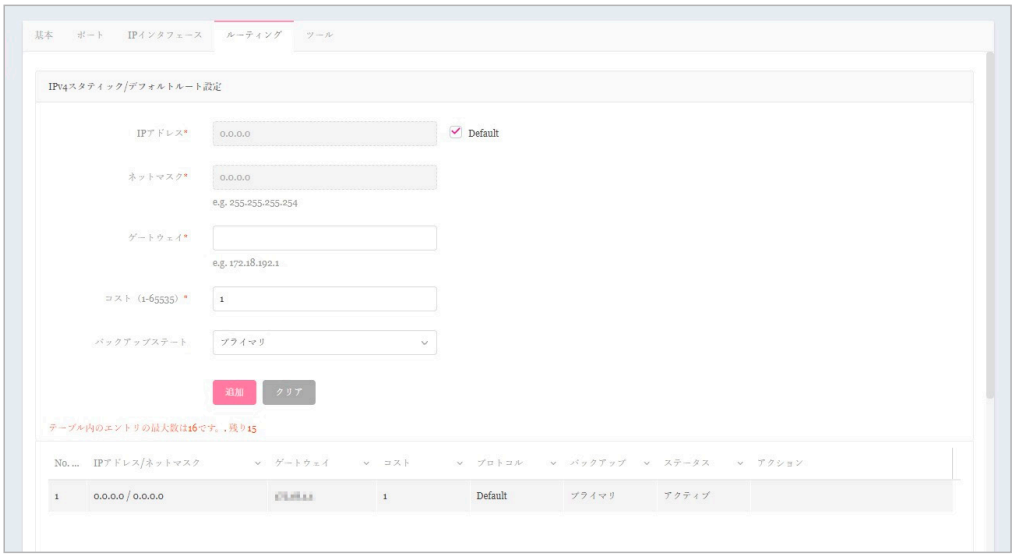


図 5-21　デバイス詳細 - ルーティングタブ

■ IPv4 スタティック / デフォルトルート設定

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

■ スタティックルートテーブルの表示

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

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

■ スタティックルートの編集・削除

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

ルートを削除する場合は、対象エントリの をクリックします。

「適用」をクリックして、設定をスイッチに適用します。

■ IPv4 ルートテーブル

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

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

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

電源タブ

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

補足　スイッチ製品は未サポートです。

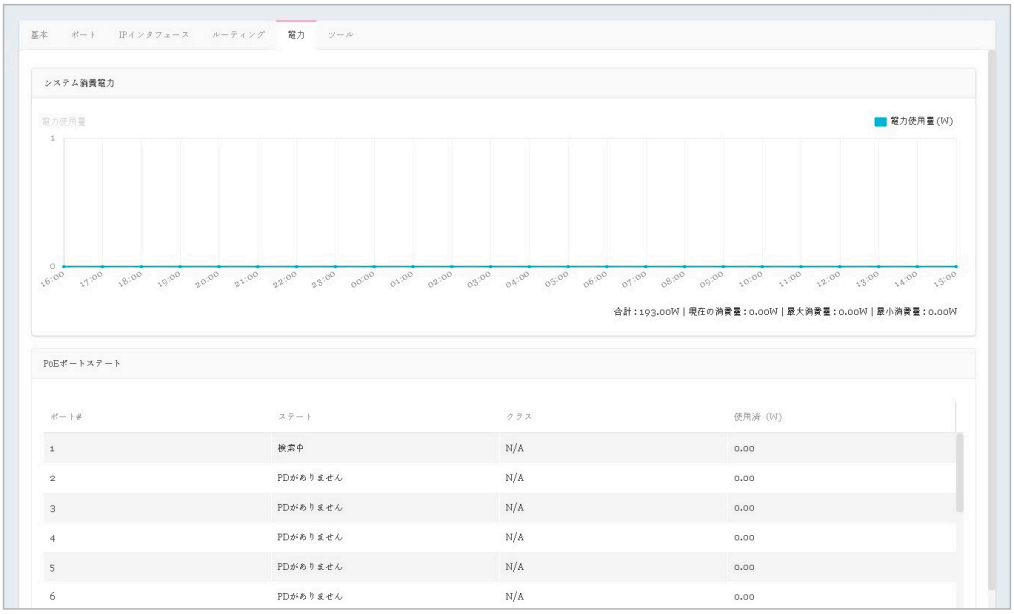


図 5-22　デバイス詳細 - 電源タブ

■ システム消費電力

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

■ PoE ポートステート

「PoE ポートステート」の一覧には、以下の項目が表示されます。

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

ツールタブ

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

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

デバイスがオフラインの場合、ツールは無効になります。

補足　スイッチ製品は未サポートです。

Ping

Ping ツールを使用すると、デバイスへの接続可否を判断できます。

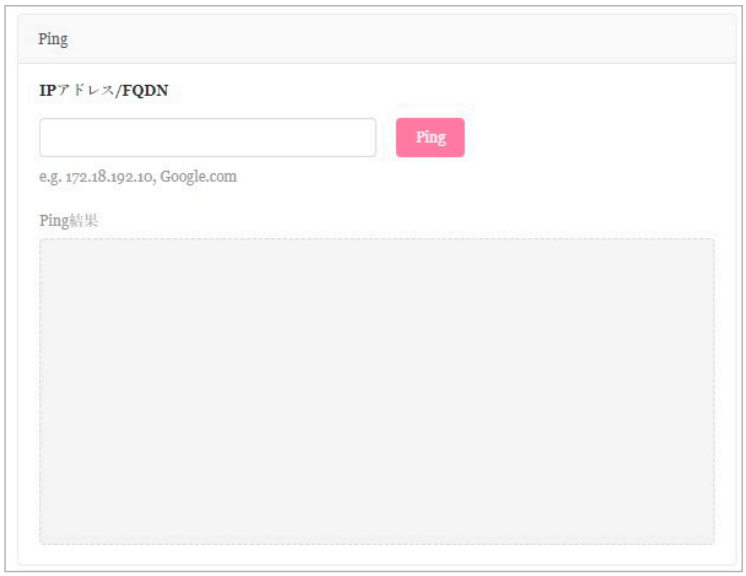


図 5-23　Ping

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

MAC 転送テーブル

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

図 5-24　MAC 転送テーブル

「実行」クリックして処理を開始します。

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

ケーブルテスト

ケーブルテストでは、1 つまたは複数のポートの接続をテストできます。

図 5-25　ケーブルテスト

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

注意　ケーブルテストにより、デバイスへのトラフィックが中断されます。

サイクル PoE

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

図 5-26　サイクル PoE

デバイスの検索

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

図 5-27　デバイスの検索

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

他のデバイスに設定をコピー

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

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

注意　コピー元とコピー先の 2 つのデバイスは同じモデルである必要があります。

図 5-28　他のデバイスに設定をコピー

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

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

スイッチ - スイッチクライアント

左側のパネルから**モニタ > スイッチ > スイッチクライアント**をクリックします。

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

補足　スイッチ製品は未サポートです。

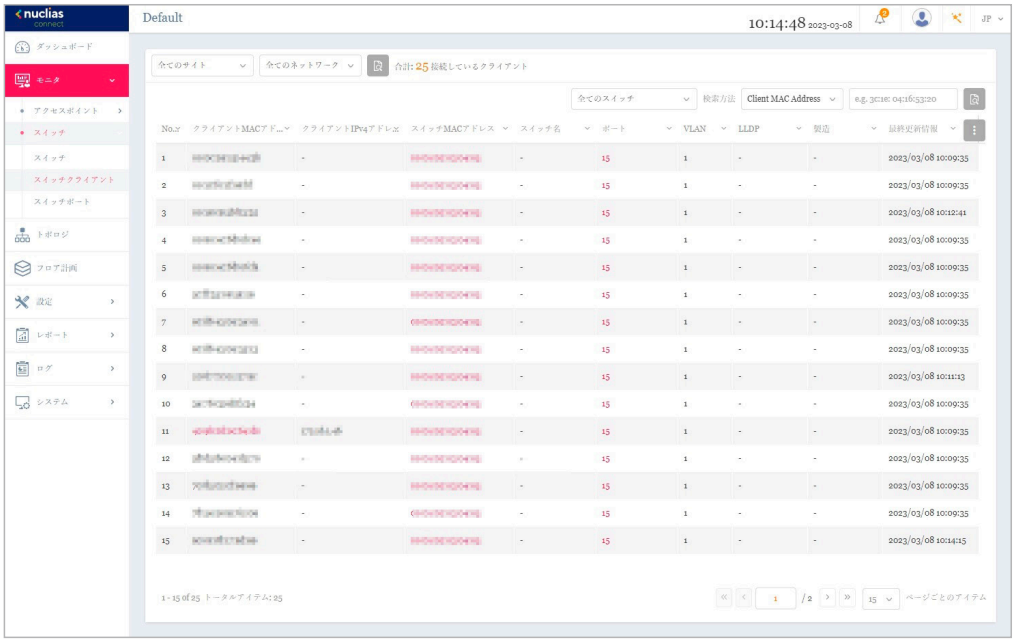


図 5-29　モニタ - スイッチ - スイッチクライアント

■ 対象範囲の指定 / クライアントの検索

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

■ レポート項目

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

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

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

スイッチ - スイッチポート

左側のパネルから**モニタ > スイッチ > スイッチポート**をクリックします。

補足　スイッチ製品は未サポートです。

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

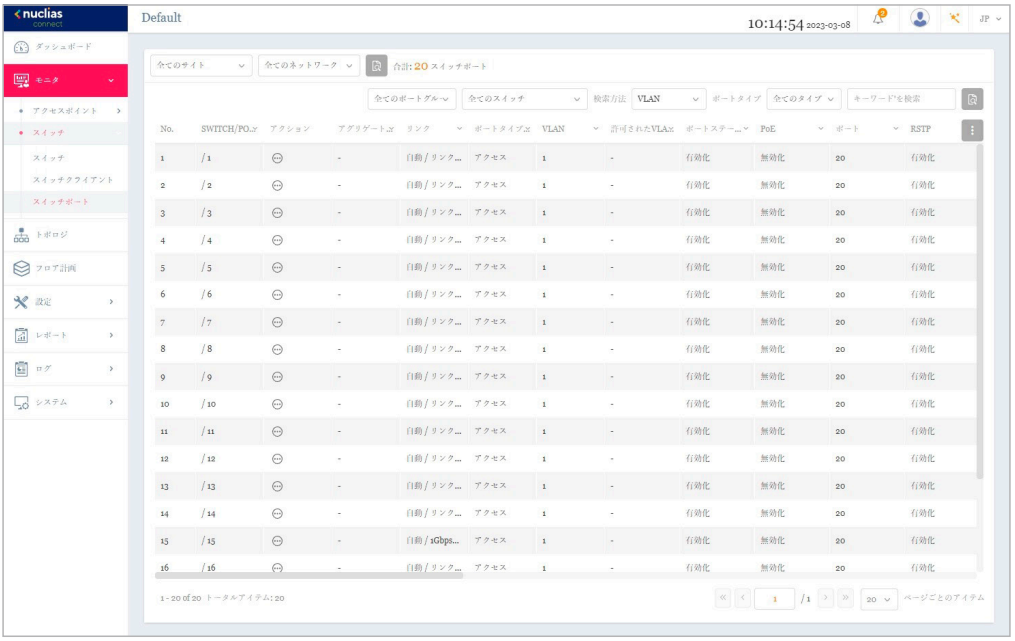


図 5-30　モニタ - スイッチ - スイッチポート

■ 対象範囲の指定 / ポートの検索

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

■ レポート項目

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

- SWITCH/PORT
- アグリゲート
- リンク
- ポートタイプ
- VLAN
- 許可された VLAN
- ポートステート
- PoE
- ポート
- RSTP
- LBD
- DDP
- ポートシャットダウンスケジュール
- PoE 供給スケジュール
- アクセスポリシー
- ミラー
- LLDP
- ポート名
- Rx ブロードキャストパケット
- Tx ブロードキャストパケット
- Rx マルチキャストパケット
- Tx マルチキャストパケット
- Rx バイト数
- Tx バイト数
- Rx パケット数
- Tx パケット数
- 合計バイト数

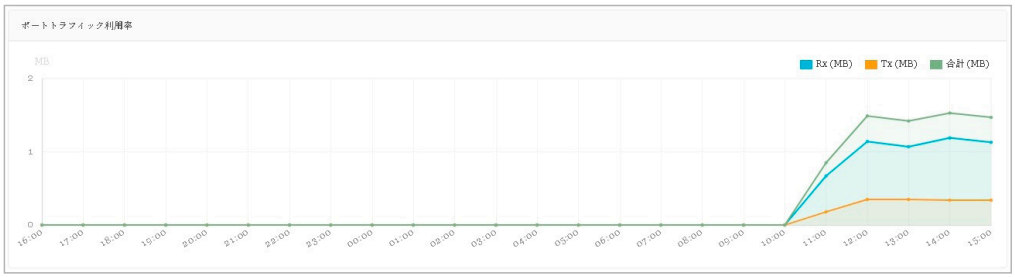
  - 「SWITCH/PORT」では、スイッチ名とポート番号を表示します。
  - 「アグリゲート」では、ポートチャネルグループのリンクアグリゲーションタイプ（Static/LACP/-）を表示します。
  - 「リンク」では、ポートのリンク設定とリンク状態を表示します。

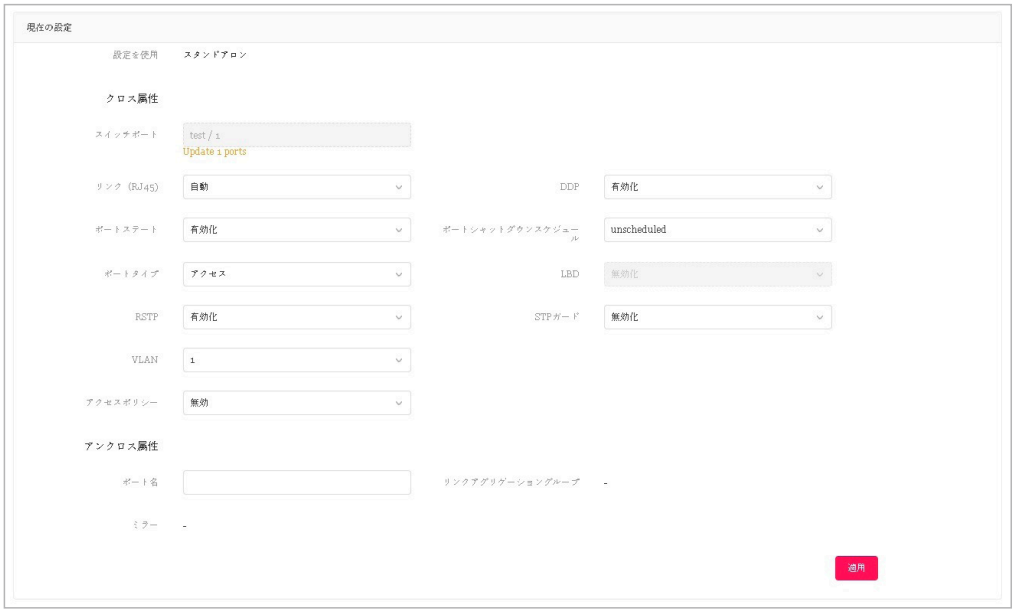
■ 特定ポートの詳細

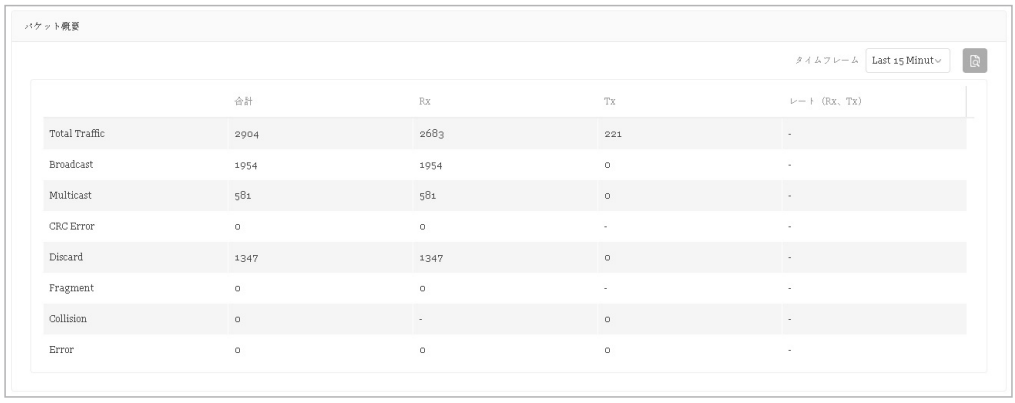
「アクション」欄で、 をクリックしてポート詳細画面に移動します。選択したスイッチの特定のポートの詳細画面が表示されます。

ポートの詳細画面では、以下の情報が表示されます。

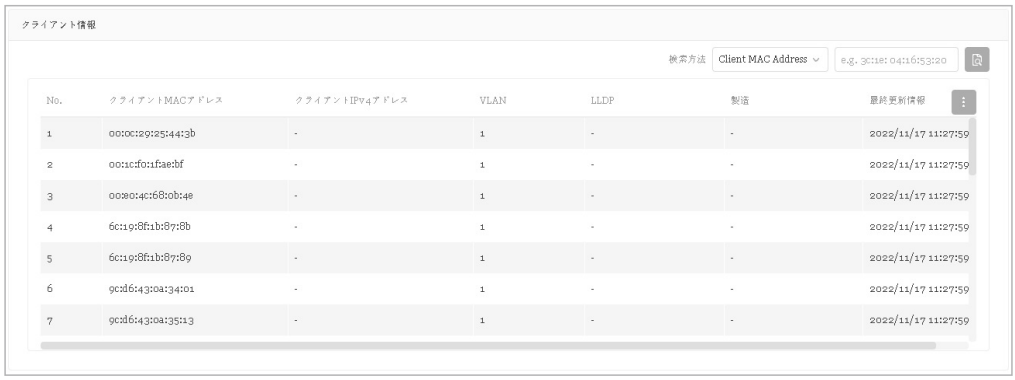
- 「Overview（ポート接続ステータス）」「ポートトラフィック利用率」「現在の設定」「ステータス」「トラブルシューティング（ケーブルテスト、サイクル PoE）」「パケット概要」「クライアント情報」







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



No.	クライアントMACアドレス	クライアントIPv4アドレス	VLAN	LLDP	製造	最終更新情報
1	00:0c:29:25:44:3b	-	1	-	-	2022/11/17 11:27:59
2	00:1c:f0:1f:ae:bf	-	1	-	-	2022/11/17 11:27:59
3	00:80:4c:68:0b:4e	-	1	-	-	2022/11/17 11:27:59
4	6c:19:8f:1b:87:8b	-	1	-	-	2022/11/17 11:27:59
5	6c:19:8f:1b:87:89	-	1	-	-	2022/11/17 11:27:59
6	9c:d6:43:0a:34:01	-	1	-	-	2022/11/17 11:27:59
7	9c:d6:43:0a:35:13	-	1	-	-	2022/11/17 11:27:59

第 6 章　トポロジ

トポロジ画面では、ネットワーク内のデバイス間のトポロジ関係を表示します。

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

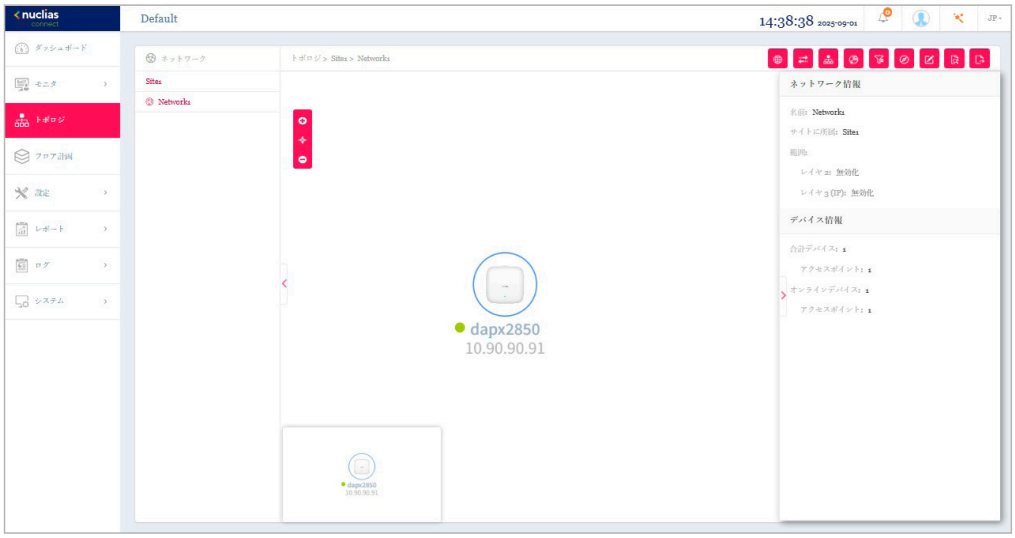


図 6-1　　トポロジ

■ 詳細情報の確認

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

デバイス情報の ⋯ をクリックすると、デバイスの詳細画面が開きます。

リンクをダブルクリックすると、リンク情報が表示されます。

■ トポロジの表示の調整

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

デバイス情報

デバイス情報には以下の項目が表示されます。

図 6-2　　デバイス情報

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

リンクの作成

デバイス間のリンクを手動で定義することができます。

1. をクリックして、編集を開始します。

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

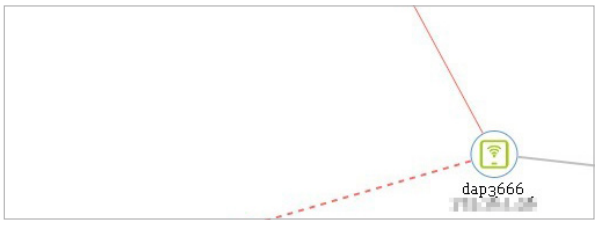


図 6-3　リンクの作成

3. リンクが作成されると、リンク設定画面が表示されます。

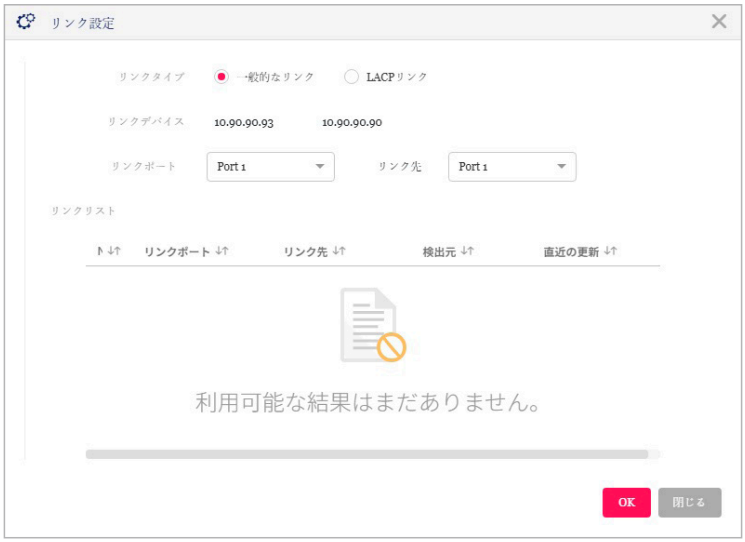


図 6-4　リンク設定

4. リンクタイプとリンクポートを設定し、「OK」をクリックします。

5. （保存して終了）をクリックして変更を保存します。

トポロジ情報の設定と表示

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

各アイコンの説明は以下の通りです。

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

第 7 章　フロア計画

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

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

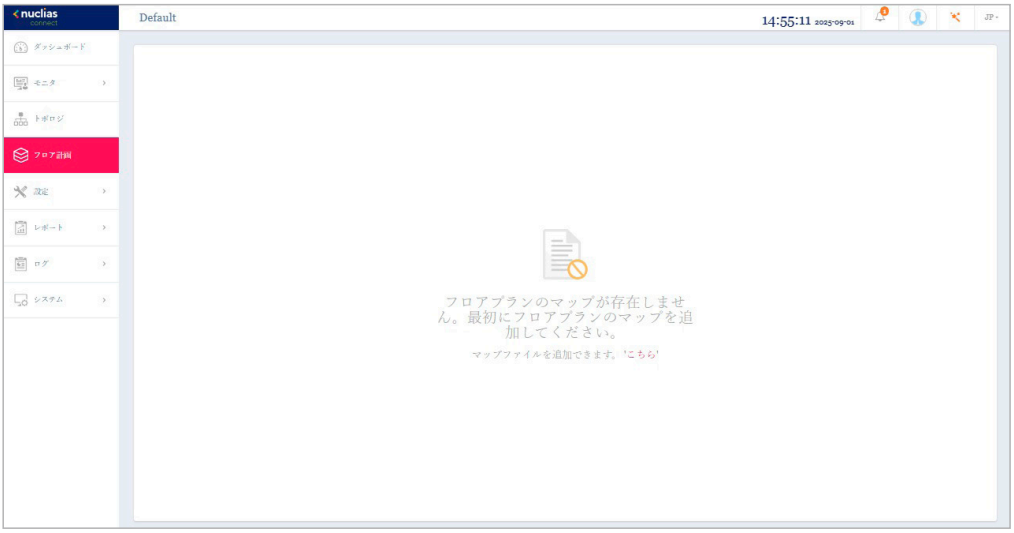


図 7-1　　フロア計画

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

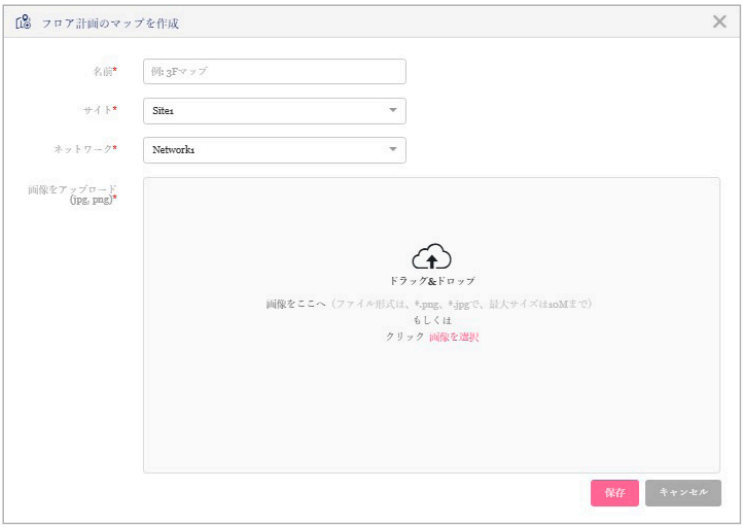


図 7-2　　フロア計画のマップを作成

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

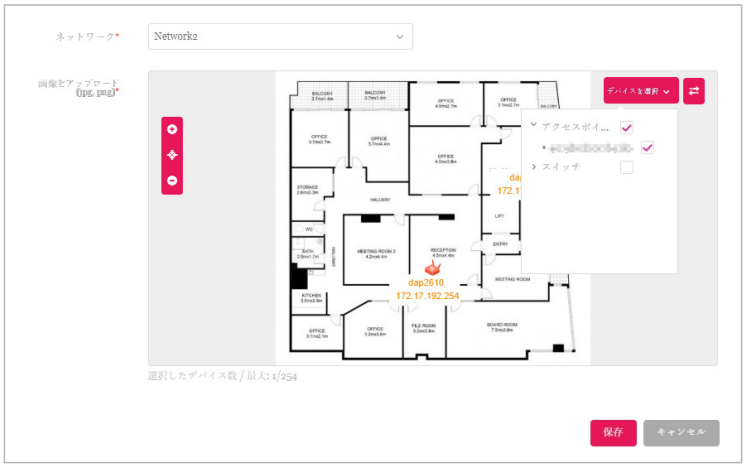


図 7-3　　デバイスの配置

5. 「保存」をクリックします。

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

第 8 章　設定

プロファイルの作成

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

図 8-1　　プロファイルを作成

既存のネットワークに対しては、以下の操作を実行することができます。

項目	説明
プロファイルを編集	選択したサイトのプロファイル設定画面を開きます。セキュリティ、アクセスコントロール、ユーザ認証などの設定を編集できます。
このネットワークにプ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	「デバイスを検出」画面を開きます。 (1)　アイコンをクリックして検出条件（L2/L3）を定義します。 (2)　「検出開始」をクリックして、デバイスを検出します。
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。

図 8-1　プロファイルを作成

2. 「ネットワークを追加」画面で、以下の項目を設定します。
「次へ」をクリックして次に進みます。設定プロセスを中止するには「キャンセル」をクリックします。

   (1) 「サイト」ドロップダウンメニューから既存のサイトを選択するか、「新しいサイト」を選択し、空のフィールドにサイトの名前を入力します。

   (2) 「ネットワーク」フィールドに、新しいネットワークの名前を入力します。

   (3) 「ネットワークID」フィールドはオプションで、REST API機能に使用されます。REST APIを使用しない場合は、入力する必要はありません。

図 8-2　ネットワークを追加

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

図 8-3　ネットワーク設定

補足　スイッチ製品は未サポートです。

4. 「デバイスを検出」ページが表示されます。「検出開始」をクリックして、利用可能なすべての非管理デバイスを検出・表示します。

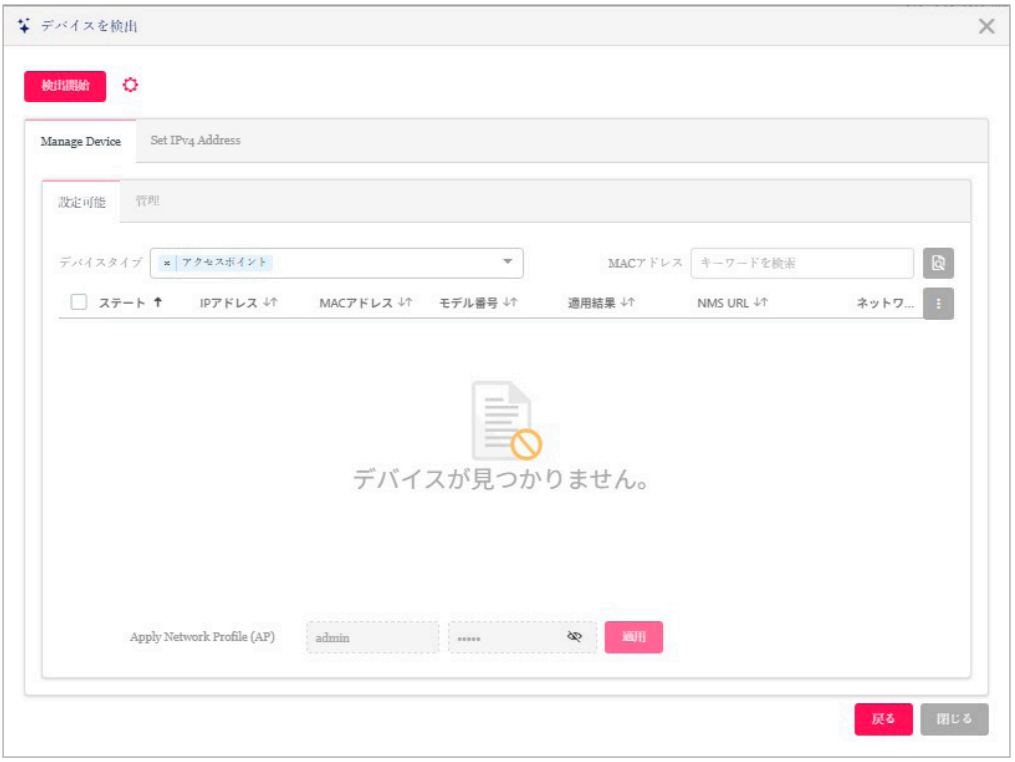


図 8-4　　デバイスを検出

検出範囲を指定する場合は、 アイコンをクリックし、「ネットワーク検出設定」画面で検出範囲を設定します。

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。

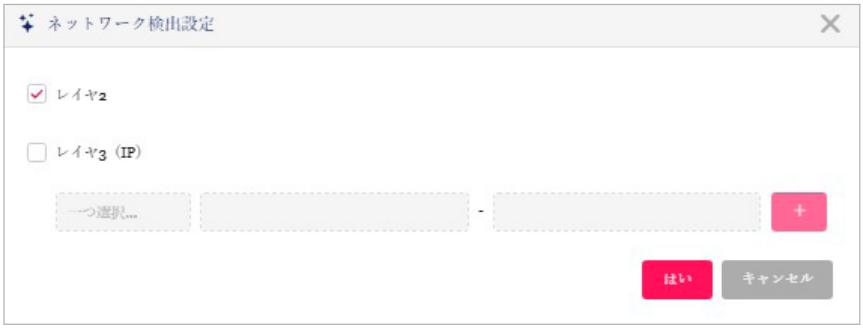


図 8-5　　ネットワーク設定を検出

5. 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」タブでは、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ができます。

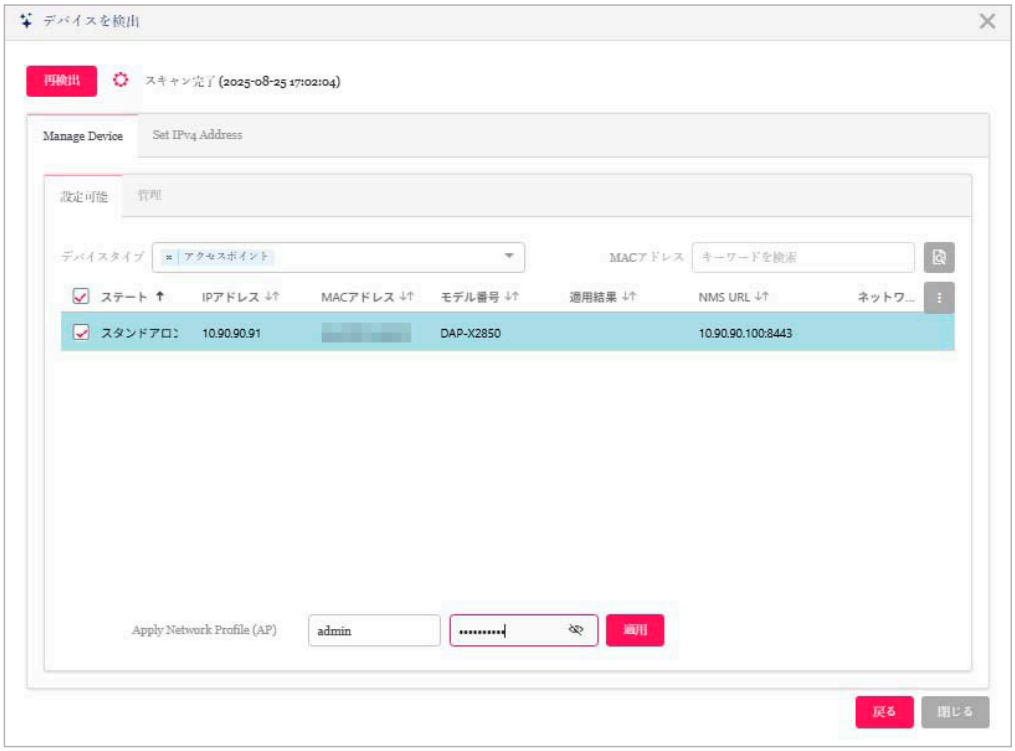


図 8-6　　デバイスを検出

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

補足 「Set IPv4 Address」設定は未サポートです。

6. 右上の「×」または「閉じる」ボタンをクリックして画面を閉じます。

プロファイル設定

プロファイル設定機能では、既存のネットワークを管理することができます。

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

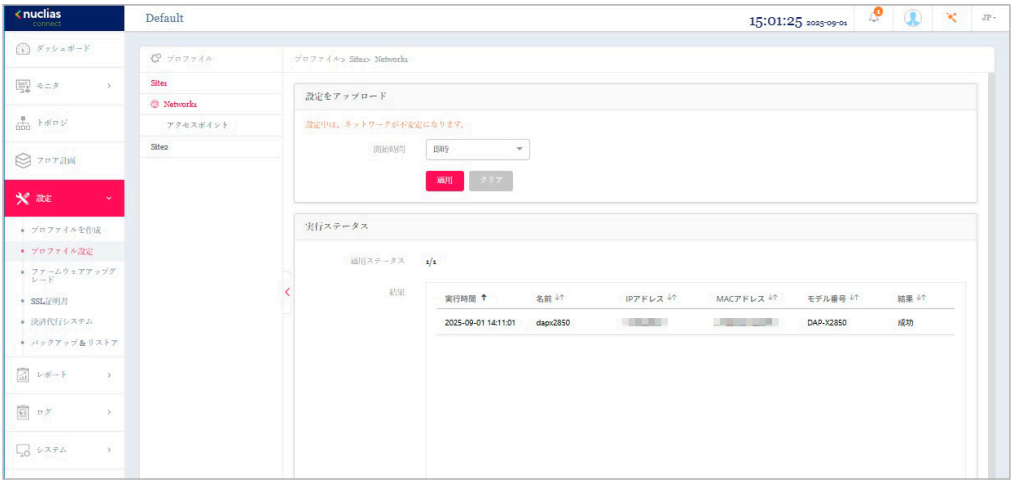


図 8-7　　プロファイル設定

■ 設定のアップロード

ネットワークを選択した後、本画面から設定のアップロード機能を利用できます。
サイトまたはネットワーク設定の更新を有効にするには、設定をアクセスポイントにアップロードする必要があります。

1. 「設定をアップロード」セクションで、「開始時間」ドロップダウンメニューをクリックし、アクセスポイントに設定を更新する時間（「即時」または「時間を選択」）を選択します。
   - 「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。
2. 「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を確認できます。更新完了後に結果が表示されます。

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

■ ネットワークの各種設定

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

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

アクセスポイント - SSID

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

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

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

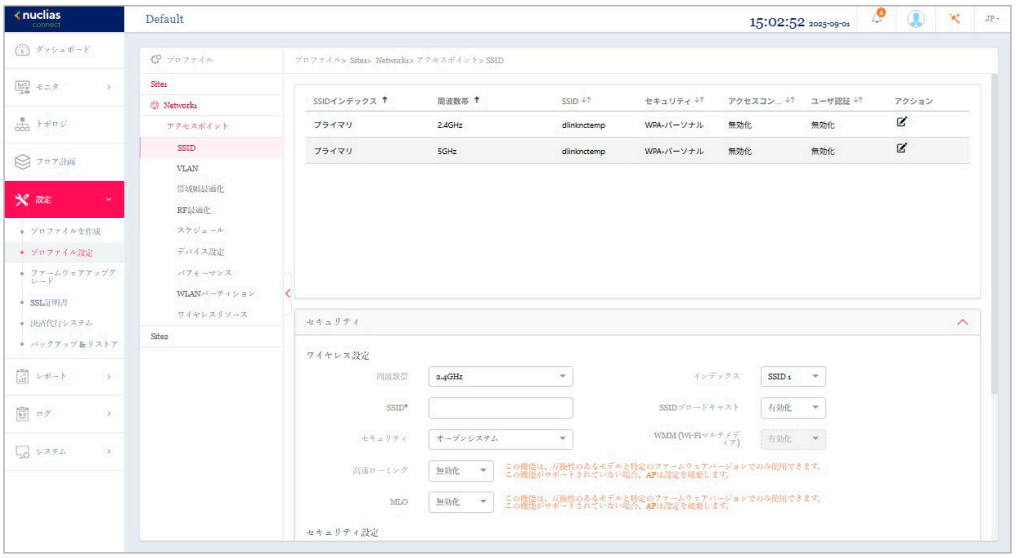


図 8-8　プロファイル設定 - アクセスポイント - SSID

セキュリティ

図 8-9　SSID - セキュリティ

「セキュリティ」セクションでは、以下の設定項目が表示されます。

項目	説明
周波数帯	ドロップダウンメニューをクリックして、無線周波数帯域を選択します。 • 選択肢：「2.4GHz」「5GHz」「6GHZ」
インデックス	ドロップダウンメニューをクリックして、SSID インデックスを選択します。新しい SSID を作成するには、最初に本項目を選択します。 • 選択肢：プライマリ、SSID1-SSID7
SSID	ワイヤレスネットワーク名を入力します。SSID はすべての周波数で同じである必要があります。また、対象の接続先アクセスポイントのネットワーク名（SSID）が、Nuclias Connect で定義されているネットワーク名（SSID）と同じであることを確認してください。詳細については、アクセスポイント側のインタフェースで **Basic Settings > Wireless Settings** と **Advanced Settings > DHCP Server > Dynamic Pool Settings** を参照してください。「Domain Name」に Nuclias Connect で定義されたネットワーク名（SSID）が反映されるようにします。
SSID ブロードキャスト	ドロップダウンメニューをクリックして、ワイヤレス SSID の可視性を有効または無効にします。

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

「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。

■ 新規 SSID の追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。
入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

補足　「高速ローミング」、「Enhanced Open」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

注意　バンドステアリング有効時は、Index 毎に共通の SSID を設定する必要があります。

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.74）」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 8-10　SSID - セキュリティ（オープンシステム）

項目	説明
セキュリティ設定	
暗号化	ドロップダウンメニューをクリックして、WEP オープンシステムの暗号化を有効または無効にします。
キーサイズ	ドロップダウンメニューをクリックして、WEP キーのサイズを選択します。 • 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 8-11　SSID - セキュリティ（WPA- パーソナル）

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

補足　「WPA3」は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて (p.140)」をご確認ください。

■「セキュリティ」項目を「WPA- エンタープライズ」に設定した場合

図 8-12　SSID - セキュリティ（WPA- エンタープライズ）

項目	説明
セキュリティ設定	
WPA モード	ドロップダウンメニューをクリックして、WPA モードを選択します。 • 選択肢：「自動 (WPA もしくは WPA2)」「WPA2 のみ」「WPA3 のみ」 注意　DAP-3666 は WPA3- エンタープライズは未サポートです。 注意　WPA3 エンタープライズは 192-bit 暗号化のみ対応しています。
暗号化タイプ	ドロップダウンメニューをクリックして、暗号化タイプを選択します。 • 選択肢：「自動」（「自動 (WPA もしくは WPA2)」を指定した場合） • 選択肢：「AES」（「WPA2 のみ」「WPA3 のみ」を指定した場合）
グループキー更新間隔	WPA グループキーの更新間隔の値を入力します。
ネットワークアクセス保護	ネットワークアクセス保護機能を有効または無効にします。

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

補足 Radius Request は AP から送信されます。

補足 「ネットワークアクセス保護」、「WPA3」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

■「セキュリティ」項目を「802.1X」に設定した場合

図 8-13　SSID - セキュリティ（802.1X）

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

アクセスコントロール

図 8-14　SSID - アクセスコントロール

「アクセスコントロール」セクションでは、以下の設定項目が表示されます。

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

■ 新規 SSID の追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。
入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

ユーザ認証

図 8-15　SSID - ユーザ認証

「ユーザ認証」セクションでは、以下の設定項目が表示されます。

項目	説明
認証タイプ	ドロップダウンメニューをクリックして、ワイヤレスクライアントに適用する認証タイプを選択します。 • 選択肢:「無効化」「Web リダイレクトのみ」「ユーザ名 / パスワード」「リモート RADIUS」「LDAP」「POP3」「パスコード」「外部キャプティブポータル」「MAC アドレス」「クリックスルー」「ソーシャルログイン」
アイドルタイムアウト（2~1440）	クライアントがアクセスポイントから切断され、指定した時間が経過すると再認証が必要となります。本値は、経過後に STA を切断する時間ではなく、再接続に際して再認証が必要となる時間を設定します。 **注意** Nuclias Connect の「アイドルタイムアウト」（本項目）が、DAP-2680/DAP-3666（v1.10b08r068）の WebUI における「Session Timeout」に該当します。
同時ログインを有効化	同時ログインを有効または無効に設定します。 「ユーザ名 / パスワード」「リモート RADIUS」「LDAP」「POP3」を選択した場合に設定します。
セッションタイムアウト (2~1440)	ログイン後、指定時間が経過すると再認証が必要になります。 「ユーザ名 / パスワード」「リモート RADIUS」「LDAP」「POP3」「クリックスルー」を選択した場合に設定します。
許可 (1~720)	ワイヤレスクライアントが 1 日に再ログインできる回数を定義します。開始時刻は 0:00 です。 「セッションタイムアウト」を有効化した場合に設定します。
間隔 (0~720)	セッションタイムアウトの制限回数を超えた後、無線クライアントがログインできるようになるまでの期間を定義します。 「セッションタイムアウト」を有効化した場合に設定します。
ホワイトリストを有効化（認証タイプが「Web リダイレクトのみ」以外の場合）	
ホワイトリストを有効化	チェックを入れると、ホワイトリスト機能が有効になります。
MAC アドレス	ホワイトリストに登録するネットワークデバイスの MAC アドレスを入力し、「追加」をクリックしてアドレスをホワイトリストテーブルに追加します。
ホワイトリストファイルをアップロード	「参照 ...」をクリックして、ローカルコンピュータに保存された MAC アドレスリストのファイルを選択します。「アップロード」をクリックして MAC アドレスリストを更新します。現在の MAC アドレスリストをダウンロードするには、「ダウンロード」をクリックします。
IP インタフェース設定	
IRIF ステータス	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト**内で設定される必要があります。
VLAN ID（VID）	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > VLAN > IP インタフェースリスト**内で設定される必要があります。
IP アドレスの取得	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント** > VLAN > **IP インタフェースリスト**内で設定される必要があります。
IP アドレス	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント** > VLAN > **IP インタフェースリスト**内で設定される必要があります。
サブネットマスク	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント** > VLAN > **IP インタフェースリスト**内で設定される必要があります。
ゲートウェイ	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント** > VLAN > **IP インタフェースリスト**内で設定される必要があります。
DNS	IP インタフェース設定は、**設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント** > VLAN > **IP インタフェースリスト**内で設定される必要があります。
ユーザ名 / パスワード（認証タイプが「ユーザ名 / パスワード」の場合）	
ユーザ名	ユーザ名を入力します。

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

項目	説明
テンプレートを選択	ドロップダウンメニューをクリックして、使用するログインスタイルを選択します。 ・「プレビュー」をクリックして、選択したスタイルをプレビューします。 ・「エディタ」をクリックして、スプラッシュページを編集します。 ・「ログインファイルをアップロード」をクリックして、新しいスタイルをアップロードします。 ・をクリックして、選択したスタイルを削除します。 ・をクリックして、スタイルテンプレートをダウンロードします。

■ 新規 SSID の追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。
入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 認証タイプで「MAC アドレス」を指定した場合、キャプティブポータル機能のため、一般的な MAC 認証機能と異なり、TCP/UDP（DNS、DHCP を除く）のみをブロックします。

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

注意 ソーシャルログイン認証は未サポートです。

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.74）」を参照してください。

補足 認証設定の一部機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

ホットスポット

図 8-16　SSID - ホットスポット 2.0

「ホットスポット 2.0」セクションでは、以下の設定項目が表示されます。

項目	説明
ホットスポット	
ホットスポット 2.0	ドロップダウンメニューをクリックして、ホットスポット 2.0 機能を有効または無効にします。
OSEN	ドロップダウンメニューをクリックして、OSEN（OSU Server-Only Authenticated L2 Encryption Network）のセキュリティ認証を有効または無効にします。
クロス接続を許可	ドロップダウンメニューをクリックして、クライアントのクロス接続を有効または無効にします。
P2P を管理	ドロップダウンメニューをクリックして、P2P 管理を有効または無効にします。
DGAF	ドロップダウンメニューをクリックして、DGAF（Downstream Group-Addressed Forwarding）を有効または無効にします。有効にすると、AP はダウンストリームのグループアドレスフレームを転送することができます。
プロキシ ARP	ドロップダウンメニューをクリックして、プロキシ ARP を有効または無効にします。
L2TIF	ドロップダウンメニューをクリックして、L2TIF（Layer 2 Traffic Inspection and Filtering）を有効または無効にします。
インターワーキング	
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」
インターネット	この接続を介したインターネットの利用を有効または無効にします。
ASRA	ドロップダウンメニューをクリックして、ASRA（Additional Steps required for Access）を有効または無効にします。
ESR	ドロップダウンメニューをクリックして、ESR（Emergency services reachable）を有効または無効にします。
UESA	ドロップダウンメニューをクリックして、UESA（Unauthenticated Emergency Service Accessible）を有効または無効にします。
Venue グループ	Venue グループの値を入力します。 • 設定可能範囲：0-255
Venue タイプ	Venue タイプの値を入力します。 • 設定可能範囲：0-255
Venue 名	言語を選択し、Venue 名を入力します。
HESSID	Homogenous Extended Service Set（ESS）ID を入力します。サービスプロバイダネットワークを識別するために使用されます。
WAN メトリック	
WAN リンクステータス	アクセスポイントの WAN リンクステータスを選択します。 • 選択肢：「リンクアップ」「リンクダウン」「テストステートでのリンク」
WAN 対称リンク	WAN 対称リンクのステータスを「はい」「いいえ」から選択します。「はい」の場合、アップロード / ダウンロードは同じ速度になります。

項目	説明
WAN 帯域	WAN 帯域のステータスを「はい」「いいえ」から選択します。アクセスポイントやネットワークがキャパシティの上限に達している場合、「はい」を選択します。
WAN メトリックダウンロードスピード（kbps）	WAN 接続のダウンロードスピードを kbps 単位で入力します。ダウンロードスピードが不明な場合は 0 を指定します。
WAN メトリックアップリンクスピード（kbps）	WAN 接続のアップロードスピードを kbps 単位で入力します。アップロードスピードが不明な場合は 0 を指定します。
リスト	
ネットワーク認証タイプ	接続タイプを選択します。 • 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」 右側の入力フィールドに Web アドレスを入力します。
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。 • 入力可能な値：6 桁または 10 桁の 16 進数
NAI レルムリスト	
NAI レルム	＋をクリックして NAI レルムを入力します。BSS で利用可能な全ての 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	以下の手順で EAP 方式を設定します。 1. EAP 方式を選択します。 2. ＋をクリックして、認証 ID とパラメータタイプを指定します。認証 ID/ パラメータタイプを削除する場合は、－をクリックします。 3. 「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：000-999（「MCC」）、00-999（「MNC」）
接続機能	
IP プロトコル	IP プロトコルを選択します。 • 選択肢：「ICMP」「TCP」「UDP」
ポート番号	ポート番号を入力します。
ステータス	IP プロトコルのステータスを選択します。 • 選択肢：「閉じる」「オープン」「不明」
オペレータフレンドリー名	言語を選択し、オペレータフレンドリー名を入力します。Hotspot Venue オペレータの識別名です。
OSU（Online Sign-Up）	
OSU SSID	OSU SSID を入力します。本機能を使用すると、モバイルクライアントで利用可能なオンラインサービスを選択してオンラインサービスにサインインすることができます。
OSU サーバ URI	OSU サーバ URI を入力します。
OSU 方式リスト	
OSU 方式	言語を選択し、OSU 方式を入力します。「追加」をクリックして、OSU 方式を追加します。
OSU コンフィグ	OSU コンフィグ選択します。 • 選択肢：「コンフィグ 1」「コンフィグ 2」
OSU フレンドリー名	言語を選択し、OSU フレンドリー名を入力します。
OSU Nai	OSU NAI（Network Access Identifier）を入力します。
OSU サービス説明	OSU サービスの説明を入力します。
OSU アイコン言語コード	OSU アイコン言語コードを選択します。
OSU アイコンファイルパス	OSU アイコンのファイルパスを入力します。

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

■ 新規 SSID の追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。
入力中のパラメータを定義済みの設定に戻すには、「リセット」をクリックします。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

補足 「Hotspot2.0」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

アクセスポイント - VLAN

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

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

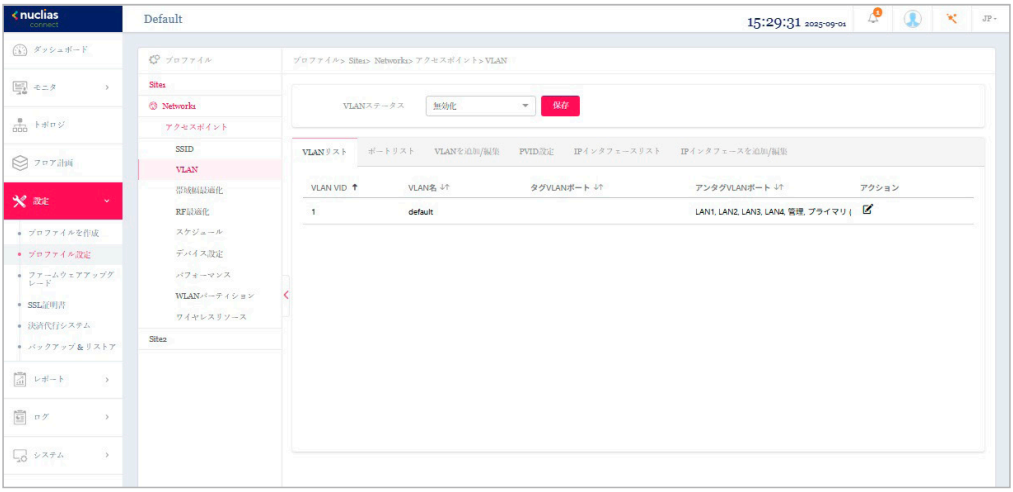


図 8-17　プロファイル設定 - アクセスポイント - VLAN

「VLAN」画面には、以下の項目が表示されます。

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

「保存」をクリックして設定を保存します。

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

VLAN リスト

「VLAN リスト」タブを選択すると、定義済みの VLAN リストが表示されます。

をクリックして、既存の VLAN を変更します。

をクリックして、既存の VLAN を削除します。

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

ポートリスト

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

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

VLAN を追加 / 編集

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

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

PVID 設定

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

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

IP インタフェースリスト

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

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

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

設定を削除するには をクリックします。

IP インタフェースを追加 / 編集

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

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

「保存」をクリックして、変更を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

アクセスポイント - 帯域幅最適化

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

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

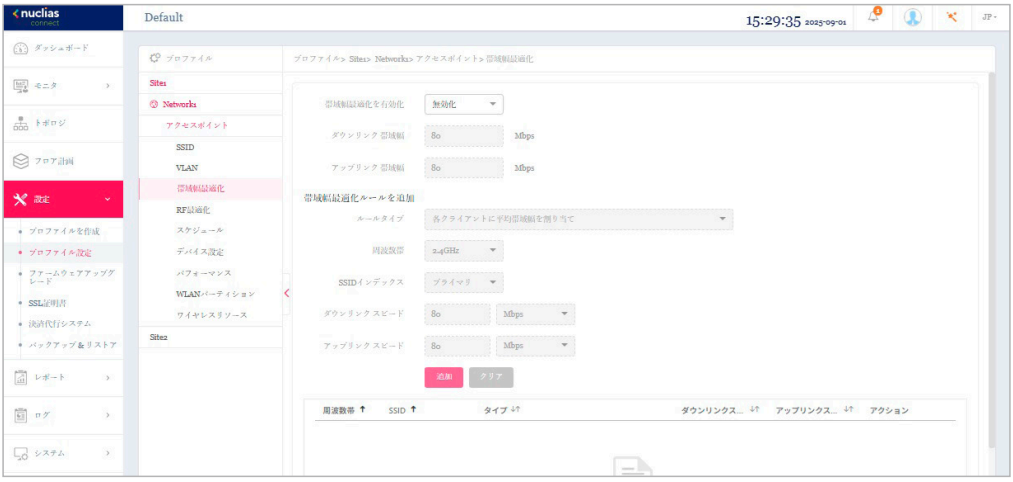


図 8-18　プロファイル設定 - アクセスポイント - 帯域幅最適化

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。11ac/ax は 11n と同じ帯域を使用します。 - （2.4GHz 帯）11b: 10%、11g: 20%、11n（11ax 含む）: 70% - （5GHz 帯）11a: 20%、11n（11ac/11ax 含む）: 80%
周波数帯	ドロップダウンメニューをクリックして、ルールを適用する無線周波数帯域を選択します。 • 選択肢：「2.4GHz」「5GHz」「6GHz」
SSID インデックス	ドロップダウンメニューをクリックして、ルールを適用する SSID を選択します。
ダウンリンク スピード	各ステーションまたは指定された SSID に割り当てるダウンリンク スピードを入力します。
アップリンク スピード	各ステーションまたは指定された SSID に割り当てるアップリンク スピードを入力します。

■ 新規ルールの追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

アクセスポイント - RF 最適化

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

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

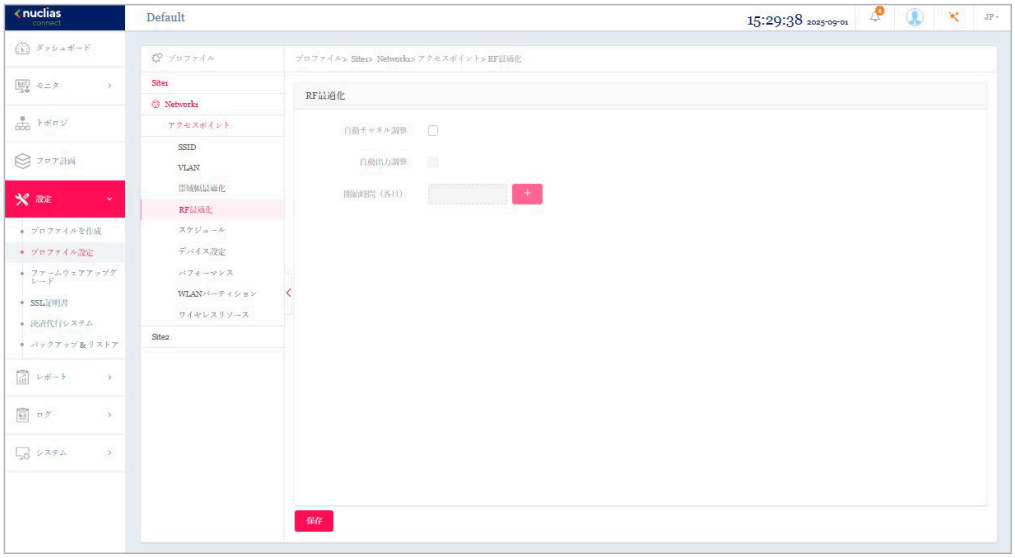


図 8-19　プロファイル設定 - アクセスポイント - RF 最適化

以下の設定項目が表示されます。

項目	説明
自動チャネル調整	チェックボックスにチェックを入れて、RF 干渉を回避するためにクライアントのチャネルを自動的に調整する機能を有効にします。
自動出力調整	「自動チャネル調整」が有効な場合に使用できます。チェックボックスにチェックを入れて、干渉が存在する場合にカバレッジを最適化するために AP 無線電力を自動的に調整する機能を有効にします。
開始時間（各日）	「＋」ボタンをクリックして、RF 最適化を開始する時間を指定します。

「保存」をクリックして設定を保存します。

注意　自動 RF 最適化機能（自動チャネル調整 / 自動出力調整）有効化時は以下の動作となります。

- 自動チャネル調整を有効にした状態で手動でチャネルを設定した場合は手動優先
- 自動出力調整を有効にした状態で手動で出力を設定した場合は自動優先

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.74）」を参照してください。

補足　「RF 最適化」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

アクセスポイント - スケジュール

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

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

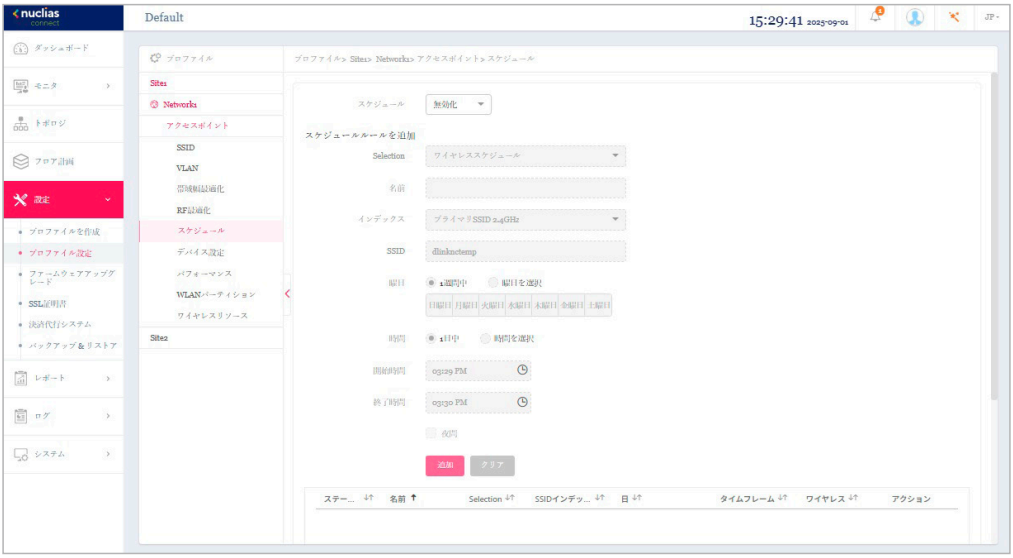


図 8-20　プロファイル設定 - アクセスポイント - スケジュール

以下の設定項目が表示されます。

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

■ 新規ルールの追加

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

■ 既存ルールの変更

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

ルールを削除する場合は、対象ルールの をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

アクセスポイント - デバイス設定

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

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

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

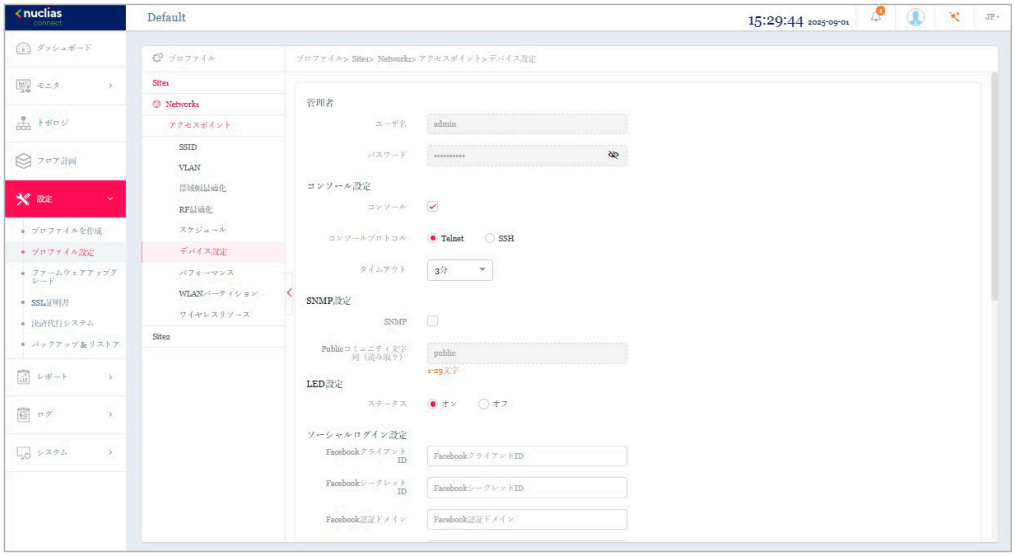


図 8-21　プロファイル設定 - アクセスポイント - デバイス設定

以下の設定項目が表示されます。

項目	説明
管理者	
ユーザ名	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理ユーザ名が表示されます。
パスワード	ネットワーク内のすべてのアクセスポイントの設定にアクセスするために使用する管理者パスワードが表示されます。
コンソール設定	
有効化	チェックを入れると、コンソール機能が有効になります。
コンソールプロトコル	ラジオボタンをクリックして、ネットワーク内のすべてのアクセスポイントに適用されるコンソールプロトコルを選択します。 • 選択肢：「Telnet」「SSH」
タイムアウト	ドロップダウンメニューをクリックして、アクティブなコンソールセッションのタイムアウト値を選択します。
SNMP 設定	
SNMP	チェックを入れると SNMP 機能が有効になります。
Public コミュニティ文字列	読み取り用のコミュニティ文字列を設定します。
LED 設定	
ステータス	デバイスの LED をオンまたはオフに設定します。
ソーシャルログイン設定	
Facebook クライアント ID	Facebook クライアント ID を入力します。
Facebook シークレット ID	Facebook シークレット ID を入力します。
Facebook 認証ドメイン	Facebook 認証ドメインを入力します。
Google クライアント ID	Google クライアント ID を入力します。
Google シークレット ID	Google シークレット ID を入力します。
Google 認証ドメイン	Google 認証ドメインを入力します。
自動時間設定	
NTP	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。 「日本」の設定から変更しないでください。

項目	説明
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
サマータイムを有効化	チェックボックスをオンにすると、サマータイム機能が有効になります。
DST 開始（24 時間）	ドロップダウンメニューをクリックして、サマータイム（DST）の開始日時を指定します。
DST 終了（24 時間）	ドロップダウンメニューをクリックして、サマータイム（DST）の終了日時を指定します。
DST オフセット	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設定	
外部シスログサーバ （キャプティブポータルログ）	外部シスログサーバの IP アドレスまたはドメイン名を入力します。本機能は、キャプティブポータルログのみ対応しています。

「保存」をクリックして設定を保存します。

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」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。

注意　ソーシャルログイン設定は未サポートです。

アクセスポイント - パフォーマンス設定

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

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

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

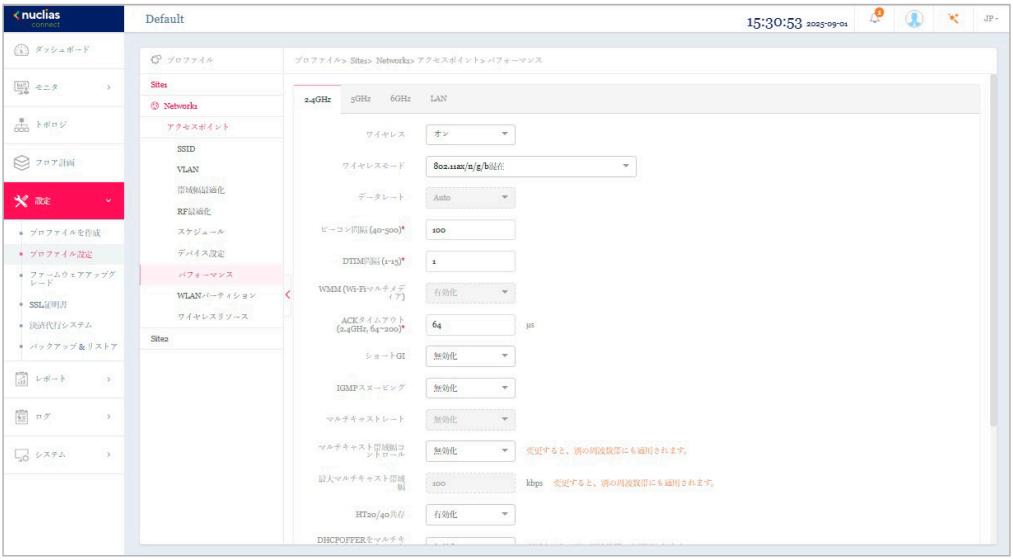


図 8-22　プロファイル設定 - アクセスポイント - パフォーマンス設定（「2.4GHz」「5Ghz」「6GHz」タブ）

2.4GHz/5Ghz/6GHz

「2.4GHz」「5Ghz」「6GHz」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/n/g/b 混在」「802.11g/b 混在」「802.11n のみ」 （5GHz の場合）「802.11n/a 混在」「802.11a のみ」「802.11n のみ」「802.11ax/ac/n/a 混在」 （6GHz の場合）「802.11ax のみ」「Mixed 802.11be/ax」
データレート	ドロップダウンメニューをクリックして、無線のデータレートを選択します。 ワイヤレスモードが「802.11g/b 混在」（2.4GHz）または「802.11a のみ」（5GHz）の場合にのみ設定できます。
ビーコン間隔	ビーコン間隔の値を入力します。 • 初期値：100
DTIM 間隔	DTIM 間隔の値を入力します。 • 初期値：1

項目	説明
WMM（Wi-Fi マルチメディア）	ドロップダウンメニューをクリックして、Wi-Fi マルチメディア（WMM）機能を有効または無効にします。 ワイヤレスモードが「802.11g/b 混在」（2.4GHz）または「802.11a のみ」（5GHz）の場合にのみ設定できます。
ACK タイムアウト	ACK タイムアウト値を入力します。 • 初期値：64
ショート GI	ドロップダウンメニューをクリックして、ショート GI 機能を有効または無効にします。（2.4GHz/5GHz のみ）
IGMP スヌーピング	ドロップダウンメニューをクリックして、IGMP スヌーピング機能を有効または無効にします。
マルチキャストレート	ドロップダウンメニューをクリックして、マルチキャストレート値を選択します。 ワイヤレスモードが「802.11g/b 混在」（2.4GHz）または「802/11n/a 混在」「802.11a のみ」（5GHz）、「Mixed 802.11be/ax」（6GHz）の場合にのみ設定できます。
マルチキャスト帯域幅コントロール	ドロップダウンメニューをクリックして、マルチキャスト帯域コントロール機能を有効または無効にします。
最大マルチキャスト帯域幅	マルチキャスト帯域幅の最大値を入力します。「マルチキャスト帯域幅コントロール」が有効の場合に設定します。 • 初期値：100
HT20/40 共存	ドロップダウンメニューをクリックして、HT20/40 共存機能を有効または無効にします。 2.4GHz 帯の「チャネル幅」で「自動 20/40MHz」を選択した場合に指定可能です。
DHCPOFFER をマルチキャストからユニキャストに変更	ドロップダウンメニューをクリックして、ユニキャストへの DHCP オファー転送を許可または拒否します。
RTS 長	RTS の長さの値を入力します。 • 初期値：2346
フラグメント長	フラグメント長の値を入力します。 • 初期値：2346
チャネル幅	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。ワイヤレスモードにより利用可能なチャネル幅は異なります。 • 選択肢：「20MHz」「自動 20/40MHz」「自動 20/40/80Mhz」「自動 20/40/80/160Mhz」「自動 20/40/80/160/320Mhz」

「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.74）」を参照してください。

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

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

LAN

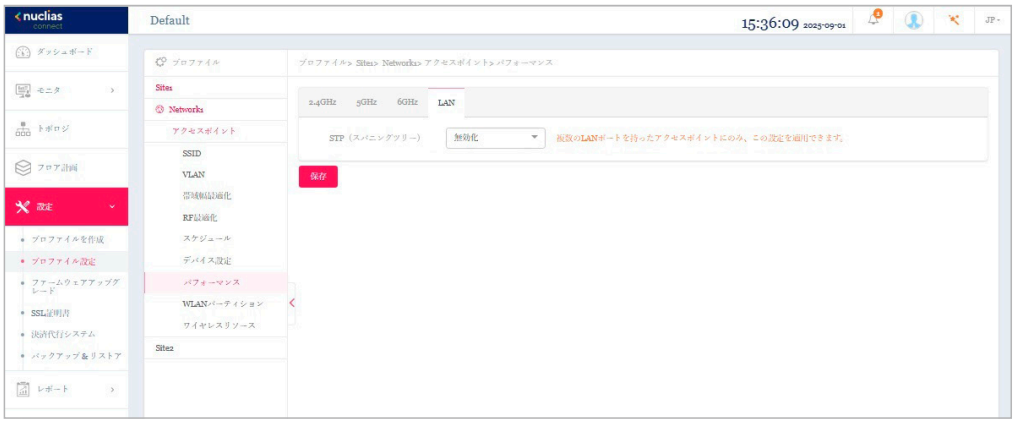


図 8-23　パフォーマンス設定（「LAN」タブ）

「LAN」タブをクリックした場合、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

補足 「STP（スパニングツリー）」の設定は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

アクセスポイント - WLAN パーティション

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

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

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > WLAN パーティションに移動し、「2.4GHz」「5GHz」「6GHz」タブをクリックして、現在の設定を表示します。

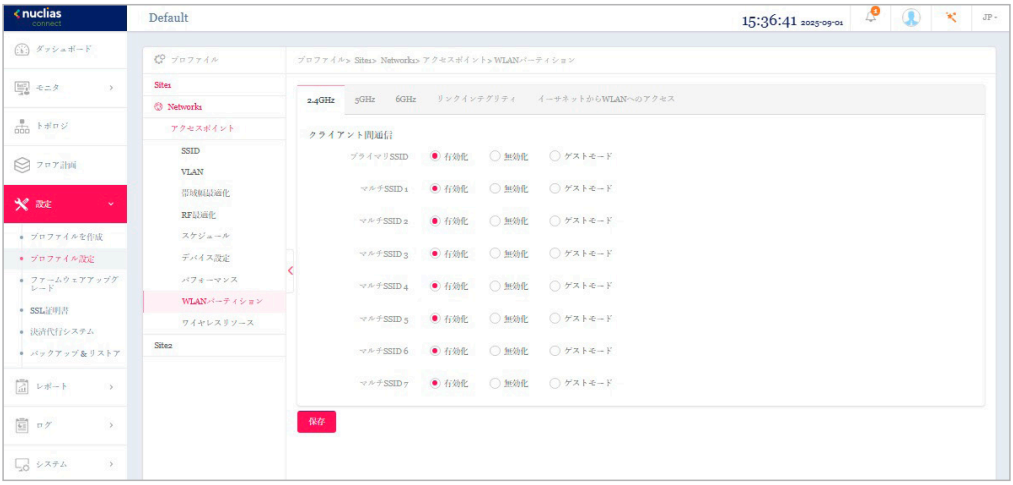


図 8-24　プロファイル設定 - アクセスポイント - WLAN パーティション（「2.4GHz」「5GHz」「6GHz」タブ）

以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74 ）」を参照してください。

リンクインテグリティ

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

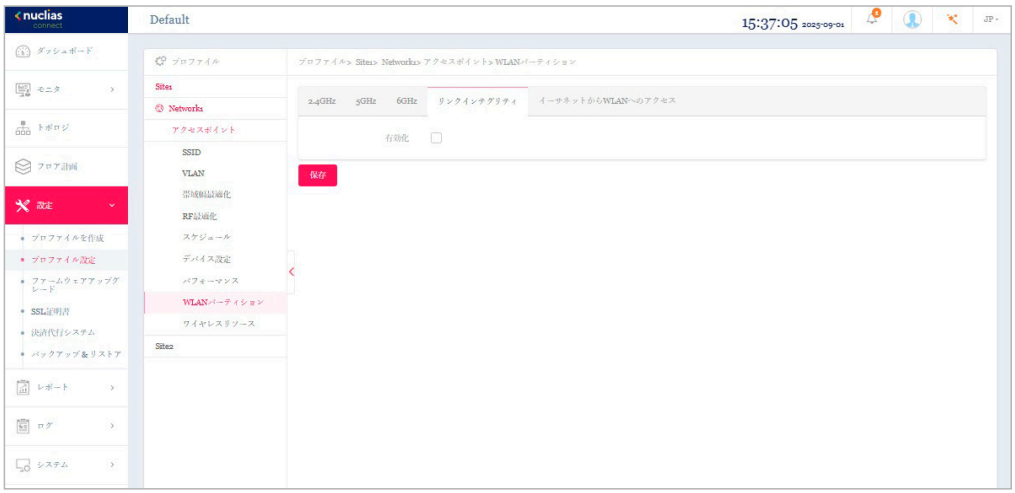


図 8-25　WLAN パーティション（「リンクインテグリティ」タブ）

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

項目	説明
有効化	チェックボックスにチェックを入れ、無線のリンクインテグリティ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.74）」を参照してください。

補足　「リンクインテグリティ」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

イーサネットから WLAN へのアクセス

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

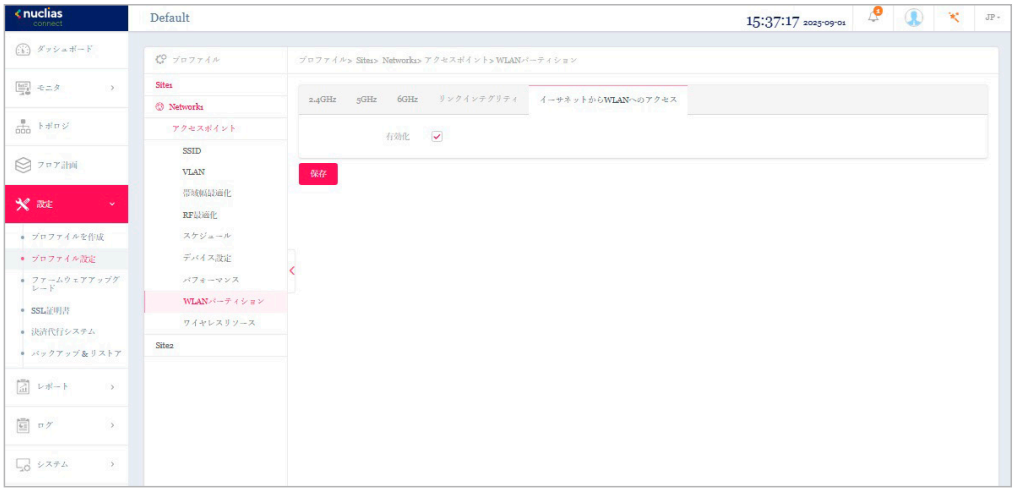


図 8-26　WLAN パーティション（「イーサネットから WLAN へのアクセス」タブ）

「イーサネットから WLAN 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
有効化	チェックボックスにチェックを入れて、有線 LAN から無線 LAN へのアクセス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.74）」を参照してください。

アクセスポイント - ワイヤレスリソース

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

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

設定 > プロファイル設定 > サイト > ネットワーク > アクセスポイント > ワイヤレスリソースに移動し、「2.4GHz」「5GHz」「6GHz」タブをクリックして、現在の設定を表示します。

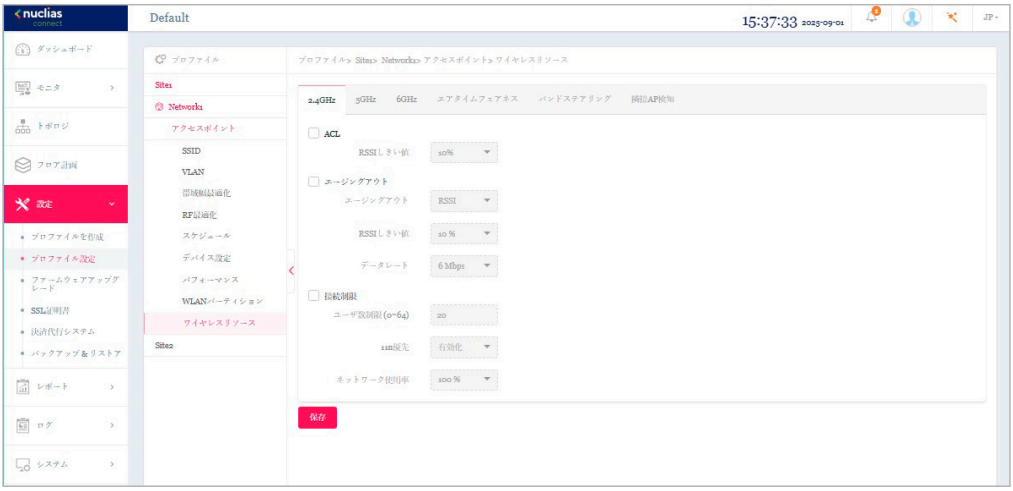


図 8-27　プロファイル設定 - アクセスポイント - ワイヤレスリソース（「2.4GHz」「5GHz」「6GHz」タブ）

「2.4GHz」「5GHz」「6GHz」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	
ACL	チェックボックスをクリックして、ACL 機能を有効 / 無効にします。
RSSI しきい値	ドロップダウンメニューをクリックして、ACL RSSI しきい値のパーセンテージを選択します。
エージングアウト	
エージングアウト	チェックボックスをクリックしてエージングアウトを有効 / 無効にします。
エージングアウト	ドロップダウンメニューをクリックして、エージングアウトモードを選択します。 • 選択肢：「RSSI」「データレート」
RSSI しきい値	エージングアウトモードで「RSSI」を選択した場合に設定可能です。 10%~100% の値を選択します。このパラメータは、無線クライアントがプローブに応答するための最小 RRSI を設定します。クライアントの RSSI 値が指定のパーセンテージより小さい場合、ワイヤレスクライアントは切断されます。
データレート	エージングアウトモードで「データレート」を選択した場合に設定可能です。 ドロップダウンメニューをクリックして、データレート接続制限を選択します。
接続制限	
接続制限	チェックボックスをクリックして接続制限を有効 / 無効にします。 接続制限は、負荷分散を提供するように設計されています。このポリシーにより、ワイヤレスネットワークでのユーザアクセス管理が可能になります。本機能が有効になっていて、ユーザ数またはネットワーク使用率が指定された値を超えた場合、それ以上のクライアントアソシエーションは許可されません。
ユーザ数制限	ユーザ接続数の上限を入力します。 • 初期値：20 • 設定可能範囲：0-64
11n 優先	ドロップダウンメニューをクリックして、802.11n の優先使用を有効または無効にします。
ネットワーク使用率	ドロップダウンメニューをクリックして、ネットワーク使用率を選択します。 **注意** この機能は、DAP-X2810/DAP-3666 でのみ使用可能です。

「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.74）」を参照してください。

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

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

エアタイムフェアネス

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

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

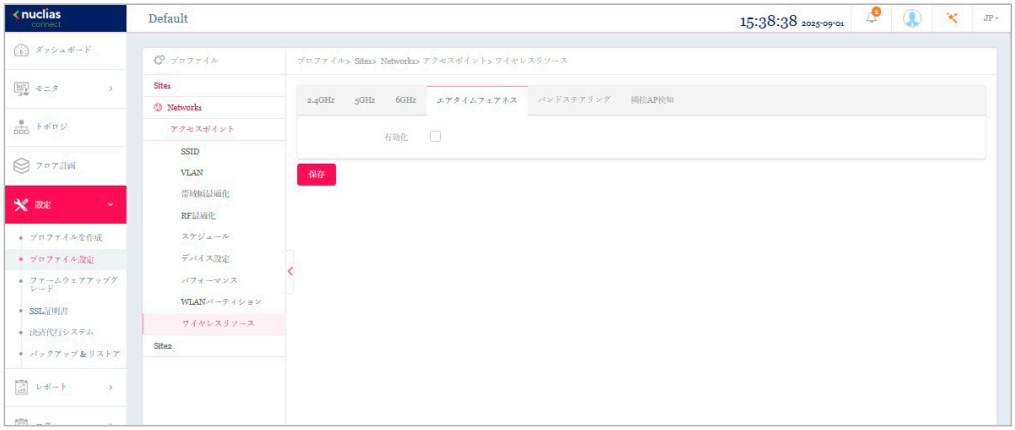


図 8-28　ワイヤレスリソース（「エアタイムフェアネス」タブ）

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

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

補足 「エアタイムフェアネス」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

バンドステアリング（5GHz 優先）

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

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

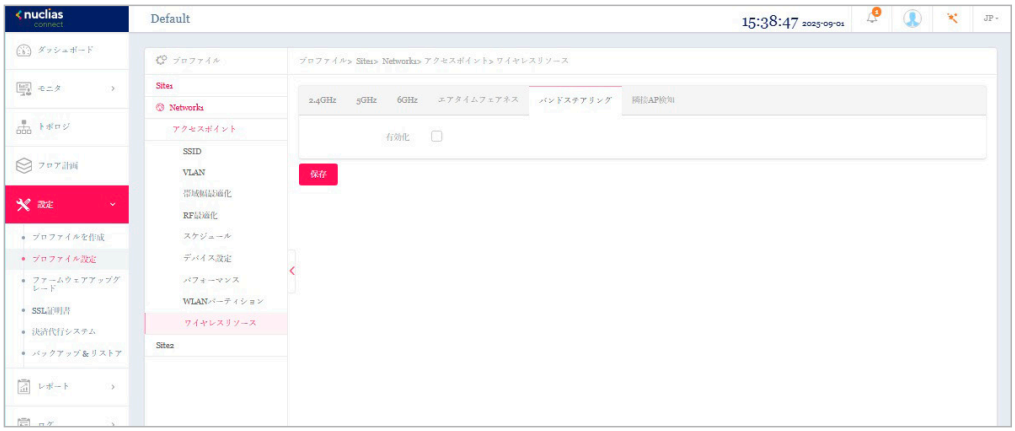


図 8-29　ワイヤレスリソース（「バンドステアリング」タブ）

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

注意 設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

隣接 AP 検知

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

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

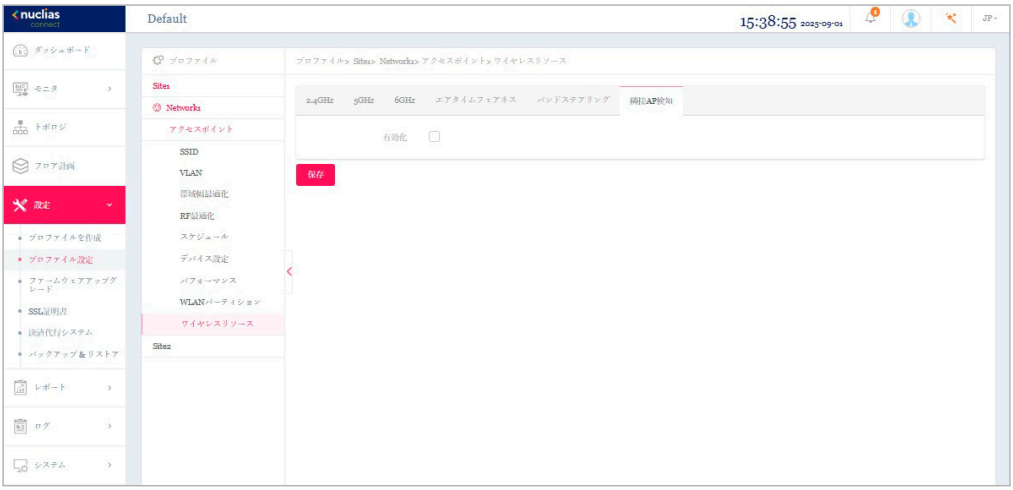


図 8-30　ワイヤレスリソース（「隣接 AP 検知」タブ）

「有効化」のチェックボックスをオンにして検出を有効にし、「保存」をクリックして設定を保存します。

■ 隣接 AP の確認

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

注意　設定を変更する場合、設定内容を更新後、設定をアクセスポイントにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

補足　「隣接 AP」機能は、製品によりサポート可否が異なります。詳細は「【付録】機能別サポート製品 / バージョンについて（p.140）」をご確認ください。

スイッチ - 一般 - RADIUS サーバ

補足　スイッチ製品は未サポートです。

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

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

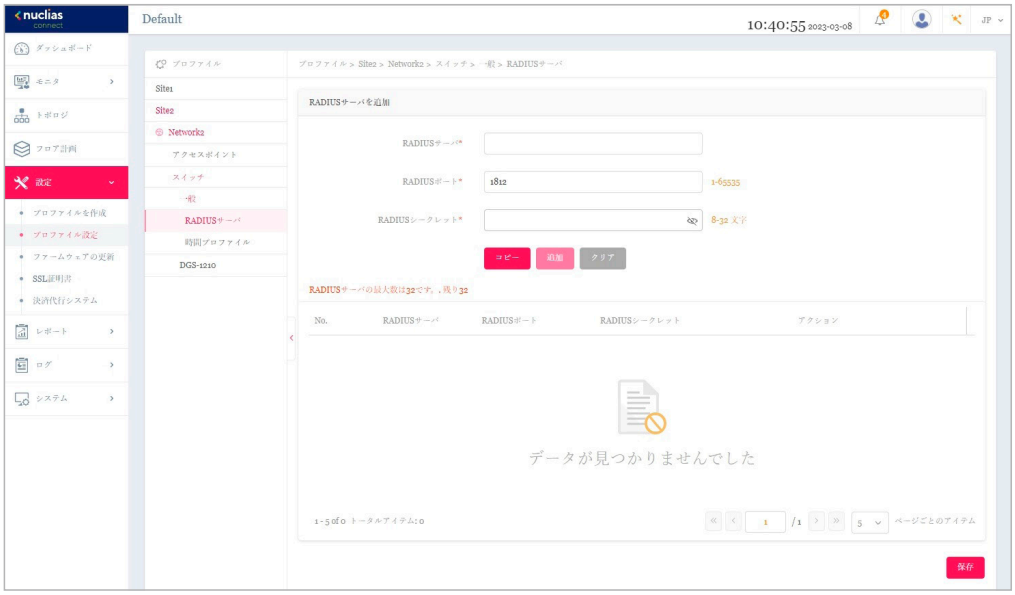


図 8-31　プロファイル設定 - スイッチ - RADIUS サーバ

■ 新規エントリの追加

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

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

■ 既存エントリの変更

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

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

■ RADIUS サーバテーブルの表示・検索

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

図 8-32　RADIUS サーバテーブル

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

スイッチ - 一般 - 時間プロファイル

補足　スイッチ製品は未サポートです。

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

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

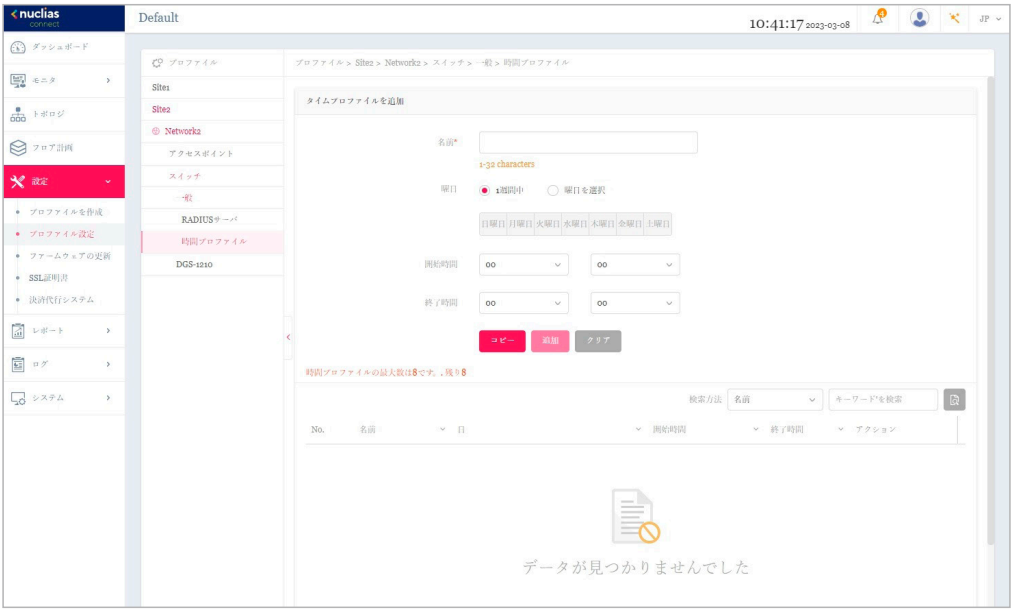


図 8-33　プロファイル設定 - スイッチ - 時間プロファイル

■ 新規エントリの追加

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

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

■ 既存エントリの変更

既存エントリの設定を変更する場合は、対象プロファイルの をクリックします。設定完了後、「保存」をクリックして設定を保存します。

エントリを削除する場合は、対象エントリの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

■ 時間プロファイルテーブルの表示・検索

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

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

図 8-34　時間プロファイルテーブル

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

スイッチ - 基本

補足　スイッチ製品は未サポートです。

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

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

VLAN 設定

このセクションでは、VLAN を追加、編集、または削除できます。

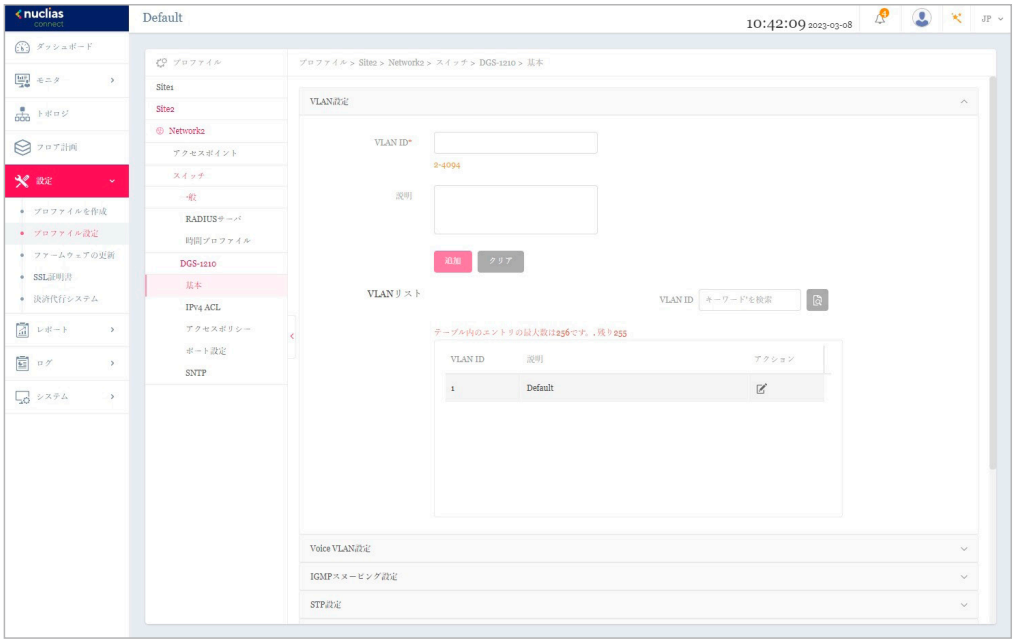


図 8-35　プロファイル設定 - スイッチ - 基本（VLAN）

■ VLAN の追加

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

■ VLAN リストの表示・検索

VLAN リストには、VLAN の概要が表示されます。

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

■ VLAN の編集・削除

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

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

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

Voice VLAN 設定

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

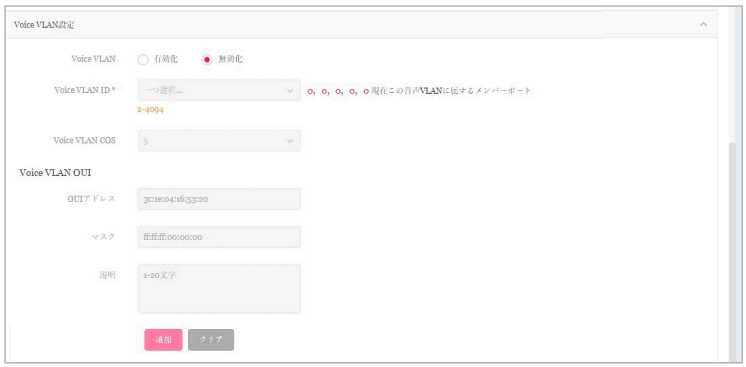


図 8-36　基本（Voice VLAN 設定）

■ 音声 VLAN の設定 / 音声 VLAN OUI の追加

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

   「Voice VLAN ID」フィールドの右側で、音声 VLAN に属するメンバポートの数を確認できます。番号をクリックすると、「ポート設定」画面に移動します。
3. 音声 VLAN のユーザ定義 OUI を追加する場合、「Voice VLAN OUI」セクションで OUI アドレスとその説明を入力します。
4. 「追加」をクリックして、音声 VLAN OUI を追加します。ユーザ定義 OUI は最大 10 件まで作成できます。
   入力した値をリセットするには「クリア」をクリックします。

■ 音声 VLAN OUI リストの表示・検索

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

図 8-37　基本（Voice VLAN 設定 - Voice VLAN OUI）

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

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

IGMP スヌーピング設定

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

図 8-38　基本（IGMP スヌーピング設定）

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

STP 設定

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

図 8-39　基本（STP 設定）

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

DHCP サーバスクリーン設定

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

図 8-40　基本（DHCP サーバスクリーン設定）

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

ジャンボフレームの設定

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

図 8-41　基本（ジャンボフレーム設定）

1. ジャンボフレームを有効または無効に設定します。

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

QoS

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

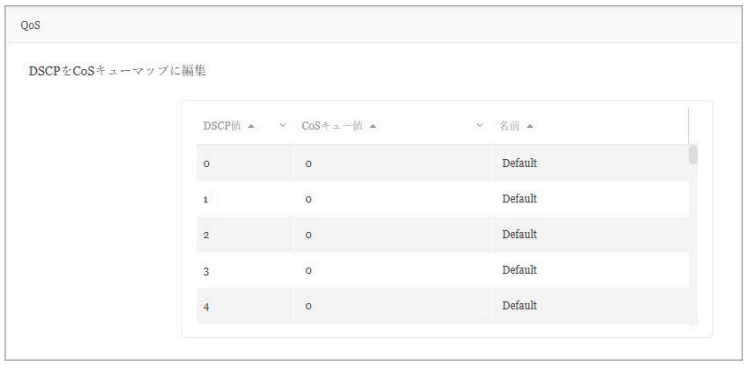


図 8-42　基本（QoS 設定）

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

LBD 設定

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

図 8-43　LBD 設定

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

DDP 設定

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

図 8-44　DDP 設定

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

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

注意 設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

ローカル資格情報設定

お使いのデバイスのユーザ名とパスワードが表示されます。

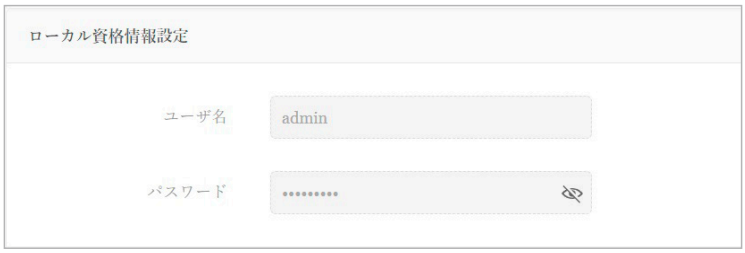


図 8-45　ローカル資格情報設定

スイッチ - IPv4 ACL

補足　スイッチ製品は未サポートです。

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

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

図 8-46　プロファイル設定 - スイッチ - IPv4 ACL

■ ルールの作成

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

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

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

■ ルールの編集・削除

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

ルールを削除する場合は、対象ルールの をクリックします。

設定を中断する場合は、「キャンセル」をクリックします。

設定完了後、画面下部の「保存」をクリックしてプロファイル設定を保存します。

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

スイッチ - アクセスポリシー

補足　スイッチ製品は未サポートです。

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

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

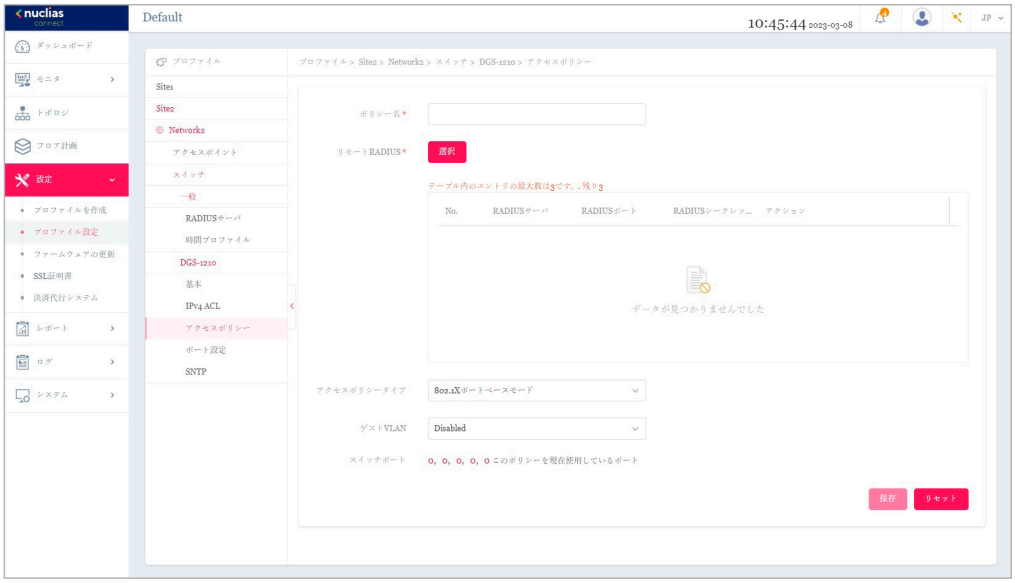


図 8-47　プロファイル設定 - スイッチ - アクセスポリシー

■ アクセスポリシーの作成

次の項目が表示されます。

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

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

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

スイッチ - ポート設定

補足　スイッチ製品は未サポートです。

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

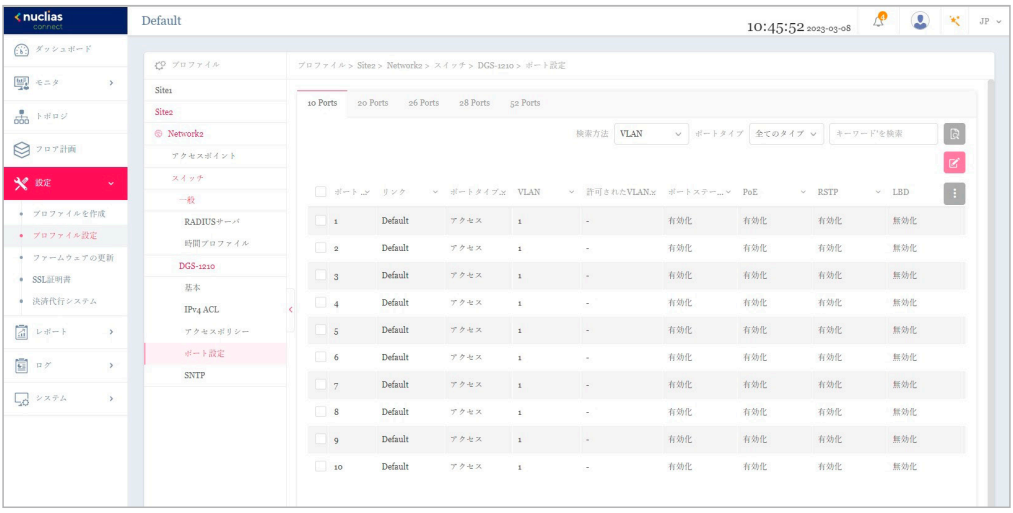


図 8-48　プロファイル設定 - スイッチ - ポート設定

■ 対象範囲の指定 / ポートの検索

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

テーブルには以下の項目が表示されます。

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

■ ポート設定の変更

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

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

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

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

スイッチ - SNTP 設定

補足　スイッチ製品は未サポートです。

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

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

図 8-49　プロファイル設定 - スイッチ - SNTP 設定

次の項目が表示されます。

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

「保存」をクリックして、設定を保存します。

注意　設定を変更する場合、設定内容を更新後、設定をスイッチにアップロードする必要があります。詳細については、「設定のアップロード（p.74）」を参照してください。

ファームウェアアップグレード

本画面では、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。

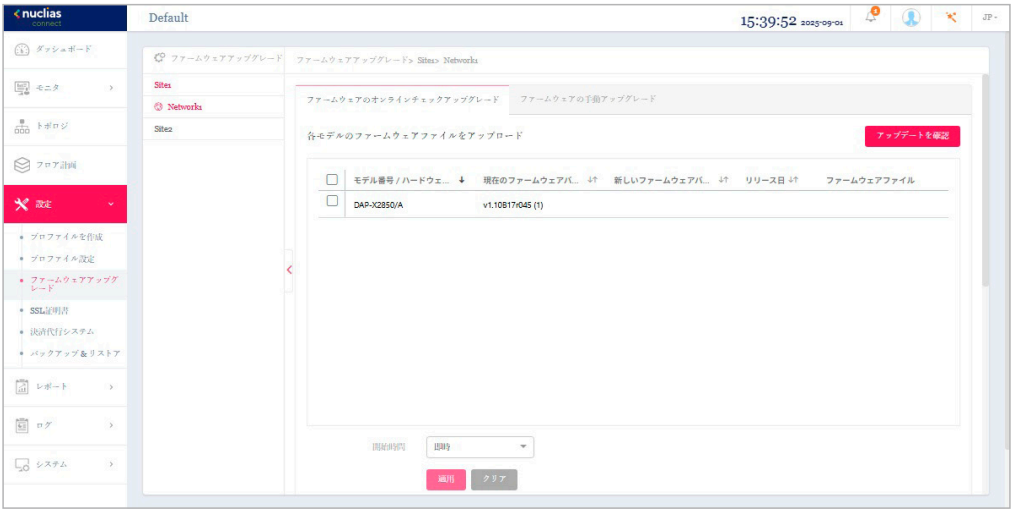


図 8-50　ファームウェアアップグレード

■ ファームウェアのオンラインアップグレード（日本で未サポートのファームウェアを使用しないため、手動更新を使用することを強く推奨します）

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

■ ファームウェアの手動アップグレード

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

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

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

図 8-51　ファームウェアアップグレード - 実行ステータス

SSL 証明書

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

設定 > SSL 証明書 > サイト > ネットワーク に移動します。

図 8-52　SSL 証明書

「SSL 証明書を更新」セクションでは、以下の設定項目が表示されます。

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

「アップロード」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。

注意　SSL 証明書のファイル名にスペースが含まれる場合、1 台のアクセスポイントに対し適用しても実行結果に複数の結果が表示されます。

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。

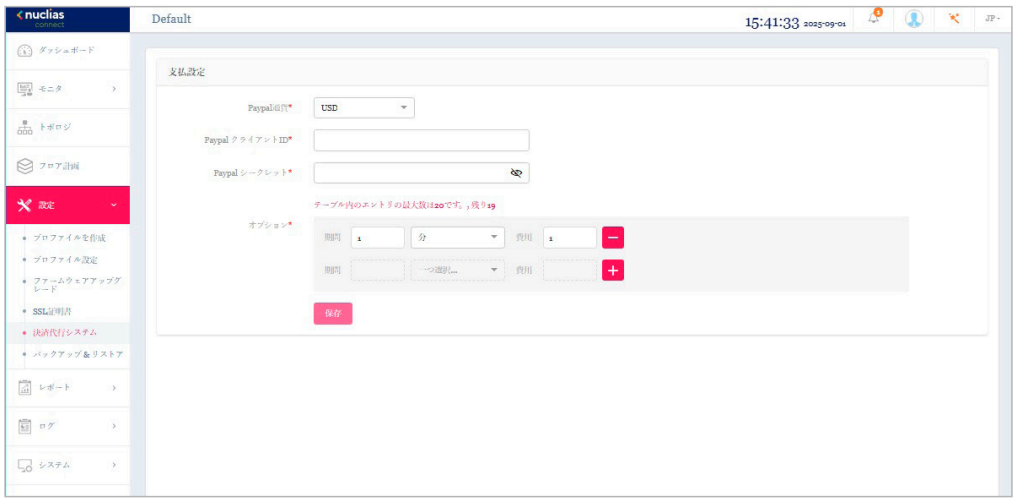


図 8-53　決済代行システム

次の項目が表示されます。

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

「保存」をクリックして設定を保存します。

バックアップ＆リストア

デバイスのバックアップ＆リストアを実行します。

補足　本機能は未サポートです。

設定 > バックアップ＆リストアに移動します。

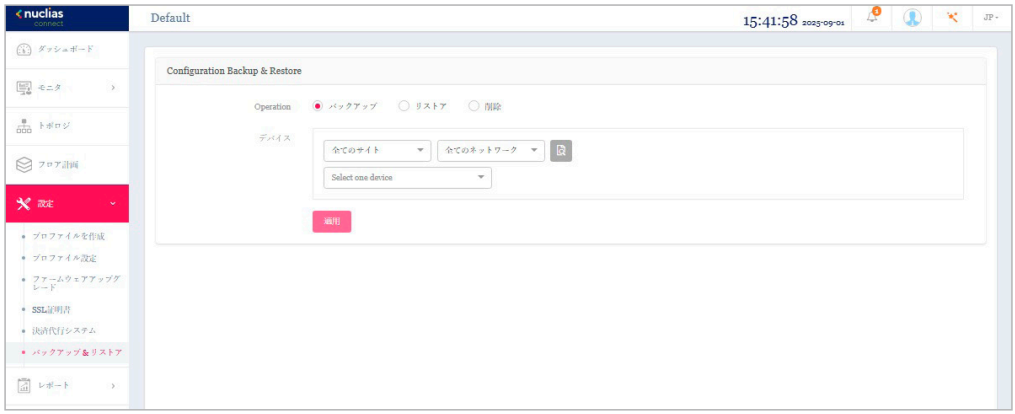


図 8-54　バックアップ＆リストア

次の項目が表示されます。

項目	説明
Operation	コンフィグレーションに対する操作を選択します。 • 選択肢：「バックアップ」「リストア」「削除」
デバイス	対象のデバイスを選択します。

「適用」をクリックして、指定した操作（バックアップ / リストア / 削除）を実行します。

第 9 章　レポート

アクセスポイントのレポート

ピークネットワークアクティビティ

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

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

図 9-1　　アクセスポイント - ピークネットワークアクティビティ

■ 対象範囲の指定

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

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

■ レポート項目

以下のレポートが表示されます。

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

時間別ネットワークアクティビティ

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

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

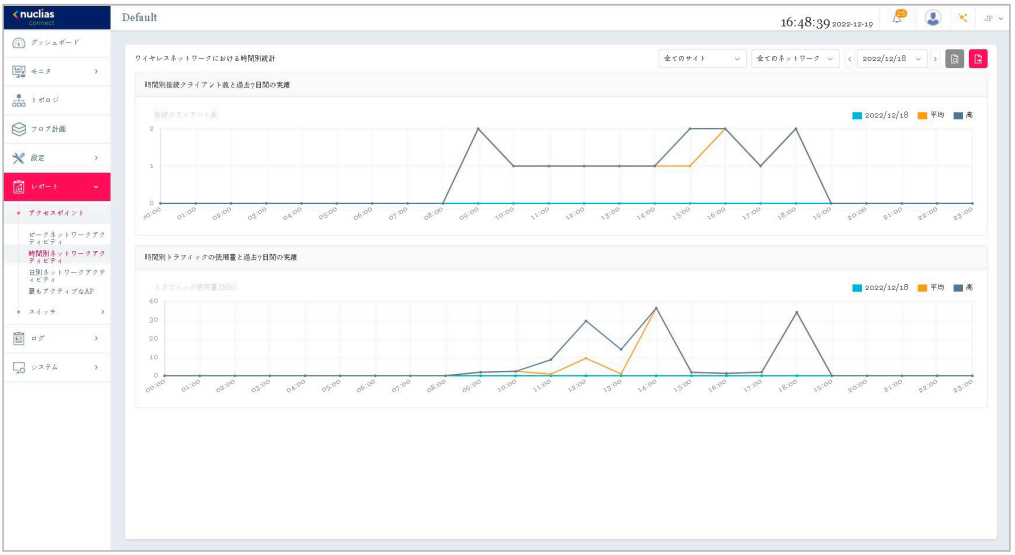


図 9-2　　アクセスポイント - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

以下のレポートが表示されます。

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

日別ネットワークアクティビティ

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

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

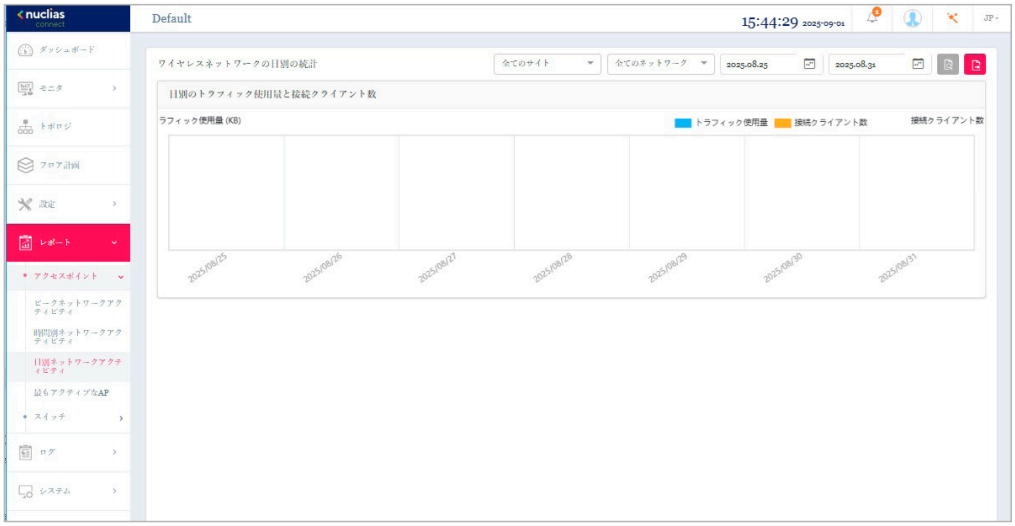


図 9-3　　アクセスポイント - 日別ネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

以下のレポートが表示されます。

- 日別のトラフィック使用量と接続クライアント数

最もアクティブな AP

特定のアクセスポイントのトラフィック使用量を表示します。

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

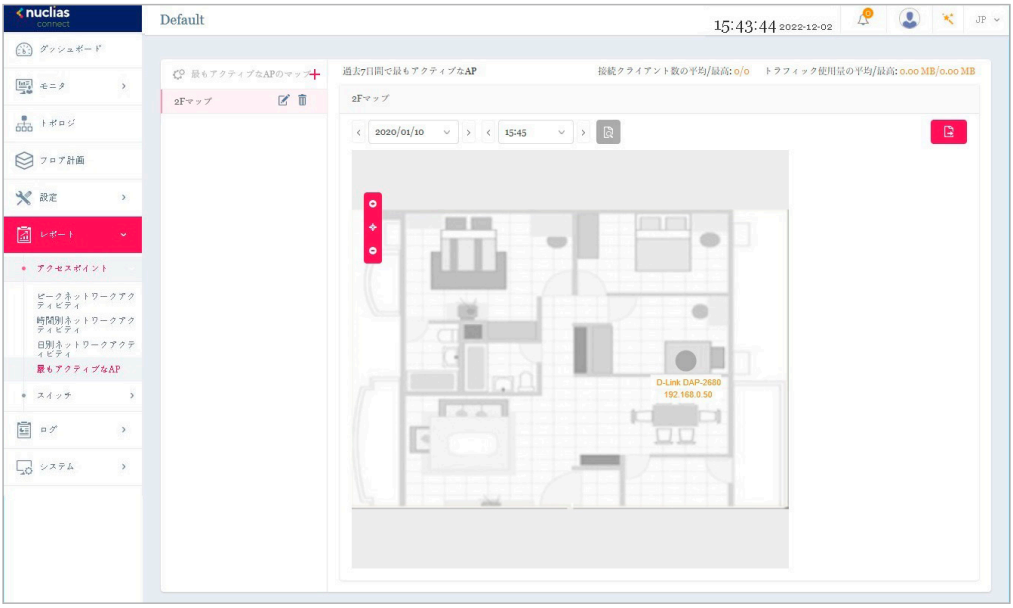


図 9-4　　アクセスポイント - 最もアクティブな AP

■ 対象範囲の指定

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

■ レポート項目

以下のデータが画面右上に表示されます。

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

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

■ マップの作成

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

■ マップの編集・削除

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

スイッチのレポート

時間別ネットワークアクティビティ

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

補足　スイッチ製品は未サポートです。

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

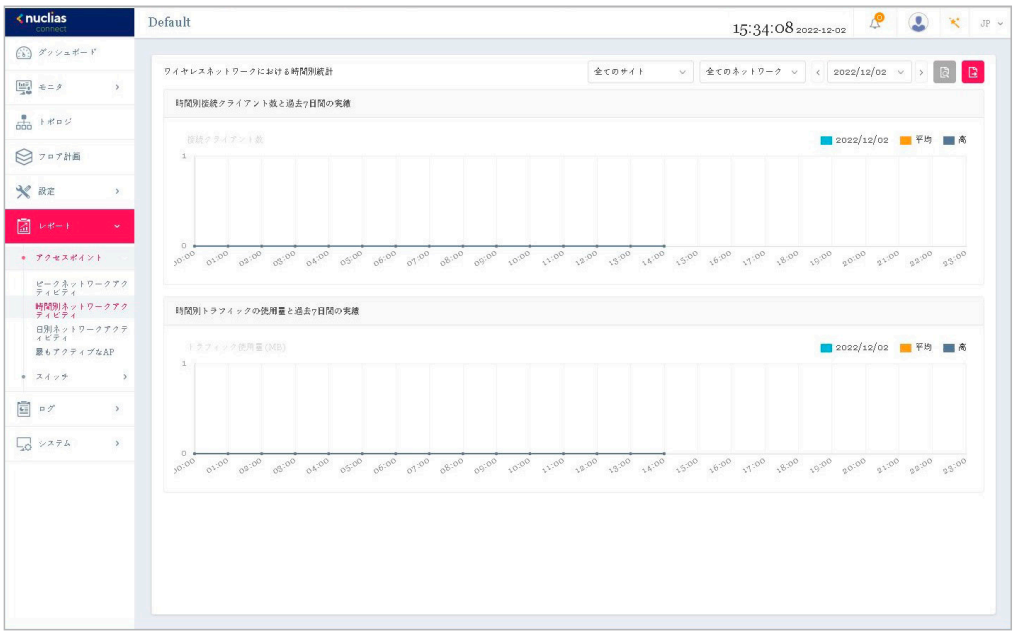


図 9-5　スイッチ - 時間単位のネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

以下のレポートが表示されます。

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

日別ネットワークアクティビティ

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

補足　スイッチ製品は未サポートです。

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

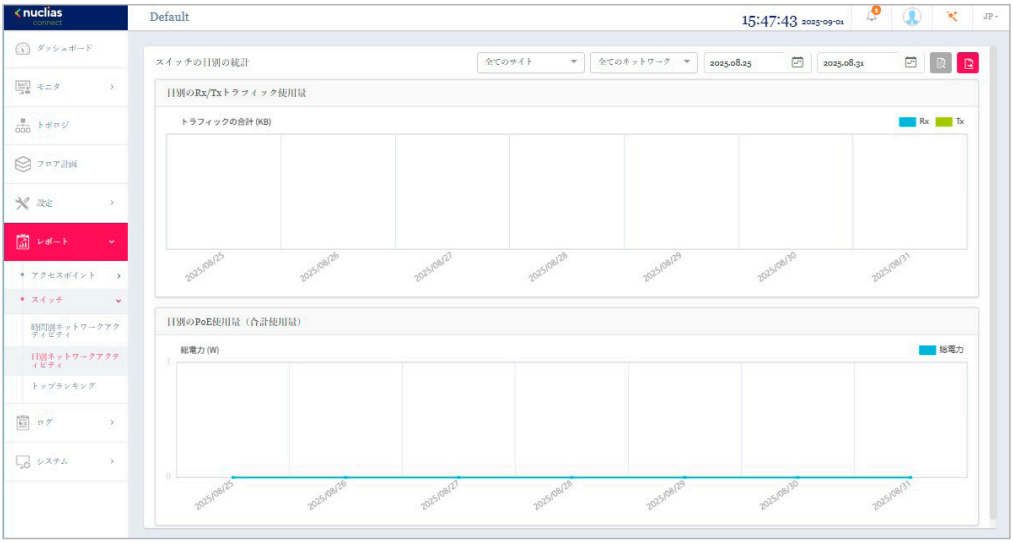


図 9-6　スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

以下のレポートが表示されます。

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

トップランキング

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

補足　スイッチ製品は未サポートです。

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

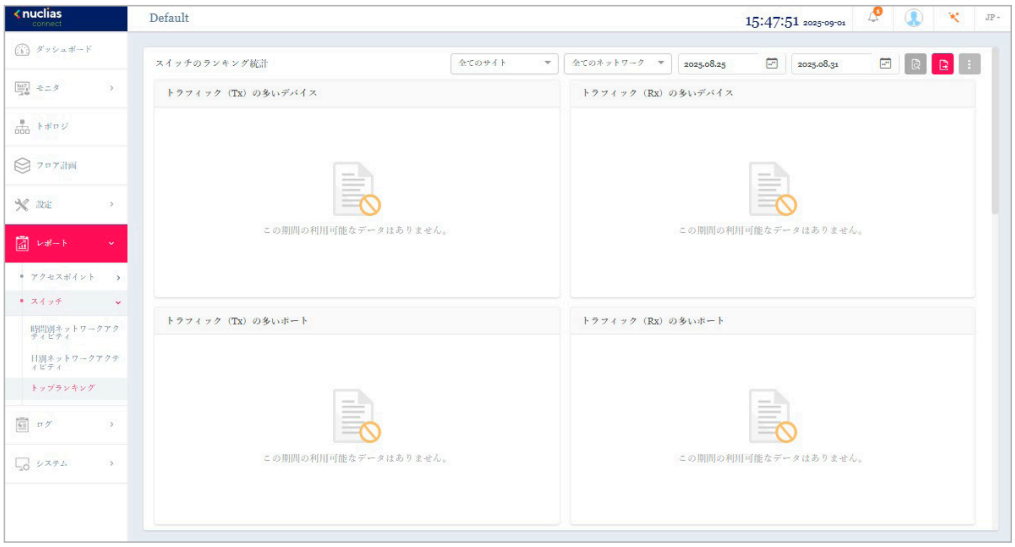


図 9-7　スイッチ - 日別ネットワークアクティビティ

■ 対象範囲の指定

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

■ レポート項目

以下のレポートが表示されます。

- トラフィック（Tx/Rx）の多いデバイス
- トラフィック（Tx/Rx）の多いポート
- エラー（Rx） の多いポート
- 破棄（Rx）の多いポート
- マルチキャスト（Rx）の多いポート
- ブロードキャスト（Rx）の多いポート
- ポート利用率の高いデバイス
- PoE 電力消費の多いデバイス
- CPU 利用率の高いデバイス

第 10 章　ログ

デバイスシスログ

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

ログ > デバイスシスログに移動して、ログ情報を表示します。

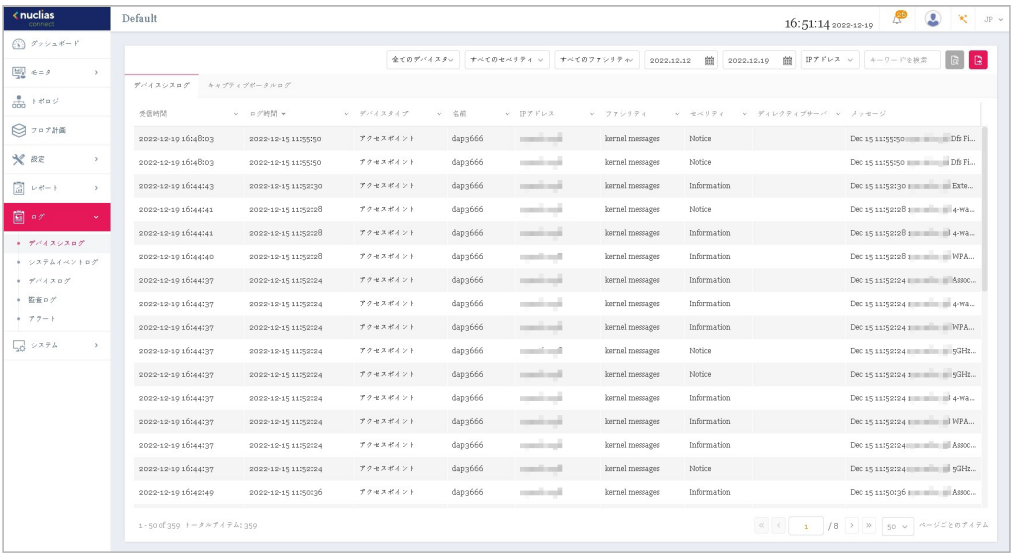


図 10-8　デバイスシスログ

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

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

レポート生成後、をクリックしてレポートを CSV 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ログ」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。

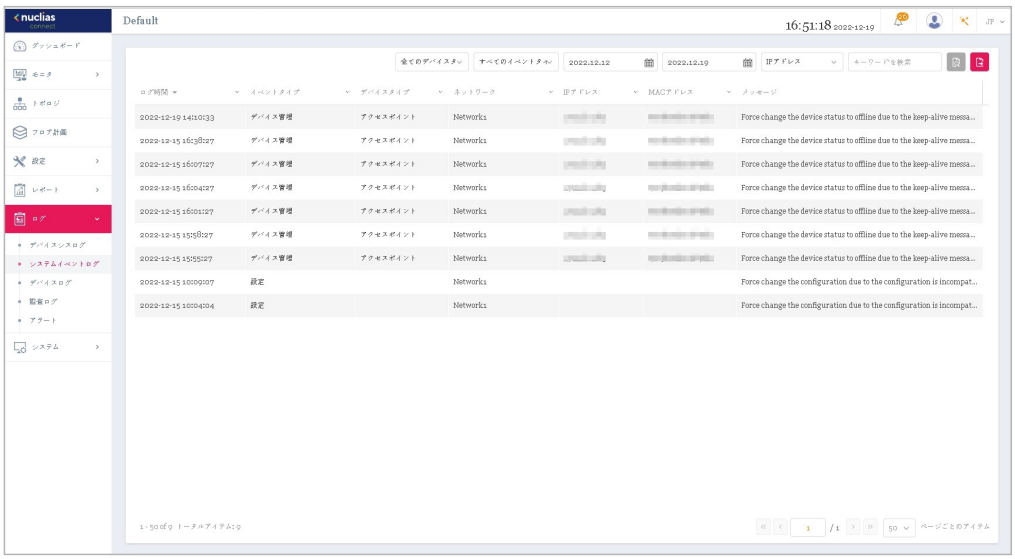


図 10-9　システムイベントログ

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

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

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

デバイスログ

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

ログ > デバイスログに移動して、レポートを表示します。

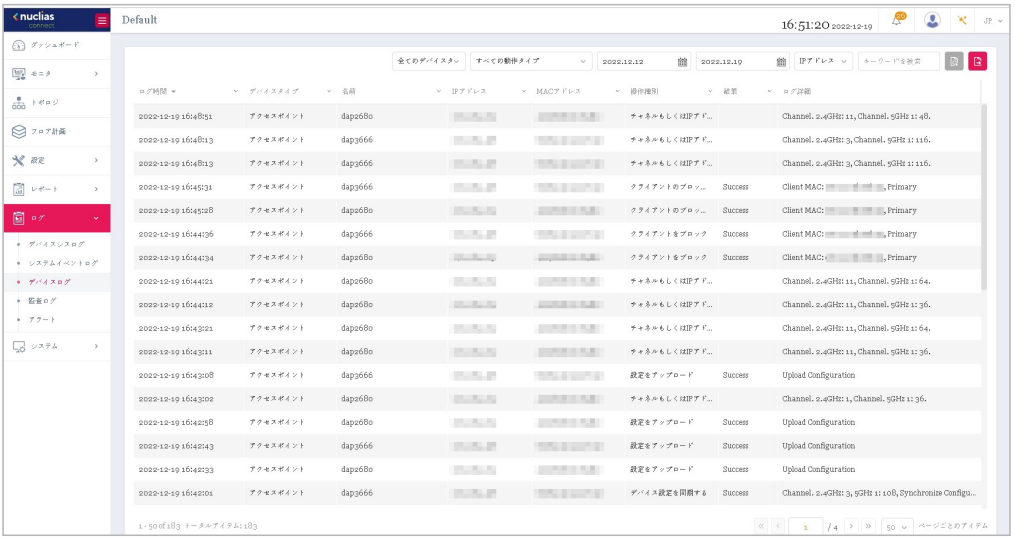


図 10-10　デバイスログ

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

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

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

監査ログ

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

ログ > 監査ログに移動して、レポートを表示します。

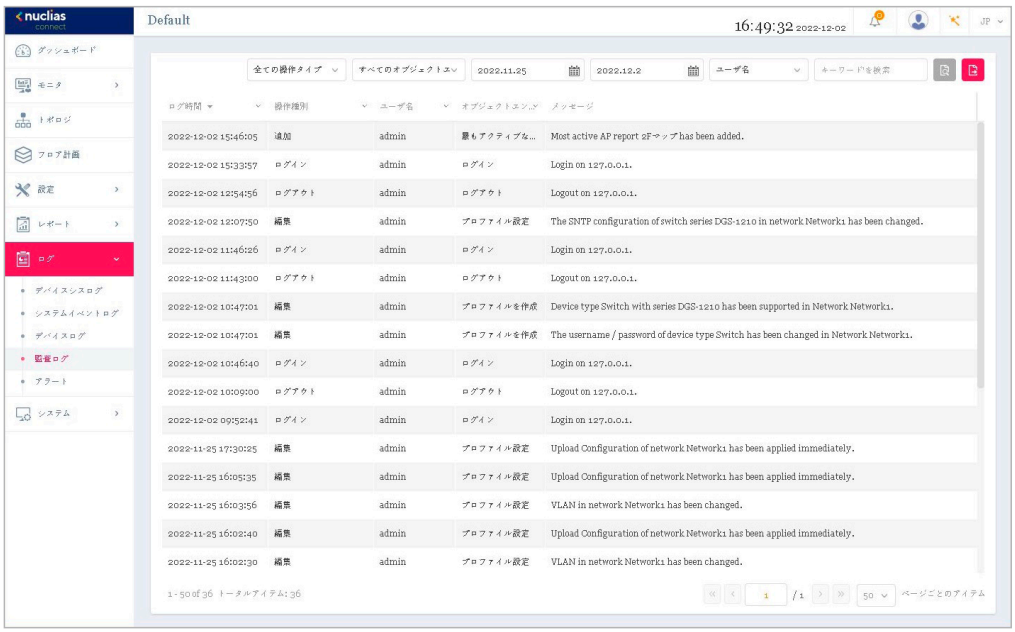


図 10-11　監査ログ

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

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

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

アラート

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

ログ > アラートに移動して、レポートを表示します。

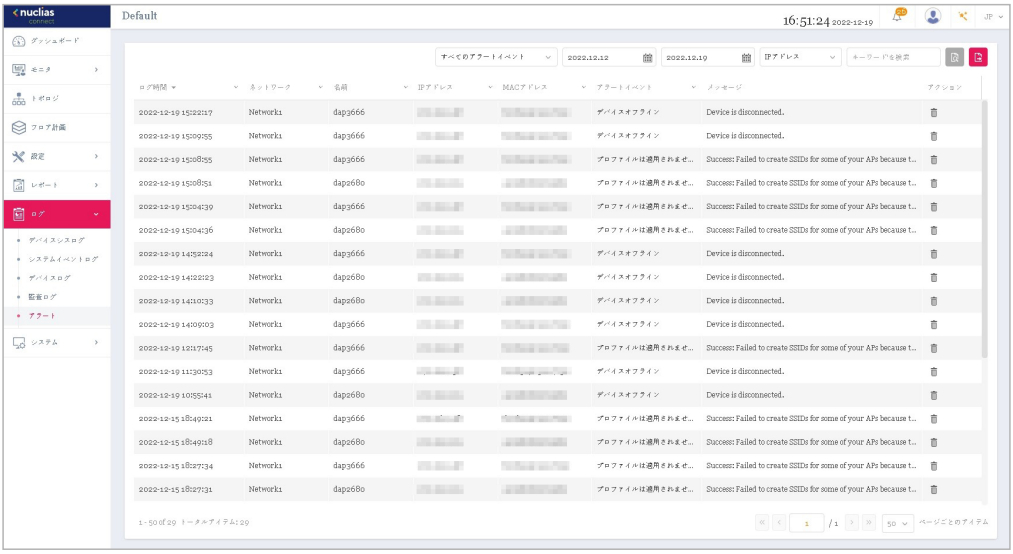


図 10-12　アラート

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

- アラートイベント
- レポート期間
- IP アドレス / メッセージ

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

第 11 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。

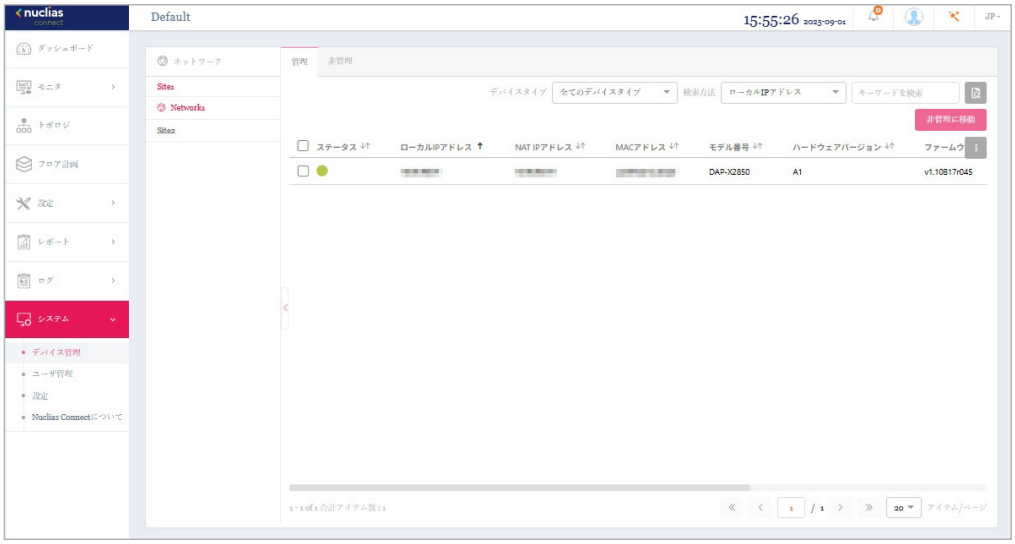


図 11-1　デバイス管理 - 管理タブ

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

■ 管理デバイスリスト / 非管理デバイスリストへの移動と削除

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

■ ネットワークの移動

「非管理」タブに表示されているデバイスは、別のネットワークに移動することができます。

（1）対象のデバイスを選択します。
（2）「管理に移動」左横に表示されるドロップダウンメニューから、別の定義済みネットワークを選択します。
（3）「管理に移動」をクリックします。

■ 表示項目

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

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

補足　管理配下のアクセスポイントに関して、以下の仕様があります。

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

ユーザ管理

ユーザステータス

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

システム > ユーザ管理に移動して、ユーザステータス情報を表示します。

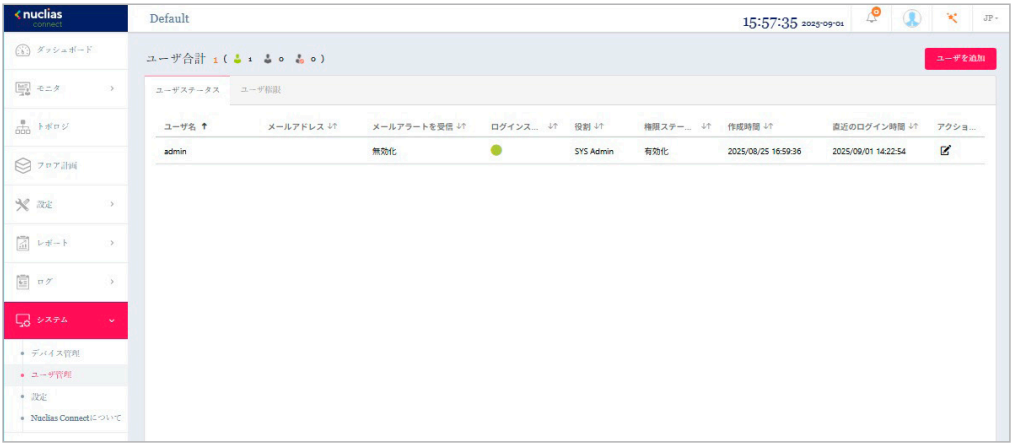


図 11-2　ユーザ管理 - ユーザステータスタブ

■ ログインステータスの確認

「ステータス」欄には、ユーザのログイン状態が表示されます。

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

■ ユーザプロファイルの作成 / 編集

1. ユーザプロファイルを作成するには、「ユーザを追加」をクリックします。
   既存のユーザプロファイルを編集するには、ユーザのアクション欄で をクリックします。

2. 以下の項目を設定します。
   - 「ユーザ名」
   - 「パスワード」
   - 「メールアドレス」
   - 「メールアラートを受信」
   - 「権限」
   - 「権限ステータス」
   - 「Authority Reduction」（ローカル管理者 / ローカルユーザのみ）
   - 「設置場所」
   - 「電話番号」
   - 「説明」

「権限」では、以下のユーザ権限を割り当てることができます。

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

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

「Authority Reduction」では、以下の権限を割り当てることができます。（ローカル管理者 / ローカルユーザのみ）

項目	説明
「ローカル管理者」を選択した場合	
Device Deployment	本項目にチェックを入れた場合、管理対象のネットワークに対してネットワーク定義を設定することができます。
Profile configurations	本項目にチェックを入れた場合、管理対象のネットワークに対してプロファイルなどのデバイス設定を行うことができます。

項目	説明
「ローカルユーザ」を選択した場合	
Access Dashboard/Monitor/ Report pages only	本項目を選択した場合、管理対象のネットワークについて、ダッシュボード / モニタ / レポート画面の閲覧が可能です。
All	本項目を選択した場合、管理対象のネットワークについて、ダッシュボード / モニタ / トポロジ / フロア計画 / 設定 / レポート / ログ / システム（「ユーザ管理」を除く）の閲覧が可能です。

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

図 11-3　ユーザを作成

ユーザ権限

「ユーザ権限」タブでは、ユーザ毎に管理可能なネットワークを設定することができます。

システム > ユーザ管理に移動し、「ユーザ権限」タブを選択します。

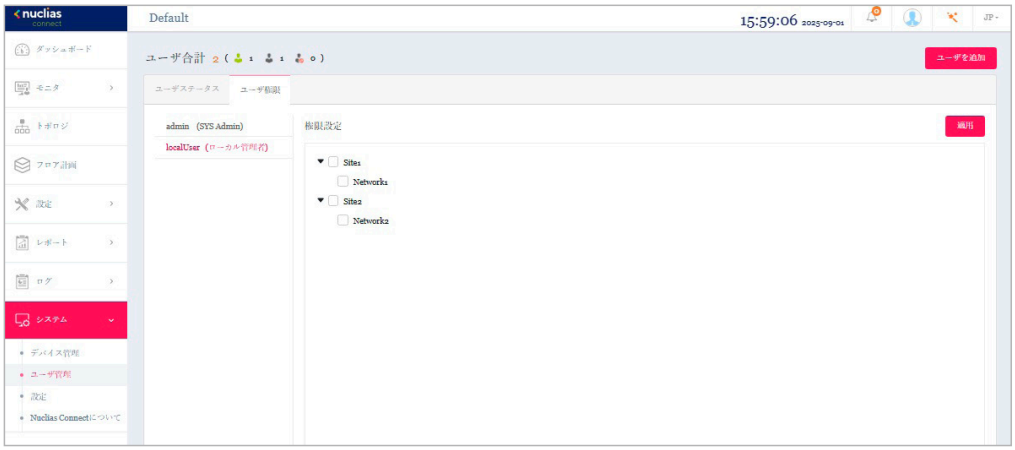


図 11-4　ユーザ管理 - ユーザ権限タブ

■ ユーザ権限の設定

1. 設定を行うユーザを選択します。
2. 管理対象とするサイト / ネットワークにチェックを入れます。
3. 「適用」をクリックして設定を保存します。

設定

「設定」画面には、以下のタブが表示されます。

- 「一般」
- 「接続」
- 「SMTP」
- 「バックアップ＆リストア」
- 「REST API」
- 「シングルサインオン（SSO）」
- 「アラート」
- 「FOTA」
- 「クライアントの説明」
- 「Remote Access」

一般

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

システム > 設定に移動して、「一般」タブを表示します。

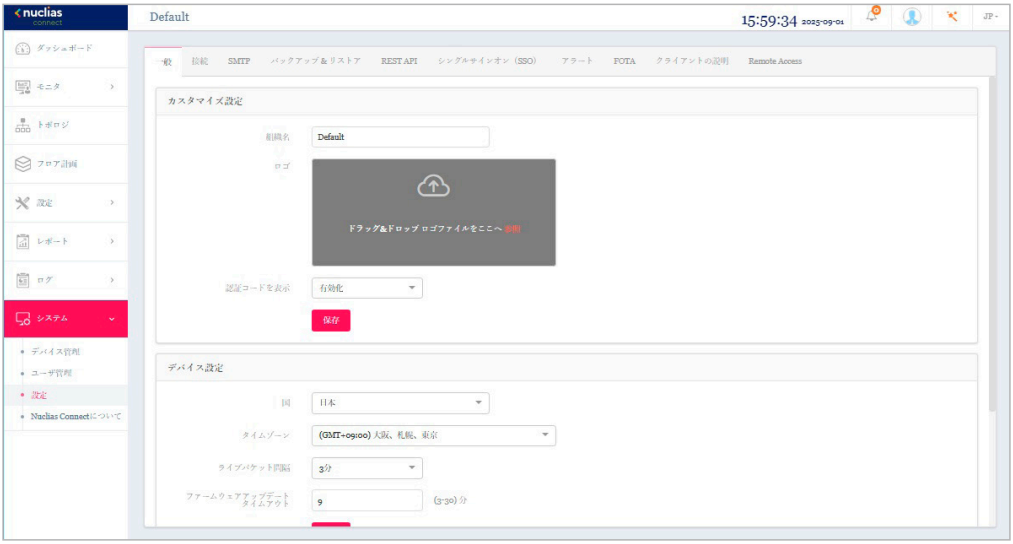


図 11-5　設定 - 一般タブ

■ カスタマイズ設定

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

「保存」をクリックして設定を保存します。

■ デバイス設定

項目	説明
国	ドロップダウンメニューをクリックして、ネットワーク内のアクセスポイントの国を選択します。 「日本」から設定変更しないでください。
タイムゾーン	ドロップダウンメニューをクリックして、タイムゾーンを選択します。
ライブパケット間隔	ドロップダウンメニューをクリックして、ライブパケット間隔時間を選択します。 • 選択肢：1-10 分
ファームウェアアップデートタイムアウト	FOTA（未サポート）のファームウェアアップデートのタイムアウトを設定します。

「保存」をクリックして設定を保存します。

■ データベース内の保存データをクリア

「レポート」「ログ」のチェックボックスにチェックを入れ「クリア」をクリックすると、データベース内の保存データが削除されます。

接続

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

システム > 設定に移動し、「接続」タブをクリックします。

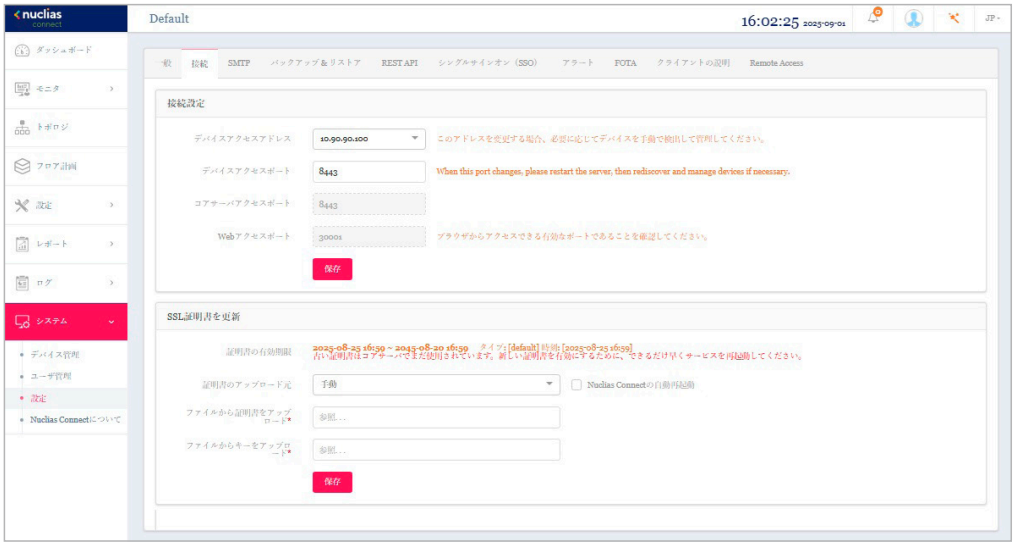


図 11-6　設定 - 接続タブ

■ 接続設定

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

「保存」をクリックして設定を保存します。

■ SSL 証明書を更新

項目	説明
証明書の有効期限	証明書の有効期限が表示されます。
証明書のアップロード元	証明書のアップロード元として手動または自動を選択します。 • 選択肢「手動」「自動 Cerbot」 SSL 証明書を更新した後、システムの自動再起動を行うには、「Nuclias Connect の自動再起動」にチェックを入れます。
ファイルから証明書をアップロード	「手動」を選択した場合、「参照…」をクリックして、アップロードする SSL 証明書ファイルを選択します。
ファイルからキーをアップロード	「手動」を選択した場合、「参照…」をクリックして、アップロードする SSL キーファイルを選択します。
システムの FQDN	「自動 Cerbot」を選択した場合、システムの FQDN を入力します。
サブスクライバーの電子メール	「自動 Cerbot」を選択した場合、サブスクライバーの電子メールを入力します。

「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。

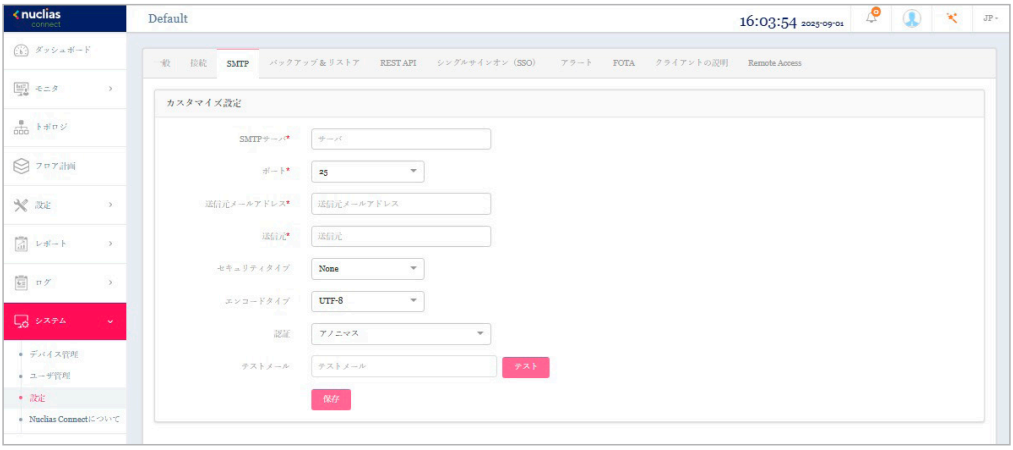


図 11-7　設定 - SMTP タブ

以下の設定項目が表示されます。

項目	説明
SMTP サーバ	SMTP サーバの IP アドレスまたはドメイン名を入力します。
ポート	SMTP サーバのポート番号を指定します。 • 選択肢：「25」「465」「587」
送信元メールアドレス	送信者のメールアドレスを入力します。
送信元	送信者の名前を入力します。
セキュリティタイプ	ドロップダウンメニューをクリックして、電子メールシステムで使用するセキュリティタイプを選択します。 • 選択肢：「None」「SSL」
エンコードタイプ	ドロップダウンメニューをクリックして、電子メールクライアントと一致するエンコードタイプを選択します。 • 選択肢：「UTF-8」「ASC-II」
認証	ドロップダウンメニューをクリックして、ログイン中の認証メカニズムを選択します。 • 選択肢：「アノニマス」「SMTP 認証」
ユーザ名	認証で「SMTP 認証」を選択した場合は、SMTP サーバの認証ユーザ名を入力します。
パスワード	認証で「SMTP 認証」を選択した場合は、SMTP サーバの認証パスワードを入力します。
テストメール	受信者の電子メールアドレスを入力して、SMTP サーバ経由の電子メールのテスト送信を行います。「テスト」をクリックしてテスト送信を開始します。

「保存」をクリックして設定を保存します。

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

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

バックアップ & リストア

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

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

■ 自動バックアップ

コンフィグレーションの自動バックアップ設定を行います。

図 11-8　自動バックアップ設定

「自動バックアップ設定」セクションには、以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

■ バックアップ設定

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

図 11-9　バックアップ設定

「バックアップ設定」セクションには、以下の設定項目が表示されます。

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

■ リストア設定

コンフィグレーションのリストアを行います。

図 11-10　リストア設定

「リストア設定」セクションには、以下の設定項目が表示されます。

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

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

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

REST API

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

システム > 設定に移動し、「REST API」タブをクリックします。

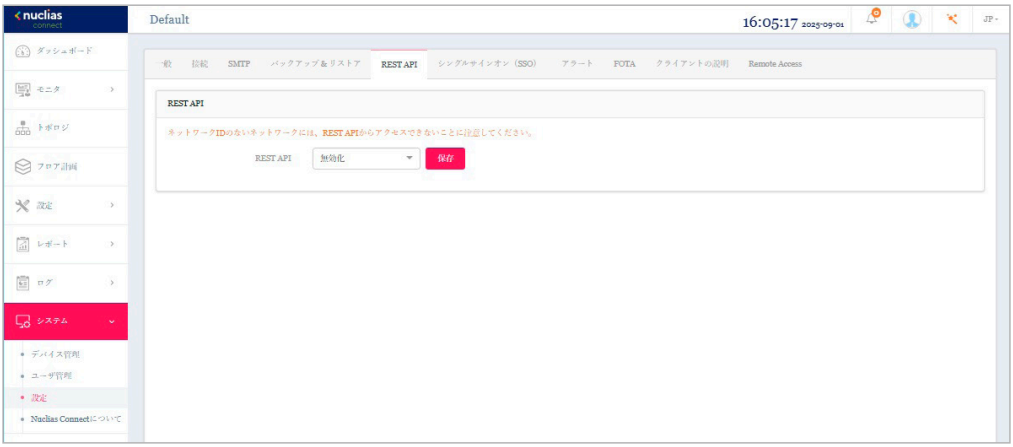


図 11-11　設定 - REST API タブ

以下の設定項目が表示されます。

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

「保存」をクリックして設定を保存します。

シングルサインオン（SSO）

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

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

図 11-12　設定 - シングルサインオン（SSO）タブ

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

■ アカウントの登録

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

図 11-13　地域 / 国の選択

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

図 11-14　アカウント情報の入力

3. 入力後、CAPTCHA 認証を行い、「アカウントの作成」をクリックします。

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

■ シングルサインオン設定

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

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

「ログイン」をクリックします。

■ Nuclias Connect ポータルへの接続

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

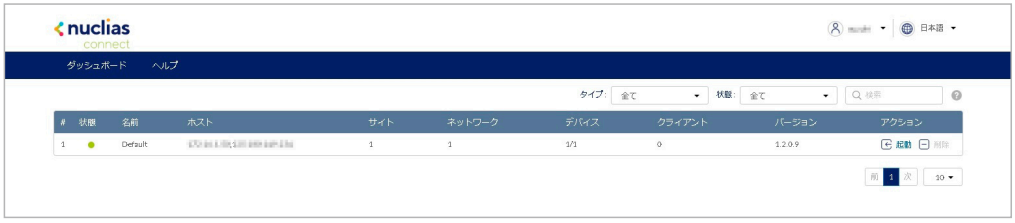


図 11-15　Nuclias Connect ポータル

Nuclias Connect ポータルでは、以下の項目が表示されます。

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

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

アラート

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

システム > 設定に移動し、「アラート」タブをクリックします。

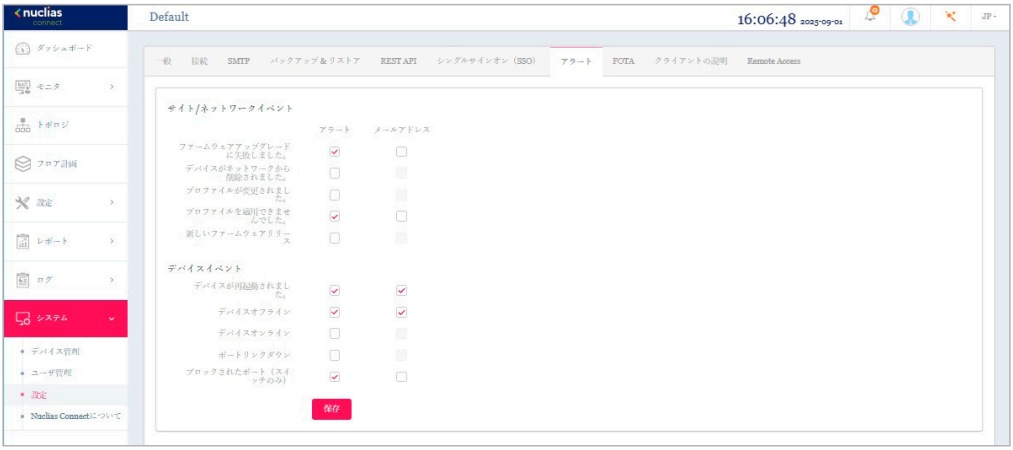


図 11-16　設定 - アラートタブ

■ アラートの設定

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

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

■ 生成されたアラートの確認

生成されたアラートは、**ログ > アラート**に移動して確認できます。

■ 電子メールアラートの設定

電子メールでアラートを受信するには、以下の設定を行います。

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

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

注意　デバイス再起動時のアラートログは、DAP-2680/DAP-2610 ではサポートされません。

FOTA

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

システム > 設定に移動し、「FOTA」タブをクリックします。

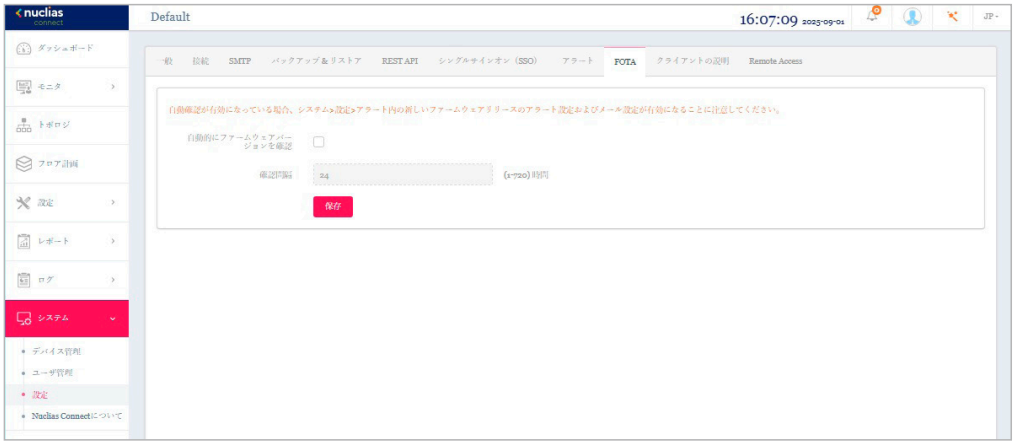


図 11-17　設定 - FOTA タブ

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

クライアントの説明

クライアント MAC アドレスを識別し易くするための説明を定義します。
MAC アドレスの説明は、クライアントモニタ画面の表示項目などで確認することができます。

システム > 設定に移動し、「クライアントの説明」タブをクリックします。

図 11-18　設定 - クライアントの説明タブ

ドロップダウンメニューから以下の項目を選択し、MAC アドレス説明の設定や表示を行います。

項目	説明
MAC 説明リスト	1. ドロップダウンメニューから「MAC 説明リスト」を選択し、＋をクリックして新しいエントリを設定します。 2. 以下の項目を入力します。 ・「クライアント MAC アドレス」：クライアントの MAC アドレスを入力します。 ・「説明」：MAC アドレスに対する説明を入力します。 3. 「保存」をクリックします。 をクリックして、MAC アドレスリストのファイルをアップロードすることもできます。
説明のない MAC アドレス	接続クライアントや ACL で使用される MAC アドレスのうち、説明が定義されていないエントリを表示します。 「ACL」「Wireless Client」「Switch Client」から対象を選択します。
MAC 説明は使用されません。	接続クライアントや ACL で使用されていない MAC アドレスを表示します。

エントリを削除する場合は、削除するエントリのアクション欄で をクリックします。
または、削除するエントリのチェックボックスにチェックを入れ、 をクリックします。

クライアントの説明リストをエクスポートするには、（検索アイコン）右横のをクリックします。

Remote Access

リモートアクセスの設定を行います。

注意　スイッチ管理は未サポートです。

システム > 設定に移動し、「Remote Access」タブをクリックします。

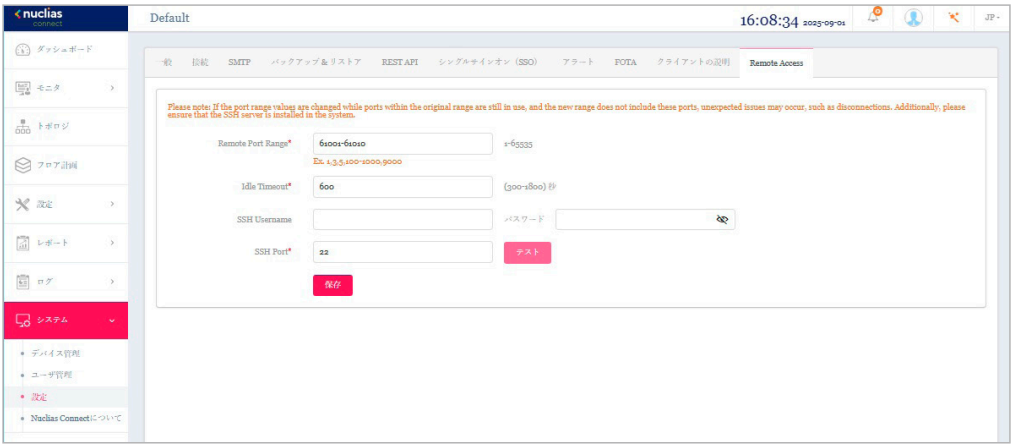


図 11-19　設定 - Remote Access タブ

以下の設定項目が表示されます。

項目	説明
Remote Port Range	リモート接続のポート範囲を設定します。 • 設定可能範囲：1 - 65535 • 初期値：61001 - 61010
Idle Timeout	アイドルタイムアウトを設定します。 • 設定可能範囲：600 • 初期値：300 - 1800
SSH Username	SSH ユーザ名を設定します。
パスワード	SSH パスワードを設定します。
SSH Port	SSH ポートを設定します。

「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 11-20　Nuclias Connect について

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

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

【付録】機能別サポート製品 / バージョンについて

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

項目	サポートされる製品 / バージョン	
	スタンドアロンモード	DNC-100 管理モード
プロファイル設定 - アクセスポイント - SSID - セキュリティ		
高速ローミング（802.11 k/r）	• DAP-3666	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）
Enhanced Open	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）
WPA3	• DAP-X2850 • DAP-3666 • DAP-2610（v2.06B06r097 以上） • DAP-X2810（v1.20r032 以上）	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）
ネットワークアクセス保護	• DAP-X2850 • DAP-X2810 • DAP-2680 • DAP-2610	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2680（v2.00B08r051 以上） • DAP-2610（v2.01B05r073 以上）
プロファイル設定 - アクセスポイント - SSID - ユーザ認証		
外部キャプティブポータル認証	—	• DAP-X2850 • DAP-3666 • DAP-2610（v2.06B06r097 以上）
MAC アドレス認証	—	• DAP-X2850 • DAP-3666（v1.11b02r095 以上） • DAP-2610（v2.06B06r097 以上）
クリックスルー認証	• DAP-X2850 • DAP-3666	• DAP-X2850 • DAP-3666 • DAP-2610（v2.06B06r097 以上）
ウォールガーデン	• DAP-2610（v2.06B06r097 以上）	• DAP-X2850 • DAP-3666 • DAP-2610（v2.06B06r097 以上）
同時ログイン	—	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）
セッションタイムアウト	—	• DAP-X2850 • DAP-X2810（v1.20r032 以上） • DAP-3666 • DAP-2610（v2.06B06r097 以上）
リモート RADIUS 認証 - NAS ID	• DAP-2610（v2.06B06r097 以上）	• DAP-X2850 • DAP-2610（v2.06B06r097 以上）
リモート RADIUS 認証 - アカウンティングサーバ設定	• DAP-X2850 • DAP-2610（v2.06B06r097 以上）	• DAP-X2850 • DAP-2610（v2.06B06r097 以上）
プロファイル設定 - アクセスポイント - SSID - Hotspot2.0		
Hotspot2.0	• DAP-3666	• DAP-3666
プロファイル設定 - アクセスポイント - RF 最適化		
RF 最適化	—	• DAP-X2850 • DAP-3666 • DAP-2680（v2.00B08r051 以上） • DAP-2610（v2.01B05r073 以上）
パフォーマンス設定		
STP（スパニングツリー）※1	• DAP-X2850 • DAP-3666	• DAP-X2850 • DAP-3666

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

※ 1　DAP-X2810 の STP（スパニングツリー）は、v1.20r032 以降でサポートされ、初期値で有効（設定変更不可）となります。
※ Nuclias Connect 対応製品のみ掲載しています。