POPCHAT, Inc.

POPCHAT シリーズ

製品マニュアル

Ver.3.2.0 版

2021 年 01 月

POPCHAT 株式会社

POPCHAT, Inc.

はじめに

この度は、本製品をご購入頂き、誠にありがとうございます。本製品は、ホテル、旅館、大学、企業等でインターネットサービスを提供するために必要な、様々な機能が盛り込まれた次世代型コミュニケーションサーバです。本製品には、従来の POPCHAT の機能である、利用者端末のネットワーク設定の変更を不要とするプラグ＆プレイ機能、任意のWebサイトへのリダイレクト、利用者管理など多彩な機能が実装されております。

また、保守メニューをご契約頂くことで、弊社サポートセンターへの設定やログのバックアップ、リモート切り分け、ソフトウェアのアップグレード、設定済み代替機の先出し発送など、様々な付加価値をご提供することができます。

製品マニュアルの主旨

本製品マニュアル（以下、マニュアル）は、本製品の操作方法や搭載機能を知るための参考資料としてお使いいただけます。事前の同意を得ることなく、本マニュアルを複写、転用、転載、修正、他言語への翻訳を行うことは禁止されています。本マニュアルに記載される内容は、事前通告なしに変更される場合があります。特に記載のない限り、本マニュアルで使用される会社名、氏名、データなどは架空のものを使用しております。

極めて高い信頼性が必要とされる環境での使用について

極めて高い信頼性が必要とされる用途（鉄道、航空、医療用等での使用のうち、通信障害による影響度が極めて高いシステム、人命に直接影響するシステム）に使用されることを意図した設計・製造はされておりません。

これらの設備は機器、制御システム体系の中に本製品を組み込んで使用される場合、安全性、信頼性の確保について、自己責任で万全を期するようご注意ください。

商標について

Apple、Mac OS、Macintosh、iOS、iPhone は、米国その他の国で登録された米国アップルコンピューター社の商標です。Windows、MS-DOS は、米国 Microsoft Corporation の米国及びその他の国における登録商標です。Android は Google LLC の米国及びその他の国における登録商標です。

その他、この文書に掲載されているソフトウェア及び周辺機器の名称はそれぞれのメーカーの商標、または登録商標です。

廃棄方法について

本製品の使用済みの際には、当社に回収依頼（都度見積り）のご連絡をいただくか、
もしくは、それぞれの自治体の定める廃棄方法（自己負担）に従ってください。

回収依頼ご連絡先：POPCHAT サポートチーム＜contact@popchat.jp＞

使用上のご注意

本製品を安全にご使用いただくために、以下の事項を必ず守って下さい。

本書中のマーク

注意

この表示を無視して、誤った取り扱いをすると、データの損失や、機器の故障の恐れがあります。

警告

この表示を無視して、誤った取り扱いをすると、火災・感電により人が死亡または重傷を負う恐れがあります。

注意

取り扱いは丁寧に

落としたり、ぶつけたり、強いショックを与えたりしないでください。

動作温度

本製品は、指定された動作周囲温度の範囲で、ご使用ください。動作可能な周囲温度範囲は、マニュアルに記載されています。特に、本製品をラックなどに組み込んでご使用になる場合、換気には充分ご注意ください。また、専用のラックが存在する製品については必ず専用のものをご使用ください。

日常のお手入れ

本製品の汚れは、やわらかい乾いた布でふいてください。ベンジン、シンナーなどは使用しないでください。製品の変形、変色の原因になります。

次のような場所での使用や保管はしないでください

・直射日光の当たる場所
・暖房器具の近くなどの高温になる場所
・急激な温度変化のある場所（結露するような場所）
・湿気の多い場所や、水などの液体がかかる場所
・振動の激しい場所
・ほこりの多い場所や、ジュータンを敷いた場所（静電気障害の原因にもなります）
・腐食性ガスの発生する場所

警告

カバーを外さないでください

本製品の内部には高電圧の箇所が存在します。感電の恐れがありますので、マニュアルに記載がある場合を除いて、絶対にカバーを外さないでください。ユーザーに必要な部品は内包されていません。

正しい電源を使ってください

本製品は、付属の電源ケーブルに明記された電圧範囲で動作します。ご使用の前に必ずご確認ください。

正しい電源ケーブル及びコンセントを使ってください

本製品に電源を供給する場合には、本製品付属の電源ケーブルをご使用してください。また、電源ケーブルを同梱した本製品以外の電気製品に使用しないでください。
電源ケーブルは無理に折り曲げたり、引っ張ったり、ねじったりしないでください。また、圧力がかかりコードがつぶれてしまうような箇所に敷設しないでください。
テーブルタップをご使用になる場合、たこ足配線をしないでください。たこ足配線は、火災の原因となる場合があります。また精密部品に静電気が溜りますので、アースの付いた 3 極コンセントをご使用ください。

ものを載せないでください

本製品の上にものを載せないでください。上にものを載せた状態で使用すると加熱などにより、故障、火災の恐れがあります。

異物を入れないでください

換気口、拡張スロットなどから金属、液体などの異物を入れないでください。本体内部に異物が入ると火災、感電などの恐れがあります。

設置、ケーブル配線、移動は電源を抜いて

本製品の設置、ケーブル配線、移動などを行う場合は、必ず電源ケーブルを抜いてから行ってください。

埃に注意してください

電源プラグや、電源アダプタは、埃が付着していないことを確認してからコンセントに差し込んでください。半年から 1 年に 1 回は、電源プラグや電源アダプタをコンセントから抜いて点検・清掃してください。埃により火災・感電の恐れがあります。

稲妻危険

稲妻が発生しているとき、本製品やケーブルの設置などの作業を行わないでください。落雷により、感電する恐れがあります。

濡れ手禁止

本製品を扱うときは、濡れた手で行わないでください。感電の恐れがあります。

水濡れ禁止

水などで濡れないようにしてください。漏電及び感電の恐れがあります。

※本製品は日本国内でのみ使用可能であり、それ以外の国または地域で使用することはできません。

目次

第 1 章　装置概要 7

1. 付属品の確認 7
2. 各部名称 8
3. 設置 10
4. 前提条件 11

第 2 章　利用者機能 12

1. インターネット接続認証 12
認証方式「ベーシック認証」の場合 12
認証方式「フリー認証」、あるいは自動認証設定を利用した場合 12
認証方式「アクセス ID 認証」の場合 13
認証方式「Radius 認証」の場合 14
2. 指定 URL 表示 15

第 3 章　管理機能 16

1. TOP 17
1－1. ステータス表示 17
1－2. 接続テスト 18
1－3. システムログ 19
1－4. バックアップ/リストア 20
1－5. 停止/再起動 21
2. 基本設定 22
2－1. ネットワーク設定 22
2－2. DHCP 設定 24
2－3. オプション設定 26
2－4. セキュリティ設定 34
2－5. 時刻設定 35
2－6. 認証画面 36
認証画面テンプレートのカスタマイズ手順 38
2－7. ローカル DNS 40
2－8. ローミング （オプション） 41
3 接続管理 43
3－1. 接続状況 43
3－2. 基本接続設定 44
3－3. 接続ポート設定 49

3－4. アクセス ID 設定 61
3－5. 接続履歴 65
3－6. 自動認証設定 66
3－7. @Cloud サービス 67
3－8. Radius 連携 （オプション） 69
4 ポート転送/制限 70
4－1. ポート転送 70
4－2. フィルタリング 71
4－3. MAC フィルタリング 72
5 ネットワーク監視 73
5－1. 監視状況 73
5－2. 監視設定 75
6 メールアドレス認証 （オプション） 76
6－1. 接続申請状況 76
6－2. オプション設定 78
6－3. 自動発行設定 79
6－4. 申請画面 81
申請画面テンプレートのカスタマイズ手順 82
申請画面テンプレートのカスタマイズの具体例 85
第 4 章 コンソール機能 86
第 5 章 システムログ 88
1. 状態監視ログ 88
2. DHCP ログ 91
3. メールログ 91
4. 認証ログ 91
5. アクティブログ 92
6. トラフィックログ 93
7. セッションログ 93
8. アクティブユーザ 93
9. パケット転送ログ （オプション） 94
第 6 章 トラブルシューティング 95
1. 起動しない 95
2. 管理 PC にログイン画面が表示されない 95
3. 管理画面でログインできない 95
4. インターネットに接続できない 95

5. 利用者端末に認証画面が表示されない 96
6. 利用者端末で認証は出来るがインターネットアクセスができない。 96
7. メールの送受信ができない..... 96

第 7 章　仕様..... 98

MicroPOPCHATⅢ 98
SecurePOPCHATⅢ 99
HyperPOPCHATⅢ 100

■付録）認証画面：エラーメッセージについて..... 101

1）認証画面表示の際のメッセージ 101
・「お使いの端末からの通信が上限セッション数を超えたため、一時的に接続を制限させていただいております。」..... 101
・「認証可能な端末の上限（XXXX）を超えています」..... 101
2）認証処理の際のメッセージ..... 101
・「処理が集中しています。しばらくしてから実行ください。」..... 101
・「ERROR: (AUTH_NOROOM)」..... 101
・「アクセス ID が正しくありません。」..... 101
・「有効な接続期間ではありません。」..... 101
・「お使いの端末の IP アドレスはすでに使用されています。IP アドレスを再設定（DHCP リースを更新）してください。」 101
・「ID/パスワードが正しくありません。」..... 101
・「認証処理エラー（NETWORK）」..... 102
・「只今、インターネットに接続できません。」..... 102

第１章　装置概要

1. 付属品の確認

本製品には以下の付属品が同梱されています。万が一、不足している場合は、お買い上げ頂いた販売店までお問い合わせください。

・MicroPOPCHATⅢ／ SecurePOPCHATⅢ／ HyperPOPCHATⅢ　本体

・SecurePOPCHATⅢ／ HyperPOPCHATⅢのみ、ラックマウント金具およびネジ

・電源ケーブル・電源アダプタ
コンセントに接続する為のケーブルです。本製品に同梱されているもの以外は絶対に使用しないでください。製品の故障や、火災の原因となる恐れがあります。

・POPCHAT 納品情報／POPCHAT＠Cloud アカウント登録票
POPCHAT 機器にユニークに付与された「User-ID」と「パスワード」、および、POPCHAT 標準機能に対して追加インストールされたオプション機能や、POPCHAT 機器に付随する POPCHAT＠Cloud アカウント（ライセンスに伴う提供機能概要）の通知書です。

・ユーザー登録のお願い
サポートサービスをご提供するのに必要となる各種情報を、オンラインからご登録いただく必要がございます。

※製品保証書

出荷時に保証書は添付されておりません。下記の要領で保証書を発行いたします。

1. ユーザ登録を行って下さい。
2. 弊社でユーザ登録の内容を確認後、販売店担当者様またはサポート担当者様へ保証書の送付先を確認させていただきます。
3. 後日、ご指定の場所に保証書を発送いたします。

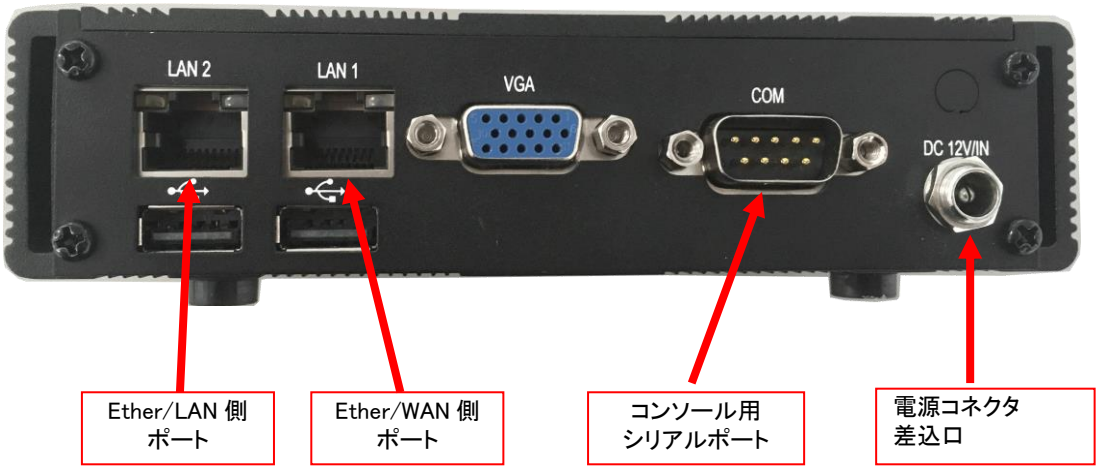
（注）保証書を紛失した場合は、製品保証期間内であっても保証を受けることができませんので、保証書が届きましたら保証書を大切に保管してください。

2. 各部名称

本製品の接続口の写真及び説明を以下に示します。

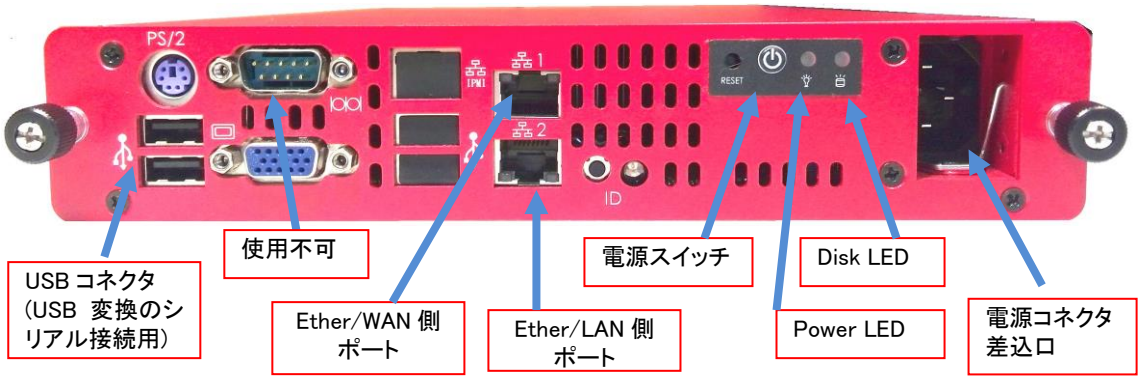
＜背面＞

MicroPOPCHAT



※電源スイッチは機器前面の左側にあります

SecurePOPCHAT / HyperPOPCHAT



・電源スイッチ　:本製品の起動／終了
終了は電源ボタンを押してすぐに放してください。通常は 30 秒程度で Power LED が消灯しますが、稼働後は状態により多少長くなります。
注）数秒間押し続けると強制終了します。強制終了した場合、ログや稼働情報は保持されません。内部ファイルが破損し、正常に起動しなくなる場合もあります。

・Ether/WAN 側ポート(LAN1)　:上位の機器とイーサネットケーブルで接続します。
（例:ルータ、ONU 等）

・Ether/LAN 側ポート(LAN2)　:下位の機器とイーサネットケーブルで接続します。
（例:スイッチングハブ、VDSL 装置）

・USB コネクタ　:　シリアル変換コネクタを利用することで本装置へのシリアル接続が可能になり、初期化等のコンソールメニューが操作できます。

注）ここで説明していないコネクタは、使用しませんので何も接続しないでください。

3. 設置

- 平置きあるいはラックに格納して下さい。
- 上部に物を乗せないで下さい。
- 機器を接続する前に、全ての配線が上位下位とも完了し且つ導通の確認も済ませる事をお勧めします。特に下位の機器に対して SNMP 等による Port 検出を行う場合は、それらの機器の設定が完了している必要があります。
- 配線時はもちろんの事、配線の組み換え等を行った場合は、本製品を再起動させてください。
- 使用する電源コンセントは、たこ足接続は避け、特にコピー機やプリンタとは別の系統の電源コンセントに接続する事をお勧めします。
- 一時的であっても大きな電圧降下は瞬断の原因になり、本機の故障を招きますので十分にご注意ください。

＜配線手順＞

1. 本製品 の WAN 側コネクタに上位回線（ルータ、ONU 等）からの Ethernet ケーブルを接続します。次に LAN 側コネクタに下位（スイッチングハブ等）からの Ethernet ケーブルを接続します。本製品のネットワークインターフェースは、WAN/LAN 共に MDI、MDI-X を自動判別しますが、念のためリンクアップすることをご確認ください。また LAN ケーブルは CAT5 規格以上のケーブルをご使用ください。

2. 設置先の電源設備又は UPS に機器の電源ケーブルを接続して下さい。

3. 電源ボタンを押し、本製品を起動させます。起動には約 3 分程度時間がかかります。

4. 前提条件

1.ルータの設定に関して

本製品は、インターネットを介してサポートセンターの専用サーバへ自動的に VPN 接続します。ネットワーク監視、バックアップ、アップグレード等の保守サービスは、専用サーバとの接続が必須です。そのため、POPCHAT 機の上位に置かれるルータは、TCP/IP の 80 番及び 443 番、Syslog 転送のため 514 番(UDP) Port を WAN 側に通すように設定されなければなりません。

2. サポートセンターVPN 接続用 IP アドレスの使用制限

①上記 1 で記載しましたように VPN 接続用のプライベートアドレスとして 10.0.0.0/24 を使用するため 10.0.0.X のアドレスは本装置に設定しないでください。また、ブロードキャストやローカルホスト等のアドレスも使用できません。

②POPCHAT 導入の対象拠点ネットワーク構成において、上記 1 の POPCHAT からサポートセンター専用サーバへの VPN 接続先アドレスとなる 10.255.255.254 と重複する IP アドレスを使用できません。

3.LAN 側に設置する機器に関して

LAN 側に接続する機器は、L2 で構成する必要があります。ルータ、L3 スイッチ、ルータモードでの無線アクセスポイント等、NAT 機能を持つ機器の動作保証はできませんので予めご了承ください。

SNMP でポート検出する場合は、接続する DSLAM/HUB にて、標準 MIB-Ⅱ及び Bridge-MIB(qBridge-MIB も可)の対応が必要です。

※本装置では、SNMP でポート検出する際、以下の OID を使用します。

＞"標準 MIB" 方式を使用する場合

1.3.6.1.2.1.2.2.1.1（IF-MIB）・・・・・・ポート検出に使用
1.3.6.1.2.1.17.4.3.1.2（Bridge-MIB）・・端末の接続ポート判定に使用
1.3.6.1.2.1.17.1.4.1.2（Bridge-MIB）・・端末の接続ポート判定に使用

＞"qBridgMIB" 方式を使用する場合

1.3.6.1.2.1.2.2.1.1（IF-MIB）・・・・・・ポート検出に使用
1.3.6.1.2.1.17.7.1.2.2.1.2（qBridge）・・端末の接続ポート判定に使用
1.3.6.1.2.1.17.1.4.1.2（Bridge-MIB）・・・端末の接続ポート判定に使用

4.POPCHAT のインタフェースは、オートネゴシエーション

POPCHAT のインターフェースは「オートネゴシエーション」のみの動作となっています。
このため、対向機器のインターフェースが、例えば「100BASE-T(full)で固定」で設定された場合、POPCHAT 側は「半二重」となり通信が不安定になります。
POPCHAT の対向機器のインターフェースを「オートネゴシエーション」でそろえていただきますようお願いします。

第 2 章　利用者機能

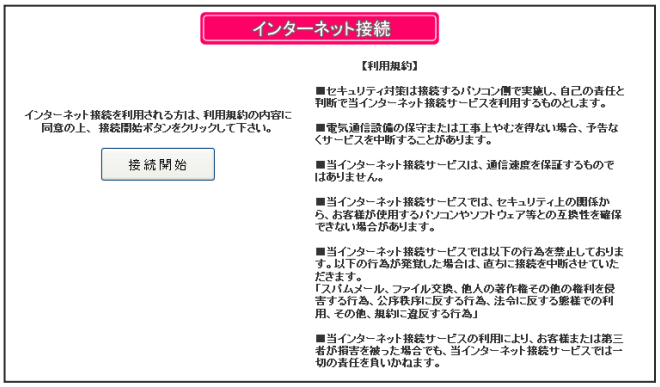
1. インターネット接続認証

本装置の LAN 側（下位）に接続されたパソコンがインターネット接続する際の認証処理をおこないます。

認証方式「ベーシック認証」の場合

①パソコンを本装置の配下のネットワークに接続
②ブラウザを起動
③ブラウザに表示された認証画面（以下）にて「接続開始」をクリック

パソコンの認証画面



スマートフォンの認証画面

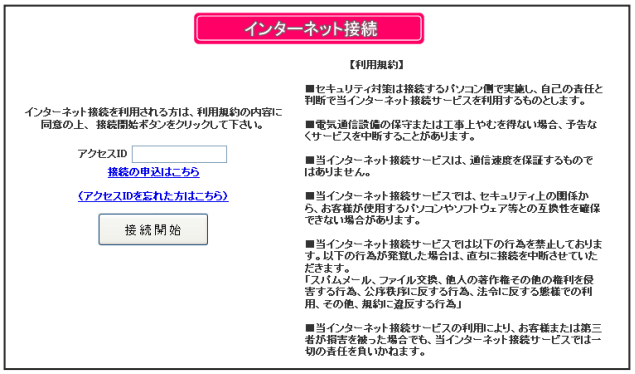
認証方式「フリー認証」、あるいは自動認証設定を利用した場合

①パソコンを本装置の配下のネットワークに接続
②認証画面の表示なしで、自動で認証されます。

認証方式「アクセス ID 認証」の場合

①パソコンを本装置の配下のネットワークに接続
②ブラウザを起動
③ブラウザに表示された認証画面（以下）にて発行されたアクセス ID を入力、「接続開始」をクリックします。

パソコンの認証画面

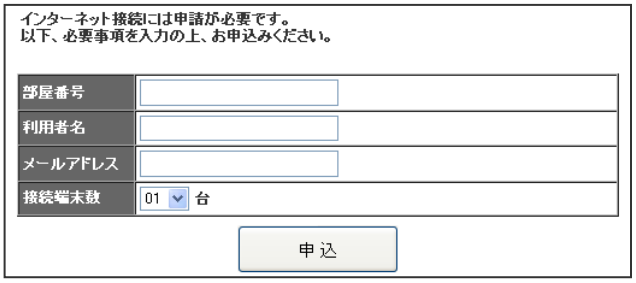


スマートフォンの認証画面

接続の申込はこちら　：　アクセス ID 申請画面が表示されます。
アクセス ID を忘れた方はこちら　：　アクセス ID リマインダ画面が表示されます。

※上記2つのリンクは「メールアドレス認証-オプション設定」にて、”利用者による申請”が「あり」の場合のみ、表示されます。

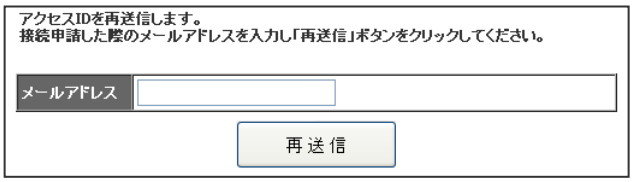
（アクセス ID 申請画面）



アクセス ID の発行を申請するための画面です。

部屋番号　：　申請情報として、部屋情報を入力します。
※基本設定-オプション設定の”接続ポート設定を使用する”が有効、かつ、自動発行設定の”接続ポート制限”がありの場合、接続ポートのリストからの選択となります。
利用者名　：　申請情報として、利用者情報を入力します。
メールアドレス　：　アクセス ID の通知先として、メールアドレスを入力します。
接続端末数　：　利用者が接続する端末数を入力します。
※発行されたアクセス ID は、この接続端末数の台数分、使用可能です。

（アクセス ID リマインダ画面）



アクセス ID を再通知させるための画面です。

メールアドレス ： アクセス ID の通知先として、メールアドレスを入力します。

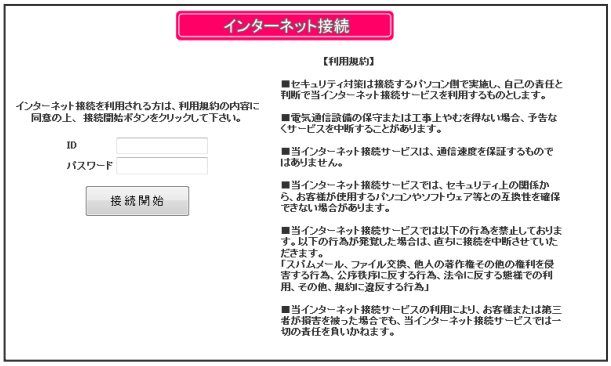
認証方式「Radius 認証」の場合

①パソコンを本装置の配下のネットワークに接続

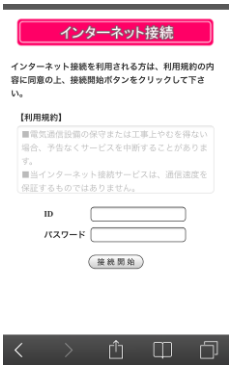
②ブラウザを起動

③ブラウザに表示された認証画面（以下）にて、Radius サーバ上のアカウントおよびパスワードを入力、「接続開始」をクリックし、認証処理します。

パソコンの認証画面



スマートフォンの認証画面



※セキュリティ上の注意勧告について

認証画面が表示される設定において、HTTPS からの SSL 接続に対して、認証画面が表示される前にセキュリティ上の注意勧告が表示されます。

これは、閲覧先のサイトの変わりに、認証画面を表示するため、ブラウザが閲覧先のサイトから変更されていることを通知するために起こります。（そのため、セキュリティに問題がでているわけではございません。）

なお、認証画面の表示の前にこのような画面が表示された場合は、そのまま続行をしてサイトを表示させるか、「http://www.yahoo.co.jp/」などの HTTP サイトをアドレスバーに打ち込んで、サイトを表示しますと認証画面が表示されます。

2. 指定 URL 表示

本装置の「指定 URL 表示」機能が有効な場合、指定された URL が、指定された間隔で、ブラウザに表示されます。

第 3 章　管理機能

本装置の設定は、LAN 側ポート（LAN2）に接続された管理用パソコンより行います。
設定操作は、Web ブラウザから行います。

接続手順）
①管理用パソコンの IP を本装置の LAN 側ポート（LAN2）の IP アドレス（出荷時設定：192.168.1.254）と同じセグメントの IP アドレスに設定
例　IP アドレス　：　192.168.1.2
　サブネット：　255.255.255.0
　ゲートウェイ：　192.168.1.254
　DNS　：　192.168.1.254

②管理用パソコンを本装置の LAN 側ポート（LAN2）に接続
③ブラウザの URL に「http://192.168.1.254:888」を指定して、下記の画面よりログインする。
　　管理者 ID　：admin
　　パスワード：xdmZph58

(ID を「staff」(staff の出荷時パスワード: hkmfdu12)でログインした場合、ステータス表示と接続確認が可能です。)

1. TOP

1－1. ステータス表示

本装置の状態を確認するための機能です。以下、ステータス情報が確認できます。

－ユーザIDセット状況

－ネットワーク設定

■ステータス表示

＊ユーザIDセット済み

ユーザID	U00[redacted]
パスワード	**********

（ネットワーク設定）

ホスト名	localhost.localdomain
WANインターフェース	< DHCP > IPアドレス 192.168.10.14 サブネット 255.255.248.0 ゲートウェイ 192.168.10.254
LANインターフェース	IPアドレス 192.168.1.254 サブネット 255.255.255.0
DNSサーバ	192.168.10.254

ユーザ ID	本装置のユーザ ID が表示されます。
パスワード	ユーザ登録のパスワードが伏せ字で表示されます。
ホスト名	ホスト名が表示されます。
WAN インターフェース	WAN 側のネットワーク情報が表示されます。
LAN インターフェース	LAN 側のネットワーク情報が表示されます。
DNS サーバ	DNS サーバの IP アドレスが表示されます。 （未表示の場合はローカルの DNS サーバを利用しています）

1－2. 接続テスト

指定IPアドレスとの接続状態（Ping 応答）の確認をするための機能です。

■接続テスト

指定IPアドレスとの接続状態(ping応答)を確認します。

IPアドレス	. . .

接続テスト

IP アドレス	PING 応答の確認をする IP アドレスを設定します。
接続テスト	設定された IP アドレスに対して PING の接続テストを実行します。

1－3. システムログ

システムログを表示するための機能です。

■システムログ　状態監視ログ

ログ内容

状態監視ログ	本装置の状態およびネットワーク監視に関するログ （保持日数：4 日）
DHCP ログ	DHCP 処理に関するログ （保持日数:28 日）
メールログ	メール送信に関するログ （保持日数：28 日）
認証ログ	接続開始（認証）、接続終了（認証切断）に関するログ （保持日数:90 日）
アクティブログ	接続開始（認証）から接続終了（認証切断）の間の端末の 接続状態を示すログ （保持日数：3 日）
トラフィックログ	POPCHAT を通過する、帯域使用量のログ （保持日数:4 日）
セッションログ	POPCHAT を通過する、セッション数のログ （保持日数：4 日）
アクティブユーザログ	接続中の利用者数のログ （保持日数:4 日）

※メモリの書き込み可能残容量が少ない場合、各ログの保持日数は保証されません。

※ログは 1 日 1 回自動でセンターサーバにバックアップされます。

※シスログ転送が有効な場合、指定されたシスログサーバに対して、ログが転送（EUC-JP）されます。

※シスログ@クラウドサービスが有効な場合、シスログ＠クラウドサーバに対してログが転送されます。

1－4. バックアップ/リストア

本装置の設定およびログをバックアップ/リストアするための機能です。
※リストア処理の際、機器の再起動を伴います。

■バックアップ/リストア

バックアップ	バックアップ	※設定およびログデータをバックアップします。
リストア	参照... ファイルが選択されていません。 リストア	※バックアップデータをリストアします。

バックアップ	ローカル上に設定及びログデータをバックアップします。 ※認証画面のテンプレートのデータはバックアップ対象には含まれません。 必要な場合、「基本管理-認証画面」のダウンロードにて、バックアップしてください。
リストア	ローカル上のバックアップファイルを参照ボタンより選択し、リストアをします。

1－5. 停止/再起動

本装置のシステムの停止/再起動をするための機能です。

■停止/再起動

システムを停止/再起動します。

システム停止

システム再起動

システム停止	終了処理を行い、電源も切ります。 ※電源ケーブル等を抜くときは、必ず本製品の電源が切れている事（正面にある LED（青）が消灯していること）を確認してください。故障の原因になります。
システム再起動	終了処理を行い、再起動します。

2. 基本設定

2－1. ネットワーク設定

本装置のネットワークインターフェースの設定をするための機能です。

※設定更新の際、機器の再起動を伴います。

■ネットワーク設定

※は必須項目ですので必ず入力して下さい

ホスト名※	localhost.localdomain
FQDN	
WANインターフェース※	◉DHCP ○固定IP IPアドレス . . . サブネット . . . ゲートウェイ . . .
LANインターフェース※	IPアドレス 192 . 168 . 1 . 254 サブネット 255 . 255 . 255 . 0
DNSサーバ	. . .

更 新

ホスト名	本装置自身のホスト名を指定する場合に設定します。 ※ メール代理送信機能を使用する場合、ホスト名は、インターネット上で有効な（名前解決可能な）FQDN をホスト名として設定するようにしてください。 （特に決まったものがなければ初期設定のままで問題ありません）
FQDN	認証画面表示の際のホスト名（FQDN）を指定します。 設定されている場合、認証画面の URL が FQDN で表示されます。 （設定されていない場合は、POPCHAT の LAN 側アドレスで表示） ※既存の FQDN 名（インターネット上で名前解決可能な FQDN）は使用しないでください。 ※FQDN は、第2レベルドメイン以上で指定してください。 （利用者端末の仕様によって、DNS による名前解決がされないことがあるため）

<table>
<tr><td rowspan="3">WAN インターフェース</td><td colspan="2">本装置の WAN 側ネットワークを設定します。</td></tr>
<tr><td>DHCP</td><td>上位ネットワーク（WAN インターフェース側）上の DHCP サーバから、
IPアドレスを自動取得する場合、こちらを選択します。</td></tr>
<tr><td>固定 IP</td><td>固定 IP アドレスを付与する場合、こちらを選択します。
以下、項目の設定が必要です。
ーIPアドレス
ーサブネット
ーゲートウェイ</td></tr>
<tr><td>LAN インターフェース</td><td colspan="2">本装置の LAN 側インターフェースを設定します。
以下、項目を設定します。
ーIPアドレス
ーサブネット
※WAN ネットワークと LAN ネットワークは異なるセグメントで設定してください。</td></tr>
<tr><td>DNS サーバ</td><td colspan="2">本装置が参照する DNS サーバを指定します。
※DNS サーバの指定がない(空白の)場合、DHCP サーバから付与された DNS サーバを使用します。また、固定 IP 設定でサーバから付与されない場合は、本装置内のローカル DNS が使用されます。</td></tr>
</table>

2－2. DHCP 設定

本装置配下の端末に対してのIP割当の設定をするための機能です。

※設定更新の際、機器の再起動を伴います。

■DHCP設定

※は必須項目ですので必ず入力して下さい

割当アドレス※	Private接続アドレス使用
アドレス設定※	◆Private接続アドレス (IPアドレス範囲) 192 . 168 . 1 . 1 ～ 192 . 168 . 1 . 253 DHCP ～ -- ～ -- ◆Global接続アドレス (IPアドレス範囲) ～ -- ～ -- ～ --

更 新

割当アドレス	端末に対して、優先して割り当てるアドレスタイプを選択します。		
	Private 接続アドレス ・端末に、Private 接続アドレス(プライベートIPアドレス)を割り当てます。 ・端末が本装置を介して、インターネット接続する際は、本装置の WAN インターフェースのIPアドレスで通信します(NAPT接続仕様)。		
	Global 接続アドレス ・端末に、Global 接続アドレス(グローバルIPアドレス)を割り当てます。 ・端末が本装置を介して、インターネット接続する際は、端末自身に割当てられたIPアドレスで通信します(ダイレクト接続仕様)。		
Private 接続アドレス	IP アドレス範囲	端末に割り当てるIPアドレスをプライベートIPアドレスで範囲指定します。 ※LAN インターフェースと同じネットワークのアドレスのみ指定可 ※本装置の IP アドレスの値を含まないようにしてください。	
	種別	DHCP	本装置の DHCP により、端末にIPを付与するアドレス範囲の場合、こちらを選択します。
		固定付与	端末に固定付与するIPアドレス範囲の場合、こちらを選択します。(本装置の DHCP サービスのアドレス範囲から除外されます)
Global 接続アドレス	IP アドレス範囲	端末に割り当てるIPアドレスを グローバルIPアドレスで範囲指定します。 ※割当アドレス「Private 接続アドレス」の場合、LAN インターフェースのネットワークのアドレス以外の任意のアドレスの指定可 ※割当アドレス「Global 接続アドレス」の場合、WAN インターフェースと同じ	

		ネットワークのアドレスのみ指定可 ※本装置の IP アドレスの値を含まないようにしてください。	
	種別	DHCP	本装置の DHCP により、端末にIPを付与するアドレス範囲の場合、こちらを選択します。
		固定付与	端末に固定付与するIPアドレス範囲の場合、こちらを選択します。（本装置の DHCP サービスのアドレス範囲から除外されます）

※DHCP 設定を変更した場合、既存の認証はクリア（初期化）されます。

※Private 接続アドレス、Global 接続アドレスともに、認証の際に、本装置配下のパソコンに、 アドレスを割り当て、認証解除されるまで、そのアドレスを保持します。

※本装置の配下の機器（SW-HUB など）に、グローバルIPを割り当て、外部（インターネット側）から接続を可能にしたい場合、「固定付与」指定した範囲のアドレスを指定してください。
（Global の IP アドレスを割り振るときのデフォルトゲートウェイは本装置の WAN 側の IP アドレスに設定をします）

※WAN 側と LAN 側はブリッジ接続にすることはできません(NAT 接続により、LAN 側の通信は POPCHAT の WAN 側インターフェースの MAC アドレスに集約して通信がされます）

2－3. オプション設定

以下、オプション設定をするための機能です。
※設定更新の際、機器の再起動を伴います。

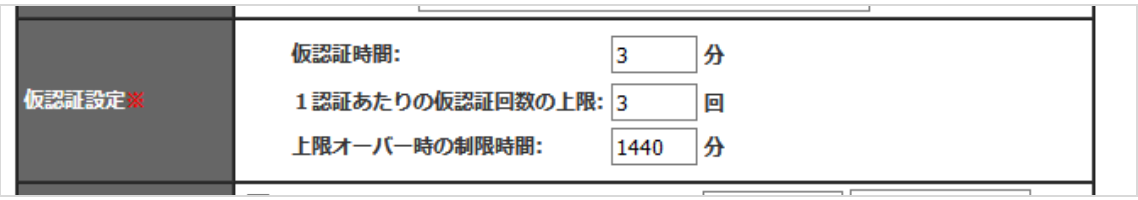
■オプション設定

※は必須項目ですので必ず入力して下さい

代理Proxy設定※	○使用しない ◉使用する ☐ 認証時のみ使用 対象プロクシポート(カンマで区切って複数指定可能): 81,8080,8888,3128
代理SMTP設定※	◉使用しない ○使用する ☐リレーサーバを使用する リレーサーバ:

代理 Proxy 設定	代理 Proxy を使用すると、端末ブラウザにて、イントラネット環境上のプロキシ(http/https)が設定されている場合でも、通信させることが可能です。 (ただし、端末ブラウザに指定されたプロキシポートは、対象プロキシポートの指定の範囲である必要があります) ※登録可能な対象プロキシポート数は、15 個までです。 ※SSL プロキシの仕様上、https 通信に対しての認証画面の表示はできません。	
	認証時のみ使用	認証処理後、本装置での代理プロキシは行いません。 (イントラネット環境での利用の場合など、認証処理後、既存のプロキシサーバ経由で、インターネット接続させたいケースでの設定)
代理 SMTP 設定	代理 SMTP を使用すると、端末に設定された SMTP サーバに接続できない場合でも、本装置が代理で処理することで、メール送信が可能になります。 ※ メール送信データのサイズは 1 送信に付き 10MB までとなります。 ※ 「基本設定-ネットワーク設定」のホスト名は、本機能によるメール送信にて、SMTP サーバ名として使用され、メール送信時に宛先メールサーバへ通知されます。不適切な名前の場合、受信拒否される場合がありますので、インターネット上で有効な(名前解決可能な)FQDN をホスト名として設定するようにしてください。	
	リレーサーバを使用する	25 番ポートへの送信を指定されたアドレスに転送します。 ※ プロバイダが提供するリレーサーバを経由して、メール送信する場合に設定します

（前の画面の続き）



仮認証設定	仮認証時間	仮認証の有効期間を指定します。（デフォルト： 3 分）
	1認証あたりの仮認証回数の上限	仮認証の上限回数を指定します。（デフォルト： 3 回）
	上限オーバー時の通信制限時間	仮認証の上限回数を超えた場合の制限時間を指定します。（デフォルト： 1440 分＜1日＞）

※2021 年 1 月リリース版の「@クラウド連携個別パッチ」を適用した POPCHAT 又は 2021 年 2 月以降に出荷された POPCHAT のみ対応可能な項目です。

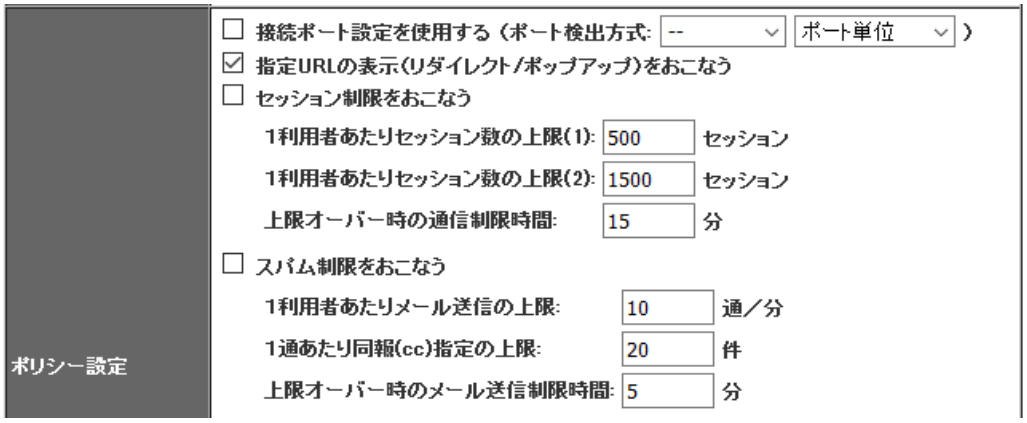
■補足１≪POPCHAT の仮認証とは≫
OPEN-ID 認証やメールアドレス認証など外部サーバへアクセスする必要がある認証手続きを行う際、POPCHAT では一時的に開放(仮認証)を行っています。
それに伴い、公衆 Wi-Fi 環境においてきちんと認証せずに不正に使用／悪用されてしまう事を防ぐため、POPCHAT の最新版ファームウェアでは以下の制限を設けております。

⇒1回あたりの仮認証時間は『**3 分間**』。
⇒同じ端末で『**3 回**』仮認証を行いながら一度も認証を完了していない場合は、本認証の意志なし（＝不正利用）の可能性を想定し、当該ユーザーの通信を『**当日 24:00**』までブロック。
⇒認証を完了せずに仮認証の状態を繰り返し上限回数を超えると
「仮認証の上限回数を超えています」
というエラーが表示され、対象端末のみ制限がかかり認証が行えなくなります。

■補足２≪2021 年 1 月リリース版の「@クラウド連携個別パッチ」≫
該当個別パッチを適用する事により、上述の「3 分間」「3 回」「当日 24:00 まで」という設定値が、可変となります。
加えて、仮認証カウント数をリセットする操作が、次に述べる方法により可能となります。

■補足３≪仮認証の制限を解除する場合≫
上記の仮認証設定が行える POPCHAT は、仮認証カウントをリセットして「0」に戻すことが可能になります。
接続管理タブの@Cloud サービスの設定ページにて「更新」ボタンを実行すると、POPCHAT⇔POPCHAT@Cloud 間の接続が確立し直されて、仮認証の累積カウントがリセットされます。
詳しくは**「3－7. @Cloud サービス」**をご覧ください。

（前の画面の続き）



ポリシー設定	接続ポート設定を使用する	部屋管理（端末の接続されているポートで管理）したい場合、チェックします。 あわせて、ポート検出方式を選択します。 ※使用した場合、登録ポートからの認証のみ受付けるようになります。	
		SNMP	SNMP（Bridge-MIB、あるいは qBridge-MIB）対応のスイッチングハブの場合、この機能を使用できます。
		タグ VLAN	タグ VLAN 対応のスイッチングハブや AP の場合、この機能を使用できます。

※ポート検出方式の設定を変更した場合、既存の認証およびアクセス ID はクリア（初期化）されます。

※ SNMP によるポート検出について

標準 MIB-Ⅱ及び Bridge-MIB(qBridge-MIB も可)に対応。但し、対応機器でも SNMP の問い合わせに対する応答の値は、それぞれの機器に依存しますので、詳細はそれぞれの機器メーカー又は販売店に、ご確認ください。

なお、本装置では、SNMP でポート検出する際、以下の OID を使用します。

＞"標準 MIB" 方式を使用する場合

1.3.6.1.2.1.2.2.1.1（IF-MIB）・・・・・・ポート検出に使用

1.3.6.1.2.1.17.4.3.1.2（Bridge-MIB）・・端末の接続ポート判定に使用

1.3.6.1.2.1.17.1.4.1.2（Bridge-MIB）・・端末の接続ポート判定に使用

＞"qBridgMIB" 方式を使用する場合

1.3.6.1.2.1.2.2.1.1（IF-MIB）・・・・・・ポート検出に使用

1.3.6.1.2.1.17.7.1.2.2.1.2（qBridge-MIB）・・端末の接続ポート判定に使用

1.3.6.1.2.1.17.1.4.1.2（Bridge-MIB）・・・端末の接続ポート判定に使用

ポリシー設定	指定 URL の表示	所定のタイミングで、自動的に、指定URLを、本装置配下の端末に表示させたい場合、チェックします。 指定URL表示は、ブラウザ上での表示となります。

ポリシー設定	セッション制限をおこなう 上限値と下限値 上限(1)1～9999 上限(2)1～9999 ※(2)＞(1) であること 通信制限時間 1～999	以下、しきい値を超えた場合、通信を制限します。	
		1 利用者あたりセッション数の上限(1)	閾値を超えた端末の新規パケットの通信数を、上限(1)の閾値の 5 分の 1 に絞りこみます。 ※上限(1)の閾値に「500」が設定した場合、500×1/5=100 パケットまでに絞り込みます。
		1 利用者あたりセッション数の上限(2)	閾値を超えた端末は通信ができなくなります。 この間、ブラウザにはセッション制限のエラー画面が表示されます。
		上限オーバー時の通信制限時間	通信制限の時間を設定します。

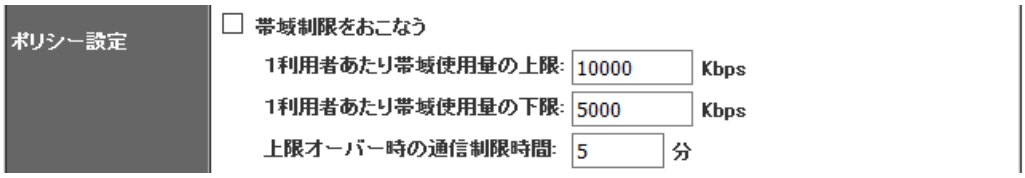
※制限のチェックは 1 分おきに行われます。
※対象端末の接続を終了(認証解除)すると、制限も解除されます。

ポリシー設定	スパム制限をおこなう 上限値と下限値 送信の上限 1～9999 同報の上限 1～9999 通信制限時間 1～999	以下、しきい値を超えた場合、スパム送信とみなし、メール送信を制限します。	
		1 利用者あたりメール送信の上限	閾値を超えた端末のメール送信が制限時間の間、エラーになります。 ※対象の端末にて「上限オーバー時のメール送信制限時間」の間、メール送信がエラーとなります。
		1 通あたり同報指定の上限	閾値を超えた端末のメール送信がエラーになります。 ※同報数が閾値を超える場合、送信されません。
		上限オーバー時のメール送信制限時間	通信制限の時間を設定します。

※制限のチェックは 1 分おきに行われます。
※対象端末の接続を終了(認証解除)すると、制限も解除されます。
※スパム制限は、代理 SMTP 設定を「使用する」場合のみ、利用可能です。

（前の画面の続き）

（MicroPOPCHAT/SecurePOPCHAT はオプション）



ポリシー設定	帯域制限をおこなう 上限値と下限値 上限　1～9999999 下限　1～9999999 上限＞下限　であること	以下、しきい値を超えた場合、通信を制限します。	
		1 利用者あたり帯域使用量の上限 1 利用者あたり帯域使用量の下限	帯域使用量の上限を超えると帯域使用量の下限の値に通信が絞り込まれます。
		上限オーバー時の通信制限時間	帯域制限の制限時間を設定します。

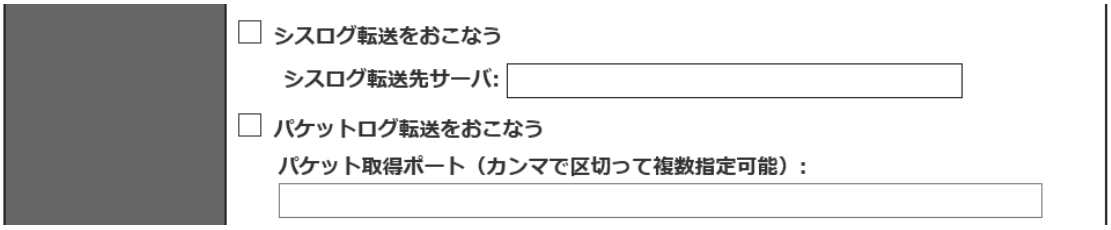
※制限のチェックは 1 分おきに行われます。
※対象端末の接続を終了（認証解除）すると、制限も解除されます。
※通信制限は、以下のように動作します。

〇送信トラフィック（TX）が「1 利用者あたり帯域使用量の上限」を超えた場合
⇒対象の端末にて「上限オーバー時の通信制限時間」の間、送信トラフィックの使用可能帯域が、「1 利用者あたり帯域使用量の下限」に絞り込まれます。

〇受信トラフィック（RX）が「1 利用者あたり帯域使用量の上限」を超えた場合
⇒対象の端末にて「上限オーバー時の通信制限時間」の間、その時点の受信トラフィックの使用帯域に対する「1 利用者あたり帯域使用量の下限」の割合に応じて、送信トラフィックの使用可能帯域が絞り込まれます。
（結果、受信トラフィックの使用帯域は、おおよそ「1 利用者あたり帯域使用量の下限」に近い値となります）

〇制御の仕様上、通信パケットの大きさにより、下限の値より数 100Kbps を超えて流れることがございます。

（前の画面の続き）

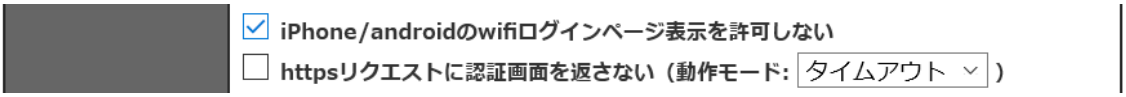


ポリシー設定	シスログ転送をおこなう	シスログサーバへログを転送するときにチェックを入れて、アドレスを入力します。
	パケットログ転送をおこなう （オプション）	シスログサーバへ通信ログを転送するときにチェックを入れ、転送対象のポート番号を記載します。

※シスログサーバに転送されるログ
※文字コード：EUC-JP

セルフテストログ　・・・　本装置の状態およびネットワーク監視に関するログ
DHCP ログ　・・・　DHCP 処理に関するログ
メールログ　・・・　メール送信に関するログ
認証ログ　・・・　接続開始（認証）、接続終了（認証切断）に関するログ
トラフィックログ　・・・　POPCHAT を通過する、帯域使用量のログ
アクティブログ　・・・　接続開始から接続終了の端末の接続状態を示すログ
セッションログ　・・・　POPCHAT を通過する、セッション数のログ
アクティブユーザログ　・・・　接続中の利用者数のログ

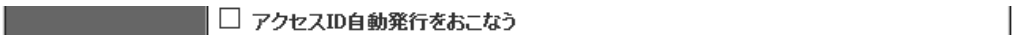
（前の画面の続き）



ポリシー設定	iPhone/android の wifi ログインページ表示を許可しない	iPhone/android の wifi 接続時に自動表示される wifi ログインページを表示させません。	
	https リクエストに認証画面を返さない	未認証の端末からの https アクセスに対しての動作モードを選択します。	
		タイムアウト	https リクエストを DROP し、応答を返しません。利用者端末からの https（ポート 443）での通信は、タイムアウトします。
		スルー	https リクエストを認証なしで、通過させます。利用者端末からの https（ポート 443）での通信は、認証なしで許可されます。

（前の画面の続き）

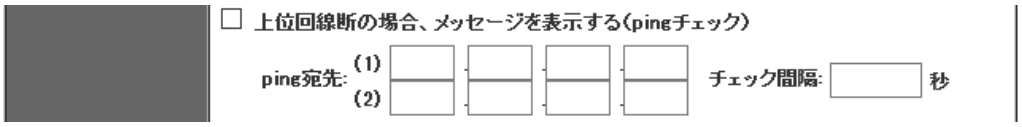
（MicroPOPCHAT/SecurePOPCHAT はオプション）



ポリシー設定	アクセス ID 自動発行をおこなう。	アクセス ID 自動発行を有効にする場合チェックします。

※この機能を使用するには「基本設定」→「オプション設定」の「iPhone/android の wifi ログインページ表示を許可しない」を有効にする必要があります。

（前の画面の続き）



ポリシー設定	上位回線断時断の場合、メッセージを表示する （ping チェック）	チェックされている場合、上位回線の通信断を検知した際、ブラウザにエラー画面を表示します。

※通信断の検知は、ping 宛先(1)、(2)に対して、指定のチェック間隔（0～9999 まで設定、0 秒にしたときは、「1 秒間隔で 3 回 ping 実行」の１セットが休みなく実行）で、ping を送信し、両者ともに、応答がない（あるいは遅延している）場合、通信断と判定します。

2－4. セキュリティ設定

セキュリティ設定をするための機能です。
－パスワード設定
－アクセス制限

■セキュリティ設定

※は必須項目ですので必ず入力して下さい

パスワード設定※	・管理WEB用ユーザ admin / ●●●●●●●●●●● ※管理者ユーザ staff / ●●●●●●●●●●● ※一般ユーザ ・コンソール用ユーザ cnsusr / ●●●●●●●●●●●
アクセス制限	◉使用しない ○使用する 許可IPリスト(改行で区切って複数指定可能) 入力例 192.168.1.1 192.168.1.1/255.255.255.0 192.168.1.1/24

更 新

パスワード設定	管理 WEB にログインする際のパスワードを設定します。	
	admin	管理権限のアカウント：すべての機能が使用可
	staff	一般権限のアカウント：以下の機能のみ使用可 TOP　（ステータス表示、接続テスト、システムログ） 接続管理　（接続状況、アクセス ID 設定、接続履歴） ネットワーク監視（監視状況） メールアドレス認証 （接続申請状況）
	コンソールにログインする際のパスワードを設定します。	
	cnsusr	コンソール用アカウント：ネットワーク設定、初期化が使用可能
アクセス制限	管理 WEB に対してのアクセス制限を選択します。 使用する場合は、許可IPリストに接続する端末のIPアドレスを指定します。	
	使用しない	すべての端末からアクセスを許可
	使用する	許可IPリストにIPアドレスを指定します ※ 設定可能な数は 100 までです

2－5. 時刻設定

時刻の表示・設定をするための機能です。

■時刻設定

2017 年 05 月 16 日 18 時 52 分 時刻設定

現在時刻	2017年05月16日 18時52分49秒

NTPサーバ	
時刻合せ間隔	分おき

更 新

時刻設定	年月日時分を指定し、時刻を設定します。 ※指定した時刻が有効な日時でない（例：2012/2/30 00:00:00 など）場合、時刻設定されません。
現在時刻	本装置のシステム時刻を表示します。
NTP サーバ	時刻合わせに使用する NTP サーバを設定します。
時刻合せ間隔	時刻合わせの間隔を設定します。（1～999 分）

2－6. 認証画面

お客様独自の認証画面にカスタマイズをおこなうための機能です。

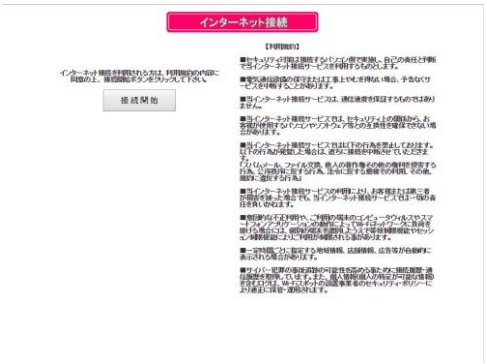
■認証画面

使用言語の選択	日本語　□中国語　□韓国語　□英語	
テンプレートの確認	日本語のテンプレートを確認 パソコン） 認証画面(index_auth)　エラー画面(index_err)　完了画面(index_global) 携帯・スマートフォン） 認証画面(index_auth)　エラー画面(index_err)　完了画面(index_global)	
テンプレートの取得	ダウンロード	※認証画面テンプレートをダウンロードします。 注意事項） ・テンプレートは、tar.gz形式で圧縮されています。 ・テンプレートのディレクトリ構成は変更しないでください。
テンプレートの更新	参照...　ファイルが選択されていません。 アップロード	※認証画面テンプレートを更新します。 注意事項） ・テンプレートのディレクトリ構成は変更しないでください。 ・登録の際、テンプレートは、tar.gz形式で圧縮してください。 ・圧縮後のテンプレートのファイルサイズが 1000KB以上のものは登録できません。
テンプレートの初期化	初期化	※認証画面テンプレートを初期状態に戻します。

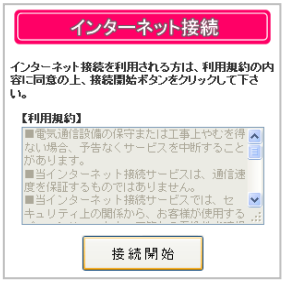
使用言語の選択	認証画面の言語を追加選択します。 ※ここで選択された言語の認証画面が、利用者ブラウザで表示切り替えの対象となります。また、選択された言語以外が利用者のブラウザで使用されたときは、選択言語に英語が含まれているときは英語のテンプレートが表示され、英語が含まれていない場合は日本語のテンプレートが表示されます。
テンプレートの確認	登録された認証画面テンプレートをプルダウンから選択し、プレビュー表示します。
テンプレートの取得	お客様独自のデザインに編集いただく際のベースとなる、認証画面テンプレートをダウンロードします。 ※テンプレートは、tar.gz 形式で圧縮されています。tar.gz が解凍可能なソフトを使い解凍した上で、編集してください。
テンプレートの更新	お客様独自デザインに編集した認証画面テンプレートを登録します。 ※テンプレートを編集する際は、既存ディレクトリ構成は変更しないでください。 （認証画面動作が正しく動作しなくなることがあります） ※テンプレートは、tar.gz 形式に圧縮してから登録してください。 ※登録可能なテンプレートサイズ（圧縮後）は、1000KB までとなります。
テンプレートの初期化	お客様の方で編集された認証画面が正しくないなど、認証画面が正しく動作しなくなるなどした場合、この機能を使い、元の状態に戻します。

※各言語のデフォルトでのテンプレートは、下記の内容で表示されます。

日本語（パソコン用）

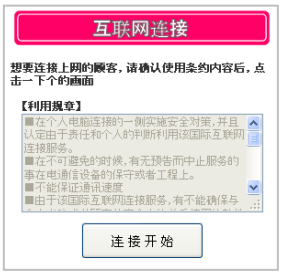


日本語（スマートフォン・携帯用）



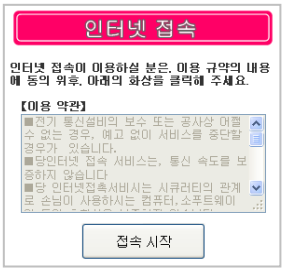
中国語（パソコン用）

中国語（スマートフォン・携帯用）

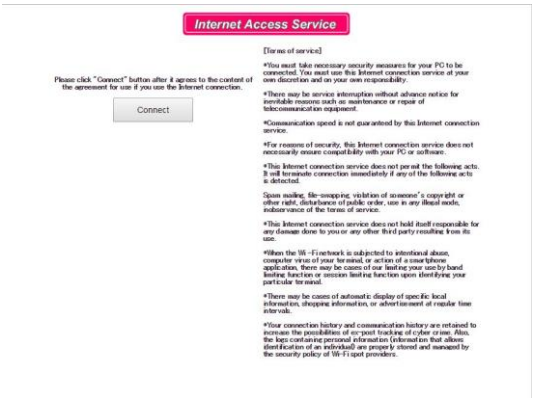


韓国語（パソコン用）

韓国語（スマートフォン・携帯用）



英語（パソコン用）



英語（スマートフォン・携帯用）

認証画面テンプレートのカスタマイズ手順

1. 認証画面テンプレートをダウンロードします
   ※"テンプレートの取得"をクリック
2. ダウンロードしたテンプレートを解凍します
3. テンプレートを編集します
   編集対象
   Custom/templates 配下の以下ファイル

パソコン用
認証画面(index_auth.tpl.html)
エラー画面(index_err.tpl.html)
完了画面(index_global.tpl.html)

携帯・スマートフォン用
認証画面(index_auth_s.tpl.html)
エラー画面(index_err_s.tpl.html)
完了画面(index_global_s.tpl.html)

※多言語対応する場合は、多言語用ファイルも編集します
（中国語：_china, 韓国語：_korea, 英語：_eng）

例）多言語用ファイル（中国語版）

パソコン用
認証画面(index_auth_china.tpl.html)
エラー画面(index_err_china.tpl.html)
完了画面(index_global_china.tpl.html)

携帯・スマートフォン用
認証画面(index_auth_china_s.tpl.html)
エラー画面(index_err_china_s.tpl.html)
完了画面(index_global_china_s.tpl.html)

編集の際の注意事項）
・テンプレートのディレクトリ構成を変更（追加含む）しないでください。
・テンプレートの文字コード（UTF-8）を変更しないでください。
・テンプレート内のシステムタグ（<!-- SYSTEM_BEGIN ・・-->、
<!-- SYSTEM_END ・・-->）で囲まれた部分に、認証画面動作に必要なロジックが埋め込みされるので、削除・編集しないでください。
・認証画面データには、以下の形式のデータのみ登録可能です
ーHTML ファイル （拡張子：html）
ースタイルシート（拡張子：css）
ー画像ファイル （拡張子：gif, jpg, jpeg, png）

※HTML ファイル、画像のリンクは、相対パスで指定してください。
－同じ階層にあるものは、「./ファイル名」
－下の階層にあるものは、「./フォルダ名/ファイル名」
－上の階層にあるものは、「../ファイル名」
※スタイル指定や JavaScript などを、HTML ファイルに直接記述する際は、記述箇所を、
{literal}{/literal}で囲んでください。

4. テンプレートを tar.gz 形式で圧縮します
5. 圧縮したテンプレートをアップロードします
※"テンプレートの更新"をクリック
6. 動作確認
以下、動作を確認します。

①認証処理されることを確認
②接続方式リストが表示されることを確認
③リダイレクト表示（あるいはポップアップ表示）されることを確認
④課金表示されることを確認
※②～④は、対象の POPCHAT の設定にあわせ、必要に応じて実施します

2－7. ローカル DNS

POPCHAT 配下の端末にて、独自に名前解決させたいドメイン／IP アドレスの組合せを登録するための機能です。

■ローカルDNS

※ドメイン、IPアドレスをローカルDNSに登録します

No	ドメイン	アドレス	
1			入力例 ドメイン：auth.popchat.jp アドレス：192.168.1.254
2			
3			
4			
5			
6			
7			
8			
9			
10			

更 新　　入力枠 追加

ドメイン	ドメインを指定します。
アドレス	ドメインに関連付ける IP アドレスを指定します。
入力枠 追加	入力枠を追加します （最大登録数は 15）

※本装置内のローカル DNS を機能させるには、ネットワーク設定の WAN インターフェースは、固定 IP で設定されている事と DNS サーバ欄は未設定である必要があります。

2－8. ローミング （オプション）

認証ローミングオプションの設定画面です。
※設定更新の際、機器の再起動を伴います。

■ローミング設定

※は必須項目ですので必ず入力して下さい

チャンネル選択	チャンネル1（38:60:77:3B:EF:71）
ローミング・グループ	※ローミングに参加させる POPCHATを登録します。（WANインターフェースの IPアドレスで指定） 入力例 192.168.1.1 改行で区切って複数指定可能

更 新

チャンネル選択	使用するチャンネル（MAC アドレス）を指定します。 ※選択されたチャンネルの MAC アドレスで、配下の端末と通信します。
ローミング・グループ	ローミングに参加させる POPCHAT を登録します。 （WAN インターフェースの IP アドレスで指定） （最大登録数は 5） ※登録された POPCHAT に対して、以下データを送信することで、ステータスおよび設定を同期します。 －認証ステータス（認証開始、認証解除） －DHCP 設定 －アクセス ID（登録、更新、削除）

○認証ローミングオプション

同一拠点の複数の POPCHAT 同士で、認証情報および、アクセス ID 情報を共有するためのオプションです。
本オプションにより、いずれかの POPCHAT で認証された端末は、別の POPCHAT 配下に移動した際、POPCHAT 内部で自動的に認証され、新たに認証画面を表示することなく、利用させることが可能です。
また、アクセス ID に関して、いずれかの POPCHAT にて作成されたアクセス ID を別の POPCHAT 配下の端末にて利用させることも可能になります。

1）認証情報のローミング

″ローミング元″： 最初に認証された POPCHAT
″ローミング先″： 端末が移動した先の POPCHAT

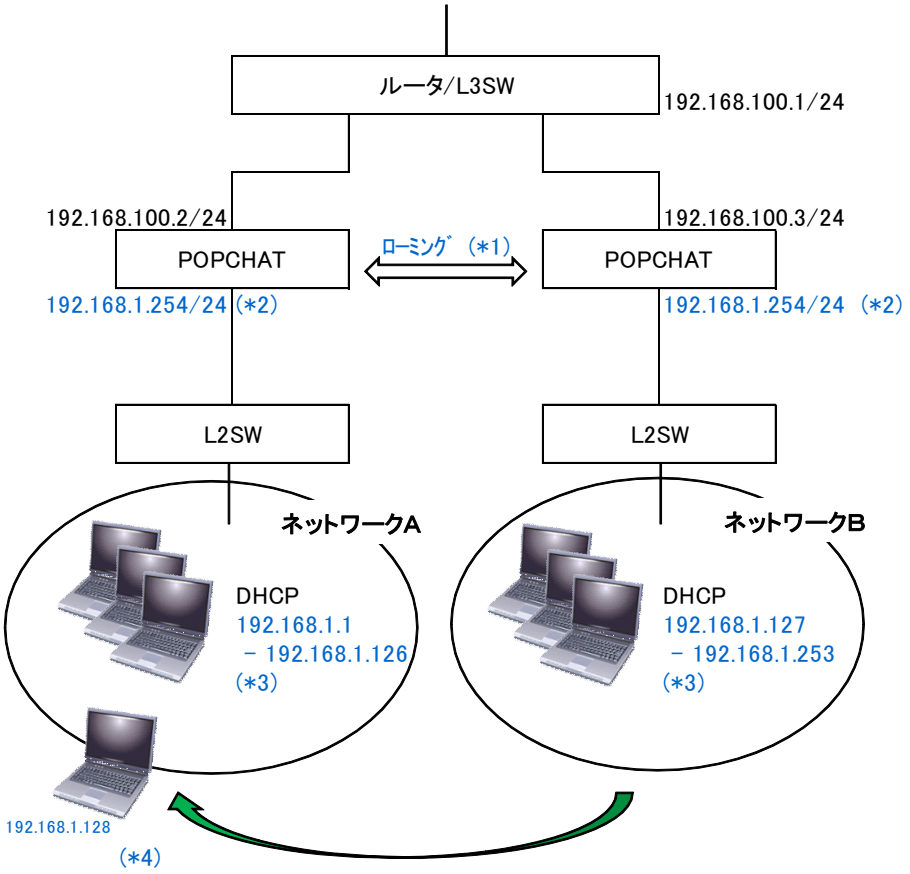
・ローミング先の認証は、端末がアクティブ状態のときのみ保持されます。
（一定時間（15 分）、通信がない場合、自動的に認証解除）
・ローミング先の認証は、ローミング元の有効期間を引き継ぎます。
・ローミング元が認証解除された場合、ローミング先の認証も解除されます。

2）アクセス ID のローミング

″ローミング元″： アクセス ID が作成された POPCHAT
″ローミング先″： 端末が移動した先の POPCHAT

・ローミング先で使用されたアクセス ID は、ローミング元のアクセス ID 設定（有効期間など）を引き継ぎます。
・ローミング元で作成されたアクセス ID は、ローミング先のアクセス ID 設定画面には表示されません。
・ローミングで使用するアクセス ID は、有効ポートの指定なしで作成する必要があります。（有効ポート指定があると、ローミング先で有効なアクセス ID として認識されません）

（認証ローミング-システム構成）



(*1) ローミング処理は、POPCHATのWAN側ネットワークを介しておこなわれます
ローミング対象データ）
－認証情報
－アクセスID
(*2) POPCHATのLAN側インターフェースは、同じIPアドレス（およびMACアドレス）にする
（ローミング設定にて、同じチャンネルに設定することで同じMACアドレスが設定されます）
(*3) ネットワークA、B間で、DHCPアドレス範囲が重ならないようにする
（DHCPアドレスは、POPCHATにて払いだされます）
(*4) 端末が別のネットワークに移動しても、DHCPアドレスはそのまま引き継がれます

3 接続管理

3－1. 接続状況

本装置配下の端末接続状況を表示するための機能です。

※現在接続中および認証済の端末が表示されます。

※物理的に接続されている場合でも、通信が発生していない場合、一定時間（15 分）たつと
表示されなくなります

■接続状況

接続ポート	IPアドレス ／MACアドレス	接続方式	開始	終了	接続開始/終了	
–	192.168.1.1 / [redacted]88:D6:C2				接続開始	
	192.168.1.2 / [redacted]3D:93:2A	Private	2017/05/16 18:59:40	2017/05/16 19:59:39		接続終了

接続状況	接続ポート	端末が接続されているポートを表示 ※オプション設定の"接続ポート設定を使用する"が有効な場合、対象ポートのポートラベルで表示されます。（「基本設定-オプション設定」のポリシー設定にて"接続ポート設定を使用する"）
	MAC アドレス	端末の MAC アドレスを表示
	接続方式	端末にて、接続認証した際の接続方式を表示
	開始	端末の接続開始日時を表示
	終了	端末の接続終了日時を表示
	接続開始ボタン	対象端末を接続認証します。
	接続終了ボタン	対象端末を接続終了します。

各種制限状態の表示

接続ポート	IPアドレス ／MACアドレス	接続方式	開始	終了	接続開始/終了	
–	192.168.1.1 / [redacted] Session				接続開始	
	192.168.1.4 / [redacted]	Private	2014/01/14 11:53:44	2014/01/18 15:54:44		接続終了
	192.168.1.3 / [redacted]	Private	2014/01/14 11:42:44	2014/01/18 15:43:44		接続終了
	192.168.1.2 / [redacted] Spam	Private	2014/01/10 22:44:35	2014/01/15 02:45:35		接続終了

各種制限が有効な場合、制限の種類を示すアイコンとともに、背景色ありで表示されます。

セッション制限（1）　：　session アイコン、背景色　黄色で表示
セッション制限（2）　：　session アイコン、背景色　赤色で表示
スパム制限　　：　spam アイコン、背景色　赤色で表示
帯域制限　　：　traffic アイコン、背景色　赤色で表示

3－2. 基本接続設定

本装置配下の端末が接続する際の基本設定（既定値）を設定するための機能です。

■基本接続設定

※は必須項目ですので必ず入力して下さい

接続方式※	Private接続
認証方式※	ベーシック認証
課金金額	円

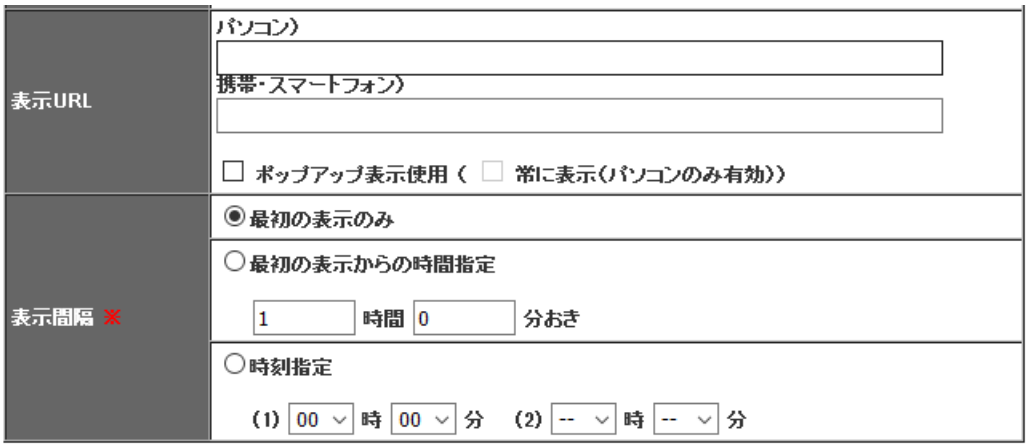
接続方式 （Global 接続アドレス（DHCP）が有効、かつ、割当アドレスが「Private 接続アドレス」がの場合のみ表示）	端末に割当てられるアドレスを選択します	
	Private 接続	端末には、Private 接続アドレスが割当てられます。 インターネット接続の際は、本装置の WAN 側 IP アドレスで通信します。
	Global/Private 接続	認証画面のプルダウンメニューで Private アドレスか Global アドレスの割当選択ができるようになります。 「基本設定-DHCP 設定」の割当アドレスの設定により動作が変わります。 ＞割当アドレスが「Private 接続アドレス」の場合 端末には、まず Private 接続アドレスがわりあてられます。接続認証後、対象端末に Global 接続アドレスがわりあてられます。 （対象端末は、再起動等により、IPアドレスの再割当させる必要があります） インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。 ＞割当アドレスが「Global 接続アドレス」の場合 端末には、Global 接続アドレスがわりあてられます。インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。

認証方式	端末が接続認証する際の認証方式を選択します	
	ベーシック認証	接続開始の際、認証画面が表示されます。 （利用者が接続開始ボタンをクリックすることで認証処理されます。）
	フリー認証	接続開始の際、認証画面を表示せずに、自動で認証処理されます。
	アクセス ID 認証	接続開始の際、アクセス ID を入力する認証画面が表示されます。 アクセス ID を入力し、接続開始ボタンをクリックすることで認証処理されます。 接続時間は、アクセス ID ごとに設定されます。
	@Cloud サービス認証	接続開始の際、@クラウドによる認証画面が表示されます。
	Radius 認証 （MicroPOPCHAT はオプション）	接続開始の際、アカウントとパスワードを入力する認証画面が表示されます。 アカウントおよびパスワードを入力し、接続開始ボタンをクリックすることで認証処理されます。
課金金額 （@Cloud サービス認証では非表示）	接続方式ごとの課金金額を設定します。 ※課金金額は認証画面で表示され、認証ログに記録されます。	
	Global 接続	課金金額を指定します。 ※接続方式が「Global/Private 接続」に設定されているときに表示されます。
	Private 接続	課金金額を指定します。

（前の画面の続き）

接続時間	接続開始からの接続有効期間を指定します。 ※アクセス ID 認証と@Cloud サービス認証の場合は表示されません。	
	接続時間指定	接続開始からの時間で指定する場合、こちらを使用します。
	時刻指定	毎日の時刻範囲で接続指定したい場合、こちらを使用します。
	期間指定	期間指定で設定したい場合、こちらを使用します。 終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。

（前の画面の続き）

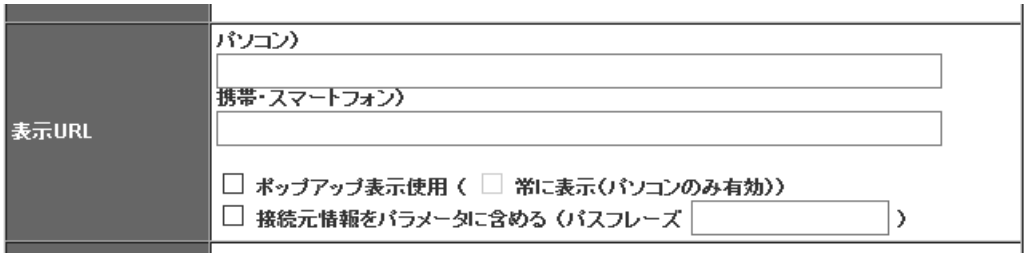


表示 URL	接続開始後、および、任意の間隔で、表示させる URL を指定します。 ※オプション設定の"指定 URL の表示(リダイレクト/ポップアップ)をおこなう"が有効な場合、表示される項目です。		
	パソコン	端末がパソコンの場合に表示させる URL を指定します	
	携帯・スマートフォン	端末が携帯・スマートフォンの場合に表示させる URL を指定します	
	ポップアップ表示使用	ポップアップ・ウィンドウで表示させる場合、チェックします。 ※認証方式が「フリー認証」および、「@Cloud サービス認証」の場合、ポップアップは表示しません。 ※端末で Java Script が無効になっている場合、ポップアップのリダイレクトは表示されません。	
		常に表示	ポップアップ・ウィンドウを常に表示させたい場合、チェックします。 ポップアップ・ウィンドウを閉じても、1～2 分で表示再開します ※端末がパソコンの場合のみ有効です。
表示間隔	表示 URL で指定された URL を表示する間隔を指定します。 ※オプション設定の"指定 URL の表示(リダイレクト/ポップアップ)をおこなう"が有効な場合、表示される項目です。		
	最初の表示のみ	認証時のみの場合に使用します。	
	最初の表示からの時間指定	時間経過で表示する場合に使用します。	
	時刻指定	毎日定刻で設定したい場合に使用します。	

○指定 URL への接続元情報の送信

オプション設定の"接続ポート設定を使用する"を有効にした場合、接続元情報を、表示 URL に送信するための設定項目(「接続元情報をパラメータに含める」)が追加されます。

接続元情報をもとに、表示 URL の宛先側にて、動作切替えるなどが可能となります。



※表示 URL に接続元パラメータを含める場合、「接続元情報をパラメータに含める」をチェックします。

※パスフレーズ欄には、改ざんチェック用のパスフレーズを指定します。

○接続元情報の改ざんチェック(以下)

①以下文字列を結合し、ハッシュ値(MD5)を求める。

事前に決めたパスフレーズ ＋接続元情報

＊接続元情報（接続ポート ＋ 接続ポートラベル ＋ 接続元アクセスポイント）

②受け取った「認証キー」が、①で求めたハッシュ値と一致する場合は、チェックOK

〇送信される接続元情報

No	パラメータ	項目	備考
1	port	接続ポート	※ポート検出「SNMP」の場合 SW-HUB の IP アドレス、ポート番号 例）192.168.1.100:1 ※ポート検出「タグ VLAN」の場合 タグ VLAN 例）100
2	label	接続ポートラベル	
3	wap	接続元アクセスポイント	※アクセスポイントの MAC アドレス

3－3. 接続ポート設定

本装置配下の端末の接続ポートを登録するための機能です。
本機能は、オプション設定の"接続ポート設定を使用する"が有効な場合のみ表示されます。

ポート検出方式により、設定画面が異なります

A）ポート検出方式：SNMP
A－1）接続ポート一覧画面

■接続ポート設定

接続ポート追加

	SNMP HUB	MIB種別	Community	ポート	ポートラベル	グループ	
□	192.168.1.2	標準MIB	public	4	gest room 01	--	ラベル・接続設定
□				5	gest room 02	--	ラベル・接続設定

接続ポート削除

接続ポート設定	SNMP HUB	スイッチングハブの IP アドレス
	MIB 種別	接続ポート追加時に指定したスイッチングハブの MIB 種別
	Community	接続ポート追加時に指定したスイッチングハブのコミュニティ
	ポート	検出されたポート ※論理的なポートも表示されることがあります。
	グループ	接続ポートが所属するグループ
	ポートラベル	接続ポートに付与されたポートラベル ※デフォルトはスイッチングハブの IP とポート番号が設定されます。
	接続ポート追加	接続ポート追加画面に遷移します。 ※最大数の登録が設定されていると、接続ポート追加ができなくなります。
	ラベル・接続設定	ラベル・接続設定画面に遷移します。
	接続ポート削除	チェックを入れた接続ポートを削除します。 ※論理ポートやカスケードポートなど削除します。

A－2）接続ポート追加

■接続ポート設定 （接続ポート追加）

※は必須項目ですので必ず入力して下さい

HUB IPアドレス※	. . .
MIB種別※	標準MIB
Community※	
グループ	-- グループ名

登 録

HUB IP アドレス	接続ポートを追加するスイッチングハブの IP アドレスを設定します。
MIB 種別	接続ポートを追加するスイッチングハブの MIB 種別を設定します。
Community	接続ポートを追加するスイッチングハブのコミュニティ名を設定します。
グループ	グループを指定します。 (「追加」を選択し、グループ名を指定することで、新規グループが作成できます)

A－3）ラベル・接続設定画面

■接続ポート設定 （ラベル・接続設定）

※は必須項目ですので必ず入力して下さい

接続ポート※	192.168.1.2:4
ポートラベル※	gest room 01
グループ	-- グループ名

☐以下項目をポート単位に設定する

接続方式※	Private接続
認証方式※	ベーシック認証
課金金額	円

接続ポート	接続ポートのスイッチングハブの IP アドレスとポート番号
ポートラベル	接続ポートの名称を指定します。(接続ポートにつながっている部屋名など)
グループ	グループを指定します。 (「追加」を選択し、グループ名を指定することで、新規グループが作成できます)

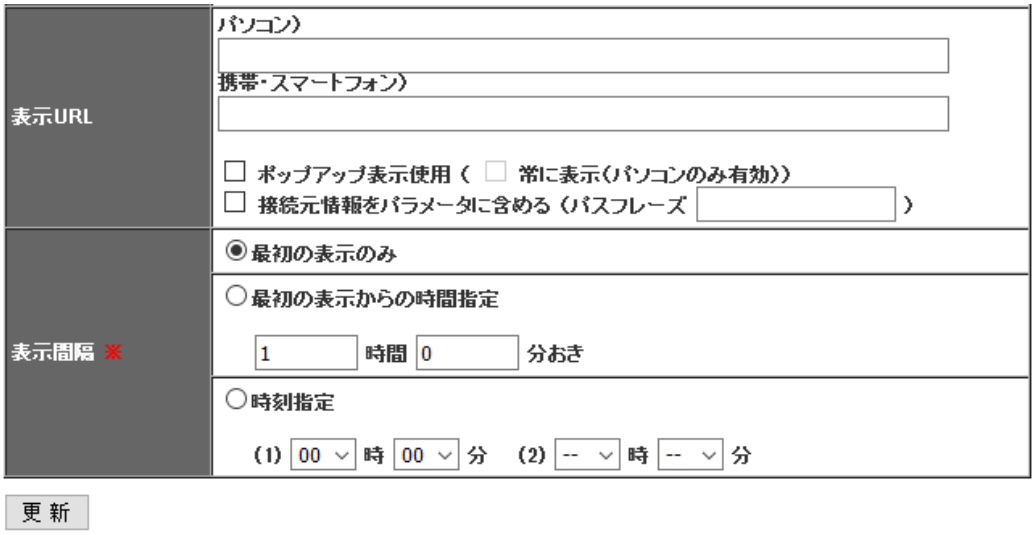
<table>
<tr><td>【以下項目を個別に設定する】</td><td colspan="2">接続ポートに個別の設定をしたい場合、チェックします。
※基本設定>オプション設定のオプションの設定により下記の動きになります。
〇ポート検出方式にて、「ポート単位」を選択の場合
「以下項目をポート単位に設定する」: 接続ポートにポート単位に接続設定したい場合にチェックします。
〇ポート検出方式にて、「グループ単位」を選択の場合
「以下項目をグループ単位に設定する」: 接続ポートにグループ単位で接続設定したい場合にチェックします。
※チェックしない場合は、基本接続設定の設定が有効となります。
※接続方式、認証方式など、各項目は、「接続管理-基本接続設定」を参照してください。</td></tr>
<tr><td rowspan="3">接続方式
（Global 接続アドレス（DHCP）が有効、かつ、割当アドレスが「Private 接続アドレス」がの場合のみ表示）</td><td colspan="2">端末に割当てられるアドレスを選択します</td></tr>
<tr><td>Private 接続</td><td>端末には、Private 接続アドレスが割当てられます。
インターネット接続の際は、本装置の WAN 側 IP アドレスで通信します。</td></tr>
<tr><td>Global/Private 接続</td><td>認証画面のプルダウンメニューで Private アドレスか Global アドレスの割当選択ができるようになります。
「基本設定-DHCP 設定」の割当アドレスの設定により動作が変わります。
＞割当アドレスが「Private 接続アドレス」の場合
端末には、まず Private 接続アドレスがわりあてられます。接続認証後、対象端末に Global 接続アドレスがわりあてられます。
（対象端末は、再起動等により、IPアドレスの再割当させる必要があります）
インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。
＞割当アドレスが「Global 接続アドレス」の場合
端末には、Global 接続アドレスがわりあてられます。インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。</td></tr>
<tr><td rowspan="4">認証方式</td><td colspan="2">端末が接続認証する際の認証方式を選択します</td></tr>
<tr><td>ベーシック認証</td><td>接続開始の際、認証画面が表示されます。
（利用者が接続開始ボタンをクリックすることで認証処理されます。）</td></tr>
<tr><td>フリー認証</td><td>接続開始の際、認証画面を表示せずに、自動で認証処理されます。</td></tr>
<tr><td>アクセス ID 認証</td><td>接続開始の際、アクセス ID を入力する認証画面が表示されます。
アクセス ID を入力し、接続開始ボタンをクリックすることで認証処理されます。
接続時間は、アクセス ID ごとに設定されます。</td></tr>
</table>

	@Cloud サービス認証	接続開始の際、@クラウドによる認証画面が表示されます。
	Radius 認証 （MicroPOPCHAT はオプション）	接続開始の際、アカウントとパスワードを入力する認証画面が表示されます。 アカウントおよびパスワードを入力し、接続開始ボタンをクリックすることで認証処理されます。
課金金額 （@Cloudサービス認証では非表示）	接続方式ごとの課金金額を設定します。 ※課金金額は認証画面で表示され、認証ログに記録されます。	
	Global 接続	課金金額を指定します。 ※接続方式が「Global/Private 接続」に設定されているときに表示されます。
	Private 接続	課金金額を指定します。

（前の画面の続き）

接続時間	接続開始からの接続有効期間を指定します。 ※アクセス ID 認証と@Cloud サービス認証の場合は表示されません。	
	接続時間指定	接続開始からの時間で指定する場合、こちらを使用します。
	時刻指定	毎日の時刻範囲で接続指定したい場合、こちらを使用します。
	期間指定	期間指定で設定したい場合、こちらを使用します。 終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。

（前の画面の続き）



表示 URL	接続開始後、および、任意の間隔で、表示させる URL を指定します。 ※オプション設定の"指定 URL の表示（リダイレクト/ポップアップ）をおこなう"が有効な場合、表示される項目です。		
	パソコン	端末がパソコンの場合に表示させる URL を指定します	
	携帯・スマートフォン	端末が携帯・スマートフォンの場合に表示させる URL を指定します	
	ポップアップ表示使用	ポップアップ・ウィンドウで表示させる場合、チェックします。 ※認証方式が「フリー認証」および、「@Cloud サービス認証」の場合、ポップアップは表示しません。 ※端末で Java Script が無効になっている場合、ポップアップのリダイレクトは表示されません。	
		常に表示	ポップアップ・ウィンドウを常に表示させたい場合、チェックします。 ポップアップ・ウィンドウを閉じても、1～2 分で表示再開します ※端末がパソコンの場合のみ有効です。
	接続元情報をパラメータに含める	表示 URL に接続元パラメータを含める場合、チェックします。	
		パスフレーズ	改ざんチェック用のパスフレーズを指定します。

表示間隔	表示 URL で指定された URL を表示する間隔を指定します。 ※オプション設定の"指定 URL の表示(リダイレクト/ポップアップ)をおこなう"が有効な場合、表示される項目です。	
	最初の表示のみ	認証時のみの場合に使用します。
	最初の表示からの時間指定	時間経過で表示する場合に使用します。
	時刻指定	毎日定刻で設定したい場合に使用します。

○接続元情報の改ざんチェック(以下)

①以下文字列を結合し、ハッシュ値(MD5)を求める。

事前に決めたパスフレーズ ＋接続元情報

＊接続元情報(接続ポート ＋ 接続ポートラベル ＋ 接続元アクセスポイント)

②受け取った「認証キー」が、①で求めたハッシュ値と一致する場合は、チェックOK

○送信される接続元情報

No	パラメータ	項目	備考
1	port	接続ポート	※ポート検出「SNMP」の場合 SW-HUB の IP アドレス、ポート番号 例)192.168.1.100:1 ※ポート検出「タグ VLAN」の場合 タグ VLAN 例)100
2	label	接続ポートラベル	
3	wap	接続元アクセスポイント	※アクセスポイントの MAC アドレス

B)ポート検出方式:タグ VLAN

B－1)接続ポート一覧画面

■接続ポート設定

接続ポート追加

	ポート(タグVLAN)	ポートラベル	グループ	
☐	10	gest room01	--	ラベル・接続設定
☐	20	gest room02	--	ラベル・接続設定

接続ポート削除

接続ポート設定	ポート(タグ VLAN)	登録したタグ VLAN ID
	ポートラベル	接続ポートに付与されたポートラベル ※デフォルトは VLAN ID が設定されます。
	グループ	接続ポートが所属するグループ
	接続ポート追加	接続ポート追加画面に遷移します。
	ラベル・接続設定	ラベル・接続設定画面に遷移します。
	接続ポート削除	チェックを入れた接続ポートを削除します。

B－2)接続ポート追加

■接続ポート設定 (接続ポート追加<タグVLAN登録>)

※は必須項目ですので必ず入力して下さい

タグVLAN※	
グループ	-- グループ名
登録数※	01個

登 録

タグ VLAN	登録する先頭のタグ VLAN ID を設定します。 ※ポート検出「タグ VLAN」の場合、登録された接続ポートからのみ認証が可能です。
グループ	グループを指定します。 (「追加」を選択し、グループ名を指定することで、新規グループが作成できます)
登録数	登録するタグ VLAN ID の数を指定します。 (複数のタグを一度に登録したい場合に使用します)

Ｂ－3）ラベル・接続設定画面

■接続ポート設定 （ラベル・接続設定）

※は必須項目ですので必ず入力して下さい

接続ポート※	10
ポートラベル※	gest room01
グループ	-- グループ名

☐以下項目をポート単位に設定する

接続方式※	Private接続
認証方式※	ベーシック認証
課金金額	円

接続ポート	接続ポートの VLANID
ポートラベル	接続ポートの名称を指定します。（接続ポートにつながっている部屋名など）
グループ	グループを指定します。 （「追加」を選択し、グループ名を指定することで、新規グループが作成できます）
【以下項目を個別に設定する】	接続ポートに個別の設定をしたい場合、チェックします。 ※基本設定>オプション設定のオプションの設定により下記の動きになります。 〇ポート検出方式にて、「ポート単位」を選択の場合 「以下項目をポート単位に設定する」: 接続ポートにポート単位に接続設定したい場合にチェックします。 〇ポート検出方式にて、「グループ単位」を選択の場合 「以下項目をグループ単位に設定する」: 接続ポートにグループ単位で接続設定したい場合にチェックします。 ※チェックしない場合は、基本接続設定の設定が有効となります。 ※接続方式、認証方式など、各項目は、「接続管理−基本接続設定」を参照してください。

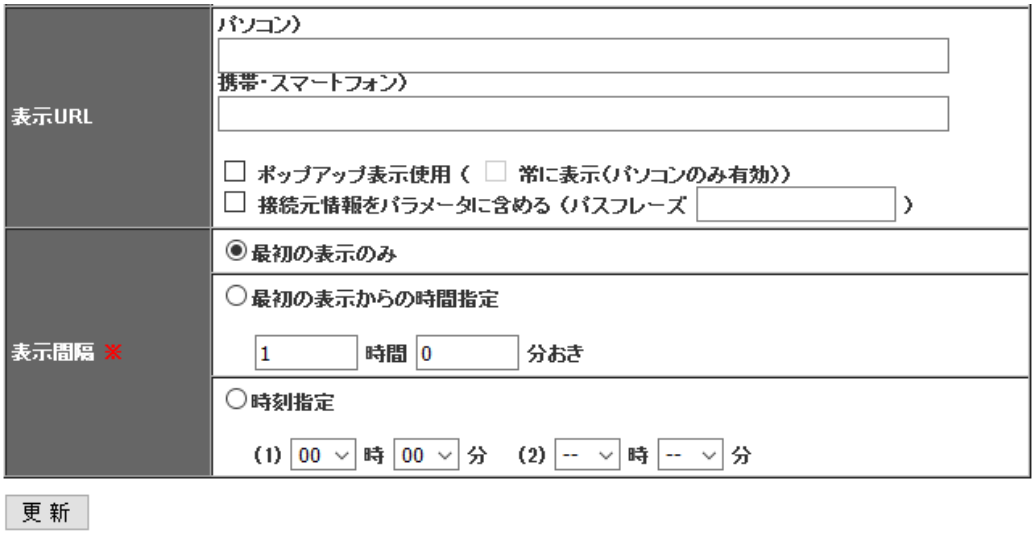
接続方式 （Global 接続アドレス（DHCP）が有効、かつ、割当アドレスが「Private 接続アドレス」がの場合のみ表示）	端末に割当てられるアドレスを選択します	
	Private 接続	端末には、Private 接続アドレスが割当てられます。 インターネット接続の際は、本装置の WAN 側 IP アドレスで通信します。
	Global/Private 接続	認証画面のプルダウンメニューで Private アドレスか Global アドレスの割当選択ができるようになります。 「基本設定-DHCP 設定」の割当アドレスの設定により動作が変わります。 ＞割当アドレスが「Private 接続アドレス」の場合 端末には、まず Private 接続アドレスがわりあてられます。接続認証後、対象端末に Global 接続アドレスがわりあてられます。 （対象端末は、再起動等により、IPアドレスの再割当させる必要があります） インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。 ＞割当アドレスが「Global 接続アドレス」の場合 端末には、Global 接続アドレスがわりあてられます。インターネット接続の際は、端末のわりあてられた Global 接続アドレスで通信します。
認証方式	端末が接続認証する際の認証方式を選択します	
	ベーシック認証	接続開始の際、認証画面が表示されます。 （利用者が接続開始ボタンをクリックすることで認証処理されます。）
	フリー認証	接続開始の際、認証画面を表示せずに、自動で認証処理されます。
	アクセス ID 認証	接続開始の際、アクセス ID を入力する認証画面が表示されます。 アクセス ID を入力し、接続開始ボタンをクリックすることで認証処理されます。 接続時間は、アクセス ID ごとに設定されます。
	@Cloud サービス認証	接続開始の際、@クラウドによる認証画面が表示されます。
	Radius 認証 （MicroPOPCHAT はオプション）	接続開始の際、アカウントとパスワードを入力する認証画面が表示されます。 アカウントおよびパスワードを入力し、接続開始ボタンをクリックすることで認証処理されます。

課金金額 （@Cloudサービス認証では非表示）	接続方式ごとの課金金額を設定します。 ※課金金額は認証画面で表示され、認証ログに記録されます。	
	Global 接続	課金金額を指定します。 ※接続方式が「Global/Private 接続」に設定されているときに表示されます。
	Private 接続	課金金額を指定します。

（前の画面の続き）

接続時間	接続開始からの接続有効期間を指定します。 ※アクセス ID 認証と@Cloud サービス認証の場合は表示されません。	
	接続時間指定	接続開始からの時間で指定する場合、こちらを使用します。
	時刻指定	毎日の時刻範囲で接続指定したい場合、こちらを使用します。
	期間指定	期間指定で設定したい場合、こちらを使用します。 終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。

（前の画面の続き）



表示 URL	接続開始後、および、任意の間隔で、表示させる URL を指定します。 ※オプション設定の"指定 URL の表示（リダイレクト/ポップアップ）をおこなう"が有効な場合、表示される項目です。		
	パソコン	端末がパソコンの場合に表示させる URL を指定します	
	携帯・スマートフォン	端末が携帯・スマートフォンの場合に表示させる URL を指定します	
	ポップアップ表示使用	ポップアップ・ウィンドウで表示させる場合、チェックします。 ※認証方式が「フリー認証」および、「@Cloud サービス認証」の場合、ポップアップは表示しません。 ※端末で Java Script が無効になっている場合、ポップアップのリダイレクトは表示されません。	
		常に表示	ポップアップ・ウィンドウを常に表示させたい場合、チェックします。 ポップアップ・ウィンドウを閉じても、1～2 分で表示再開します ※端末がパソコンの場合のみ有効です。
	接続元情報をパラメータに含める	表示 URL に接続元パラメータを含める場合、チェックします。	
		パスフレーズ	改ざんチェック用のパスフレーズを指定します。

表示間隔	表示 URL で指定された URL を表示する間隔を指定します。 ※オプション設定の"指定 URL の表示(リダイレクト/ポップアップ)をおこなう"が有効な場合、表示される項目です。	
	最初の表示のみ	認証時のみの場合に使用します。
	最初の表示からの時間指定	時間経過で表示する場合に使用します。
	時刻指定	毎日定刻で設定したい場合に使用します。

○接続元情報の改ざんチェック(以下)

①以下文字列を結合し、ハッシュ値(MD5)を求める。

事前に決めたパスフレーズ ＋接続元情報

＊接続元情報(接続ポート ＋ 接続ポートラベル ＋ 接続元アクセスポイント)

②受け取った「認証キー」が、①で求めたハッシュ値と一致する場合は、チェックOK

○送信される接続元情報

No	パラメータ	項目	備考
1	port	接続ポート	※ポート検出「SNMP」の場合 SW-HUB の IP アドレス、ポート番号 例)192.168.1.100:1 ※ポート検出「タグ VLAN」の場合 タグ VLAN 例)100
2	label	接続ポートラベル	
3	wap	接続元アクセスポイント	※アクセスポイントの MAC アドレス

3－4. アクセス ID 設定

本装置配下の端末が接続認証する際のアクセス ID を登録するための機能です。
アクセス ID は、認証方式が「アクセス ID 認証」の場合に使用します。

1）アクセス ID 一覧画面

■アクセスID設定

アクセスID作成　CSVファイル出力

	発行日時	アクセスID名称	アクセスID	有効ポート	有効期間(From)	有効期間(To)	有効回数

アクセスID削除

アクセス ID 設定	発行日時	アクセス ID の発行日時
	アクセス ID 名称	アクセス ID の名称
	アクセス ID	認証時に入力する文字列(アクセス ID をクリックすることでアクセス ID 印刷画面が表示されます)
	有効ポート	アクセス ID が有効（使用可能）な接続ポート、あるいはグループ ※"－"の場合、有効ポートの制限なく、どの接続ポートでも使用が可能であることを意味します。
	有効期間	アクセス ID で接続認証した際の接続有効期間
	有効回数	アクセス ID が使用可能な回数
	アクセス ID 作成	アクセス ID 作成画面に遷移します。
	CSV ファイル出力	一覧データを CSV ファイルで出力します。
	アクセス ID 削除	アクセス ID を削除します。

2)アクセス ID 作成画面

（接続ポート検出なし）

■アクセスID設定 （アクセスID作成）

※は必須項目ですので必ず入力して下さい

アクセスID名称	
先頭コード※	PWD
有効期間 ※	◉接続時間指定 時間 分まで ○時刻指定 00 時 00 分 ～ 00 時 00 分 ○期間指定 開始 2017 年 05 月 26 日 10 時 10 分 終了 2017 年 05 月 26 日 10 時 20 分
有効回数※	○無制限 ◉ 1 回
発行数※	01個 個

更 新

アクセス ID 名称	アクセス ID の名称を指定します。	
先頭コード	アクセス ID の先頭コードを指定します。（1～3 桁まで指定が可能、大文字小文字を判定しません）	
有効期間	アクセス ID で接続した際の接続有効期間を指定します。	
	接続時間指定	接続開始からの時間で指定する場合、選択します。
	時刻指定	毎日、定刻で設定したい場合、選択します。
	期間指定	期間指定で設定したい場合、選択します。 期間指定で、終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。 期間指定の終了時間が過ぎた場合、当該アクセス ID は自動削除されます。
有効回数	アクセス ID が使用可能な回数を指定します。（無制限 or 1～99）	
発行数	アクセス ID の発行数を指定します。 （同じ設定でアクセス ID を複数作成したい場合などに使用します）	

（接続ポート検出あり） ※接続ポート設定を使用する"（「基本設定-オプション設定」）場合

■アクセスID設定 （アクセスID作成）

※は必須項目ですので必ず入力して下さい

アクセスID名称	
先頭コード※	PWD
有効ポート ※	◉指定しない ○ポート指定 gest room01 gest room02 ○グループ指定
有効期間 ※	◉接続時間指定 時間 分まで ○時刻指定 00 時 00 分 ～ 00 時 00 分 ○期間指定 開始 2017 年 05 月 26 日 10 時 20 分 終了 2017 年 05 月 26 日 10 時 30 分
有効回数※	○無制限 ◉ 1 回
発行数※	01個 個

更 新

アクセス ID 名称	アクセス ID の名称を指定します。	
先頭コード	アクセス ID の先頭コードを指定します。（1～3 桁まで指定が可能、大文字小文字を判定しません）	
有効ポート	アクセス ID の有効（使用可能）範囲を「指定しない」、「ポート単位」、「グループ単位」から指定します	
有効期間	アクセス ID で接続した際の接続有効期間を指定します。	
	接続時間指定	接続開始からの時間で指定する場合、選択します。
	時刻指定	毎日、定刻で設定したい場合、選択します。
	期間指定	期間指定で設定したい場合、選択します。 期間指定で、終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。 期間指定の終了時間が過ぎた場合、当該アクセス ID は自動削除されます。
有効回数	アクセス ID が使用可能な回数を指定します。（無制限 or 1～99）	

発行数	アクセス ID の発行数を指定します。 （同じ設定でアクセス ID を複数作成したい場合などに使用します）

3)アクセス ID 印刷画面

■アクセスID設定

アクセスID作成　CSVファイル出力

	発行日時	アクセスID名称	アクセスID	有効ポート	有効期間(From)	有効期間(To)	有効回数
☐	2017/05/24 19:02:00	1dayチケット	PWD51892	-	00:00	00:00	00/01

アクセスID削除

（日本語での表示）

日本語での表示　プリント

1dayチケット

（アクセスID） PWD51892

有効期間　00時00分 ～ 00時00分

※インターネット接続開始画面に入力してください。
※ご利用可能回数:1

（中国語での表示）

中国語での表示　プリント

1dayチケット

（ID） PWD51892

有效期　00:00 ～ 00:00

※请在连接开始画面输入
※是到利用的终端 1 台可以使用

（韓国語での表示）

韓国語での表示　プリント

1dayチケット

（ID） PWD51892

유효기간　00:00 ～ 00:00

※접속 화면에 입력해 주십시오
※이용의 단말 1 대까지 사용가능합니다

（英語での表示）

英語での表示　プリント

1dayチケット

（ID） PWD51892

Available time　00:00 ～ 00:00

* This ID is for Internet Access Service.
* You can use up to 1 terminal of available.

※言語選択プルダウンを選択することで、表示言語を切り替え
※"プリント"ボタンをクリックすることで、以下内容が印刷されます。(ブラウザの印刷機能を使用)
　ーアクセス ID 名称
　ーアクセス ID
　ー有効期間
　ー有効端末数
※アクセス ID 印刷画面のウィンドウサイズ(400×250)
※用紙サイズ:A4、はがき、名刺　での印刷に対応
(各用紙サイズに合わせて、ブラウザのページ設定で、余白、ヘッダ、フッタの調整が必要です。)

3－5. 接続履歴

本装置配下の端末の接続履歴を表示するための機能です。

■接続履歴

※最新100件まで表示
（それ以前のものは「CSV出力」で確認してください）

CSVファイル出力

開始	終了	IPアドレス	MACアドレス	接続方式	接続ポート	アクセスID	言語
2017/05/16 20:13:59	2017/05/16 20:15:44	192.168.1.2	E4:98:D6:3D:93:2A	Private	-		ja

---

接続履歴	開始	接続開始日時（端末が接続認証した日時）
	終了	接続終了日時 （端末の接続認証が終了/解除された日時）
	IP アドレス	端末の IP アドレス
	MAC アドレス	端末の MAC アドレス
	接続方式	端末が接続認証した際の接続方式
	接続ポート	端末が接続認証した際の接続ポート ※"接続ポート設定を使用する"（「基本設定-オプション設定」）の場合のみ該当する接続ポートのポートラベルが表示されます。
	アクセス ID	端末が接続認証した際のアクセス ID ※認証方式が「アクセス ID 認証」の場合、アクセス ID が表示されます。「Radius 認証」の場合、Radius アカウントが表示されます。
	言語	端末ブラウザの言語設定
	CSV ファイル出力	一覧データを CSV ファイルで出力します。

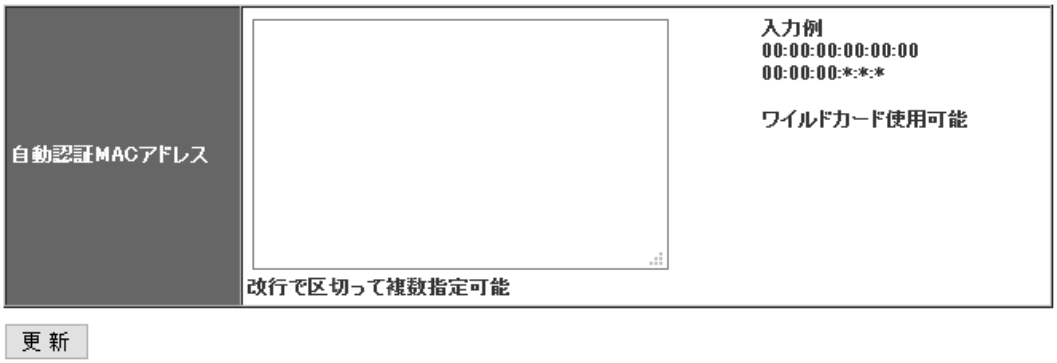
※接続履歴の保持日数は 90 日。ただし、ディスクの書き込み可能残容量が少ない場合、保持日数は保証されません。（ログは 1 日 1 回、自動でセンターサーバへバックアップされます。）

※認証方式「@Cloud サービス認証」の接続履歴は、@クラウドに保存され、本画面上には表示されません。

3－6. 自動認証設定

本装置配下の端末のうち、認証画面を表示することなく、自動で認証させる端末を設定するための機能です。

■自動認証設定



自動認証 MAC アドレス	認証画面を表示することなく、自動で認証する MAC アドレスを指定します。（改行で区切って複数指定及び、ワイルドカード指定が可能です。） ※自動認証設定による認証の場合、接続期間は無期限です。 ※自動認証設定は、接続されたポートの認証方式（フリー認証、アクセスID認証）より優先されます。 （登録可能な MAC アドレスは 100）

3－7. @Cloud サービス

接続する @Cloud サービスのサーバ（クラウド認証エンジン）を設定します。

■@Cloudサービス

アカウントID　　パスワード

※は必須項目ですので必ず入力して下さい

サーバアドレス※	. . .
サーバFQDN	☐ httpsを使用する

更 新

アカウント ID	@Cloud サービスのアカウント ID を指定します。
パスワード	@Cloud サービスのパスワード を指定します。 ※アカウント ID、パスワードが正しくない場合、サーバドレスは設定されません。
サーバドレス	@Cloud サービスのサーバ（クラウド認証エンジン）のアドレスを指定します。
サーバ FQDN	@Cloud サービスのサーバ（クラウド認証エンジン）の FQDN を指定します。
https を使用する	@Cloud の認証画面を、https で表示させる場合、チェックします。

アカウント ID・パスワード・サーバアドレス・サーバ FQDN の情報は製品に添付されている『POPCHAT 納品情報・@Cloud アカウント登録票』を参照ください。

※以下は、2021 年 1 月リリース版「@クラウド連携個別パッチ」を適用した POPCHAT 又は 2021 年 2 月以降に出荷された POPCHAT のみが対象となります。

■@Cloudサービス

アカウントID　　パスワード

※は必須項目ですので必ず入力して下さい

認証サーバ（FQDN）※	

更 新

「サーバアドレス」と「https を使用する」の項目が廃止となっております。

■ 仮認証制限を解除する

上記設定画面にて何も変更しない状態（パスワードは必要となります）で「更新」ボタンを押下すると、全ての端末の仮認証制限は解除され、仮認証回数も「0」からのカウントとなります。

※上記の更新では POPCHAT の再起動は伴いません。

3－8. Radius 連携 （オプション）

本装置配下の端末が接続認証する際のアカウント／パスワードを問い合わせる Radius サーバを設定するための機能です。 （MicroPOPCHAT はオプション）
※Radius サーバは、認証方式が「Radius 認証」の場合に使用します。

■Radius連携

サーバアドレス	. . .
ポート番号	
暗号キー	
優先設定	☐ Radiusの有効期間を使用する

更 新

サーバドレス	Radius サーバのアドレスを設定します。
ポート番号	Radius サーバのポート番号を設定します。
暗号キー	暗号キーを設定します。
優先設定	認証の接続期間を、Radius アカウントの有効期間にする場合チェックします。

※Radius サーバ連携仕様
問合せの再送回数 ： 3 回 （タイムアウト:5 秒）
認証方式 ： PAP

※POPCHAT から Radius サーバに受け渡す情報
NAS-IP-Address ： NAS の IP アドレス（POPCHAT の IP アドレス）
User-Name ： ユーザ ID
User-Password ： パスワード
Calling-Station-Id ： 端末の MAC アドレス
（以下、VSA）
POPCHAT_CALLING_STATION_IP_ADDRESS ： 端末の IP アドレス ＜VSA＞
POPCHAT_CALLING_STATION_CONPORT ： 端末の接続ポート ＜VSA＞

⇒ VSA 登録用の dictionary ファイルは以下よりダウンロード可能
http://popchat.jp/download/radius_vsa_dictionary.zip

4 ポート転送/制限

4－1. ポート転送

本装置の WAN 側から LAN 側の機器へ本装置の WAN 側 IP アドレスのポートを通して転送をするための機能です。

■ポート転送

※ルールは上から順に適用されます

No	tcp/udp	対象ポート番号	転送先アドレス	転送先ポート番号
1	--			
2	--			
3	--			
4	--			
5	--			
6	--			
7	--			
8	--			
9	--			
10	--			

更 新　　入力枠 追加

ポート転送	tcp/udp	転送対象のプロトコルを「tcp」「udp」「tcp/udp」より選択します。
	対象ポート番号	転送（される本装置）のポート番号を指定します。 ※ポート番号は、49152 から 65535 までの範囲のみ指定可
	転送先アドレス	転送先の IP アドレスを指定します。
	転送先ポート番号	転送先のポート番号を指定します。
	入力枠 追加	入力枠を追加します （最大登録数は 100）

4－2. フィルタリング

IP アドレス及び、ポート指定による通信の遮断/許可をするための機能です。

※フィルタリング設定は、未認証／認証済にかかわらず、利用者端末に対して適用されます。

■フィルタリング

※ルールは上から順に適用されます

No	発信元(from)	相手先(to)	tcp/udp/icmp	ポート番号	遮断/許可
1			--		--
2			--		--
3			--		--
4			--		--
5			--		--
6			--		--
7			--		--
8			--		--
9			--		--
10			--		--

更 新　　入力枠 追加

フィルタリング	発信元(from)	発信元の IP アドレスを入力します。 ※ネットワークアドレスでの設定も可能 （例、192.168.1.1 から 192.168.1.254 までのアドレスを指定するときに、「192.168.1.0/24」で設定します）
	相手先（to）	通信の相手先の IP アドレスを指定します。 ※ネットワークアドレスでの設定も可能
	tcp/udp/icmp	通信プロトコルとして、以下から選択します。 「tcp」、「udp」、「tcp/udp」、「icmp」
	ポート番号	通信の相手先のポート番号を指定します。
	遮断/許可	通信の「遮断」あるいは「許可」を選択します。
	入力枠　追加	入力枠を追加します （最大登録数は 100）

4－3. MAC フィルタリング

登録された MAC アドレスによる通信の遮断と遮断対象からの除外をするための機能です。

※認証やフィルタリングよりも下層での制御となり、arp やブロードキャスト・フレームなどのレイヤ 2 レベルでの制御が可能です。
※フィルタリングルールは上から順に適用されます。
特定アドレスを遮断の対象外にしたい場合、遮断のルールの前に、対象アドレスの許可ルールを登録します。

■MACフィルタリング

※ルールは上から順に適用されます

No	発信元(from)	遮断/除外
1		--
2		--
3		--
4		--
5		--
6		--
7		--
8		--
9		--
10		--

更 新　　入力枠 追加

MAC フィルタリング	発信元(from)	通信の発信元の MAC アドレスを入力します。 ※ワイルドカード指定によるベンダーコードの指定も可能です。 例、00:00:00:*:*:* など。
	遮断/除外	通信の「遮断」あるいは「除外」を選択します。
	入力枠 追加	入力枠を追加します （最大登録数は 100）

5 ネットワーク監視

5－1. 監視状況

本装置の状態、及びネットワーク機器の状態を確認するための機能です。

■監視状況

ホスト	サービス	状態	チェック時刻		状況説明
_U00100029OP	[Net] ActiveUser	OK	05-16-2017 20:35:50	1/1	ActiveUser OK - active 1 users
	[Net] AuthLimit@Cloud	OK	05-16-2017 20:35:14	1/1	AuthLimit@Cloud OK - 1
	[Net] DNS	OK	05-16-2017 20:34:37	1/3	OK DNS - 127.0.0.1 reply answer
	[Net] Session	OK	05-16-2017 20:35:01	1/1	Session OK - 閾値範囲内 (95) (limit 500-1500s/1user)
	[Net] Traffic	OK	05-16-2017 20:35:24	1/1	Traffic - TX 0bps, RX 0bps
	[ping] ROUTR 192.168.10.254	OK	05-16-2017 20:35:36	1/3	PING OK - Packet loss = 0%, RTA = 0.60 ms

---

監視項目	監視内容	CRITICAL の閾値
[Net] Active User	インターネット接続中の利用者数	―
[Net] AuthLimit@Cloud	認証された利用者数 (@Cloud サービス上の接続件数)	@Cloud サービス上の認証上限に達した場合
[Net] DNS	DNS サーバの応答監視	DNS サーバから応答がない場合
[Net] Session	全体、および 1 利用者あたりのセッション数	利用者のセッション数が「オプション設定-セッション制限」の"1 利用者あたりセッション数の上限(2)"を超えた場合
[Net] Spam	1 利用者あたりのメール送信数 ※「オプション設定-スパム制限」が有効な場合のみ表示	利用者のメール送信数が「オプション設定-スパム制限」の"1 利用者あたりメール送信の上限"を超えた場合
[Net] Traffic	全体、および 1 利用者あたりのトラフィック	利用者のトラフィックが「オプション設定-帯域制限」の"1 利用者あたり帯域使用量の上限"を超えた場合
[ping] XXXX	「監視設定」画面で登録した監視対象の死活監視	監視対象から ping 応答が正常に返らない場合

※2021 年 1 月リリース版「@クラウド連携個別パッチ」を適用した POPCHAT 又は 2021 年 2 月以降に出荷された POPCHAT のみ下記の項目が追加されております。

■監視状況

ホスト	サービス	状態	チェック時刻		状況説明
_U00100030OP	[Net] ActiveUser	OK	11-18-2020 13:39:18	1/1	ActiveUser OK - active 1 users
	[Net] AuthLimit	OK	11-18-2020 13:38:40	1/1	AuthLimit OK - 5
	[Net] AuthLimit@Cloud	OK	11-18-2020 13:39:02	1/1	AuthLimit@Cloud OK - 2
	[Net] DNS	OK	11-18-2020 13:37:24	1/3	OK DNS - 127.0.0.1 reply answer
	[Net] Session	OK	11-18-2020 13:38:46	1/1	Session - (71)
	[Net] Traffic	OK	11-18-2020 13:39:08	1/1	Traffic - TX 168bps, RX 480bps

---

追加された項目の詳細は以下の通りです。

監視項目	監視内容	CRITICAL の閾値
[Net] Auth Limit	認証された利用者数 (POPCHAT 上の接続件数)	POPCHAT の認証上限に達した場合

5－2. 監視設定

本装置にて、監視するネットワーク機器を登録するための機能です。

■監視設定

※PINGによる監視をおこなう対象を登録します

No	監視対象IPアドレス	監視対象タイプ	
1			監視対象タイプには“SWHUB”、“ROUTR”など、監視対象機器の種類を任意の英数字5文字で指定してください。
2			
3			
4			
5			
6			
7			
8			
9			
10			

更 新　　入力枠 追加

監視設定	監視対象 IP アドレス	監視対象の IP アドレスを指定します。
	監視対象タイプ	監視対象の略称を指定します。 ここで指定した値で、「監視状況」画面にて、表示されます。
	入力枠 追加	入力枠を追加します （登録最大数は 25）

6 メールアドレス認証 （オプション）

アクセス ID の接続申請を管理するための機能です。
（SecurePOPCHAT、MicroPOPCHAT はオプション）
※この機能を使用するには「基本設定」→「オプション設定」の「iPhone/android の wifi ログインページ表示を許可しない」を有効にする必要があります。

6－1. 接続申請状況

接続申請状況を表示するための機能です。
※指定された保持期間（オプション設定）中に更新されない、申請情報（ステータスが「未承認」「承認」「解約」のものが対象）は、自動削除されます。
※自動発行されるアクセス ID のアクセス ID 名称は「（自動発行）」で固定となります。

■接続申請状況

CSVファイル出力　接続申請登録

		申請日時	部屋番号	利用者（メールアドレス）	利用開始	利用終了	アクセスID（有効回数）	
□		2017/05/24 19:15:44	gest room 02	gest B (gest_b@mail.com)			PWD43412 (--/--)	承認
承認		2017/05/24 19:14:31	gest room 01	gest A (gest_a@mail.com)			PWD35885 (00/--)	解除

接続申請削除

ステータス	以下、ステータスを表示 「未承認」、「承認」、「利用中」、「解約」 ※「未承認」「解約」は、申請削除のチェックボックスでの表示
更新ボタン	接続申請情報の更新画面に遷移します
申請日時	接続申請の日時を表示
部屋番号	接続申請時の部屋番号を表示
利用者	接続申請時の利用者名を表示
メールアドレス	接続申請時のメールアドレスを表示
利用開始	接続申請によって発行されたアクセス ID での認証日時を表示
利用終了	解約された日時を表示
アクセス ID	接続申請によって発行されたアクセス ID を表示
接続端末数	接続申請によって発行されたアクセス ID の接続可能（使用可能）な端末数を表示
承認ボタン	ステータス「未承認」（解約状態含む）を承認します。
解除ボタン	ステータス「承認」を解除します。
解約ボタン	ステータス「利用中」を解約します。

※登録されたメールアドレスに対してメール送信失敗した場合は「送信エラー」と表示されます

☐		2017/07/06 12:39:52	101	利用者A [redacted]			146129 (00/--)	送信 エラー

2)接続申請登録

■接続申請状況　(接続申請登録)

※は必須項目ですので必ず入力して下さい

部屋番号※	
利用者名※	
メールアドレス ※	
有効回数※	01 回

更 新

部屋番号	接続申請情報として、部屋情報を入力します。 ※基本設定-オプション設定の"接続ポート設定を使用する"が有効、かつ、自動発行設定の"接続ポート制限"がありの場合、接続ポートのリストからの選択となります。
利用者名	接続申請情報として、利用者情報を入力します。
メールアドレス	アクセス ID の通知先として、メールアドレスを入力します。
有効回数	利用者がアクセス ID を使用する回数を入力します。 ※自動発行設定で指定された有効端末数が「無制限」の場合、接続端末数も「無制限」となり、表示されません。

6－2. オプション設定

アクセス ID 自動発行機能のオプション設定をするための機能です。

■オプション設定

※は必須項目ですので必ず入力して下さい

アクセスID通知メールの署名	
申請内容の確認※	○確認する ◉確認しない(自動承認)
利用者による申請※	◉あり ○なし
申請情報の保持※	90日(初期値)

更 新

アクセス ID 通知メールの署名	アクセス ID 通知メールに、記載される署名を指定します。 ※署名は、通知メールの件名と本文に記載されます。
申請内容の確認	申請内容の確認する/確認しないを選択します。 (確認しない場合、自動で承認されます。)
利用者による申請	利用者による申請のなし／ありを選択します。 ※ありの場合、認証画面にて、申請画面へのリンクが表示されます
申請情報の保持	申請情報の保持期間を指定します。 ※指定された保持期間中に更新されない、申請情報 （ステータスが「未承認」「承認」「解約」のものが対象）は、自動削除されます。 ※申請情報の保持は以下より選択します。 90 日(初期値)、1 日、5 日、10 日、20 日、40 日

6－3. 自動発行設定

アクセス ID 自動発行機能のオプション設定をするための機能です。

■自動発行設定

※は必須項目ですので必ず入力して下さい

先頭コード※	PWD
有効期間 ※	◉接続時間指定 1 時間 0 分まで
	○時刻指定 00 時 00 分 ～ 00 時 00 分
	○期間指定 開始 2017 年 05 月 29 日 09 時 50 分 終了 -- 年 -- 月 -- 日 -- 時 -- 分
有効回数※	○無制限 ◉ 01 回

更 新

自動発行設定	先頭コード	アクセス ID の先頭コードを指定します。(3 桁まで指定が可能)

<table>
<tr><td rowspan="5"></td><td>接続ポート制限</td><td colspan="2">自動発行されるアクセス ID の接続ポート制限の有無を選択します。
「あり」の場合、アクセス ID は申請（接続申請）された接続ポートでのみ有効（使用可能）になります。
（″接続ポート設定を使用する″（「基本設定-オプション設定」）場合のみ表示）
※ 例として、客室 A でアクセス ID の申請をした場合、送られてきたアクセス ID は、客室 A では利用可能ですが、客室 B では利用ができません。</td></tr>
<tr><td rowspan="4">有効期間</td><td colspan="2">自動発行されるアクセス ID の接続した際の接続有効期間を指定します。</td></tr>
<tr><td>接続時間指定</td><td>接続開始からの時間で指定する場合、こちらを使用します。</td></tr>
<tr><td>時刻指定</td><td>毎日、定刻で設定したい場合、こちらを使用します。</td></tr>
<tr><td>期間指定</td><td>期間指定で設定したい場合、こちらを使用します。
期間指定で、終了時間を指定しない場合（終了の項目をすべて「--」で指定）接続時間は「無制限」となります。
期間指定の終了時間が過ぎた場合、当該アクセス ID は自動削除されます。</td></tr>
<tr><td>有効回数</td><td colspan="2">アクセス ID が有効（使用可能）な端末数を指定します。</td></tr>
</table>

6－4. 申請画面

申請画面のテンプレートの確認及び、カスタマイズを行うための機能です。

■申請画面

使用言語の選択	日本語　☑中国語　☑韓国語　☑英語	
テンプレートの確認	日本語のテンプレートを確認 パソコン） 申請(U_accessid_add_form)　確認(U_accessid_add_confirm)　完了(U_accessid_add_regist) エラー(U_accessid_add_mess) リマインダー(U_reminder_form)　確認(U_reminder_confirm)　完了(U_reminder_regist) エラー(U_reminder_mess) 携帯・スマートフォン） 申請(U_accessid_add_form)　確認(U_accessid_add_confirm)　完了(U_accessid_add_regist) エラー(U_accessid_add_mess) リマインダー(U_reminder_form)　確認(U_reminder_confirm)　完了(U_reminder_regist) エラー(U_reminder_mess)	
テンプレートの取得	ダウンロード	※申請画面テンプレートをダウンロードします。 注意事項） ・テンプレートは、tar.gz形式で圧縮されています。 ・テンプレートのディレクトリ構成は変更しないでください。
テンプレートの更新	参照...　ファイルが選択されていません。 アップロード	※申請画面テンプレートを更新します。 注意事項） ・テンプレートのディレクトリ構成は変更しないでください。 ・登録の際、テンプレートは、tar.gz形式で圧縮してください。 ・圧縮後のテンプレートのファイルサイズが 1000KB以上のものは登録できません。
テンプレートの初期化	初期化	※申請画面テンプレートを初期状態に戻します。

使用言語の選択	申請画面の言語を追加選択します。 ※ここで選択された言語の申請画面が、利用者ブラウザで表示切り替えの対象となります。また、選択された言語以外が利用者のブラウザで使用されたときは、選択言語に英語が含まれているときは英語のテンプレートが表示され、英語が含まれていない場合は日本語のテンプレートが表示されます。
テンプレートの確認	登録された申請画面テンプレートをプルダウンから選択し、プレビュー表示します。
テンプレートの取得	お客様独自のデザインに編集いただく際のベースとなる、申請画面テンプレートをダウンロードします。 ※テンプレートは、tar.gz 形式で圧縮されています。tar.gz が解凍可能なソフトを使い解凍した上で、編集してください。
テンプレートの更新	お客様独自デザインに編集した申請画面テンプレートを登録します。 ※テンプレートを編集する際は、既存ディレクトリ構成は変更しないでください。 （認証画面動作が正しく動作しなくなることがあります） ※テンプレートは、tar.gz 形式に圧縮してから登録してください。 ※登録可能なテンプレートサイズ（圧縮後）は、1000KB までとなります。

テンプレートの初期化	お客様の方で編集された申請画面が正しくないなど、認証画面が正しく動作しなくなるなどした場合、この機能を使い、元の状態に戻します。

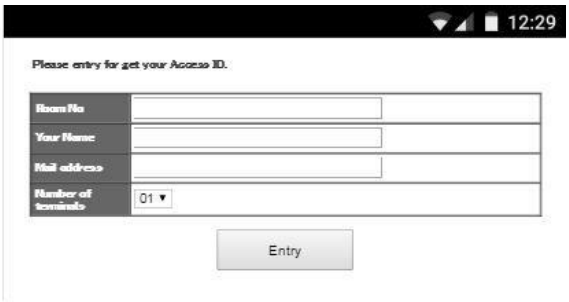
※各言語のデフォルトでのテンプレートは、下記の内容で表示されます。

・日本語

・中国語

・韓国語

・英語



申請画面テンプレートのカスタマイズ手順

1. 申請画面テンプレートをダウンロードする
   ※管理画面「メールアドレス認証-申請画面」の"テンプレートの取得"する

2. ダウンロードしたテンプレートを解凍する
3. テンプレートを編集
   編集対象）
   Custom/templates 配下の以下ファイル

   パソコン用
   申請(U_accessid_add_form.tpl.html)
   確認(U_accessid_add_confirm.tpl.html)
   完了(U_accessid_add_regist.tpl.html)

エラー(U_accessid_add_mess.tpl.html)

リマインダー(U_reminder_form.tpl.html)
確認(U_reminder_confirm.tpl.html)
完了(U_reminder_regist.tpl.html)
エラー(U_reminder_mess.tpl.html)

携帯・スマートフォン用
申請(U_accessid_add_form_s.tpl.html)
確認(U_accessid_add_confirm_s.tpl.html)
完了(U_accessid_add_regist_s.tpl.html)
エラー(U_accessid_add_mess_s.tpl.html)

リマインダー(U_reminder_form_s.tpl.html)
確認(U_reminder_confirm_s.tpl.html)
完了(U_reminder_regist_s.tpl.html)
エラー(U_reminder_mess_s.tpl.html)

※多言語対応する場合は、多言語用ファイルも編集する
（中国語：_china，韓国語：_korea，英語：_eng）

例）多言語用ファイル（中国語版）

パソコン用
申請(U_accessid_add_form_china.tpl.html)
確認(U_accessid_add_confirm_china.tpl.html)
完了(U_accessid_add_regist_china.tpl.html)
エラー(U_accessid_add_mess_china.tpl.html)

リマインダー(U_reminder_form_china.tpl.html)
確認(U_reminder_confirm_china.tpl.html)
完了(U_reminder_regist_china.tpl.html)
エラー(U_reminder_mess_china.tpl.html)

携帯・スマートフォン用
申請(U_accessid_add_form_china_s.tpl.html)
確認(U_accessid_add_confirm_china_s.tpl.html)

完了(U_accessid_add_regist_china_s.tpl.html)
エラー(U_accessid_add_mess_china_s.tpl.html)

リマインダー(U_reminder_form_china_s.tpl.html)
確認(U_reminder_confirm_china_s.tpl.html)
完了(U_reminder_regist_china_s.tpl.html)
エラー(U_reminder_mess_china_s.tpl.html)

編集の際の注意事項)
・テンプレートのディレクトリ構成を変更(追加含む)しないこと。
・テンプレートの文字コード(UTF-8)を変更しないこと。

・テンプレート内のシステムタグ(<!-- SYSTEM_BEGIN ・・-->、
<!-- SYSTEM_END ・・-->)で囲まれた部分に、申請画面動作に
必要なロジックが埋め込みされるので、削除・編集しないこと。
(以下記載の「カスタマイズの具体例」のケースを除く)

・申請画面データには、以下の形式のデータのみが登録可能
ーHTML ファイル (拡張子:html)
ースタイルシート(拡張子:css)
ー画像ファイル (拡張子:gif, jpg, jpeg, png)

※HTML ファイル、画像のリンクは、相対パスで指定してください。
ー同じ階層にあるものは、「./ファイル名」
ー下の階層にあるものは、「./フォルダ名/ファイル名」
ー上の階層にあるものは、「../ファイル名」

※スタイル指定や JavaScript などを、HTML ファイルに直接記述する際は、記述箇所を、
{literal}{/literal}で囲んでください。

4. テンプレートを tar.gz 形式で圧縮
5. 圧縮したテンプレートをアップロード
※管理画面「メールアドレス認証-申請画面」の"テンプレートの更新"する

6. 動作確認
以下、動作を確認する。

①更新したテンプレートで、申請画面が表示されることを確認
②申請が登録されることを確認
③更新したテンプレートで、リマインダー画面が表示されることを確認
④リマインダーにより、アクセス ID が再送されることを確認

申請画面テンプレートのカスタマイズの具体例

1)「部屋番号」を非表示にする場合

・部屋番号の SYSTEM タグ領域のフォーム項目(room_name)を領域の外に、hidden で記載し、適切な値(ここでは「-」)が渡るようにする。

```
<input type='hidden' name='room_name' value='-'>
```

・部屋番号の SYSTEM タグ領域(以下)を削除

```
<!-- SYSTEM_BEGIN @U_accessid_add_form_ROOM_NAME -->
<input type='text' name='room_name' size='30'>
<!-- SYSTEM_END @U_accessid_add_form_ROOM_NAME -->
```

2)「部屋番号」の項目名を変更する場合

・編集領域の項目名を変更

・JavaScript の入力チェックをおこなうようにする(*1)。

(*1)申請処理における入力チェックに引っかかると、元の項目名でエラーメッセージが表示されてしまいます。
このため、申請画面内で入力チェックをおこない、申請処理の入力チェックにかからないようにします。

第 4 章　コンソール機能

シリアル接続でコンソールメニューによる設定の初期化等をおこなうことができます。

必要なもの）
・シリアルケーブル（クロス）
・USB シリアル変換コネクタ※1

接続手順）
① SecurePOPCHAT／HyperPOPCHAT：USB シリアル変換コネクタを本装置の USB に接続
MicroPOPCHAT：本装置のコンソール用シリアルポートを利用可能
②USB シリアル変換コネクタ経由で、シリアル（クロス）に接続
③以下設定でターミナル接続
転送速度　　：38400
データ長　　：8
ストップビット：1
パリティ　　：なし
フロー制御　：XON/XOFF
④以下のアカウントでログインします。※2
コンソール用ユーザ：cnsusr
パスワード：12345

ログイン後の画面

※1　推奨アダプタ　UC-SGT1（エレコム製）、BSUSRC06（Buffalo 製）
※2　パスワードは管理画面の「基本設定」-「セキュリティ設定」の箇所で変更が可能です

0:Quit	コンソールメニューの終了
1:Network Configuration	ネットワーク設定を行います。 ※　選択すると確認メッセージが表示されますので「y」または「n」をキー入力し Enter を押します。「n」の場合はサブメニューに戻ります。「y」の場合は下記の処理を実行します。 ①ホスト名を登録します。（②-①へ進みます） ②-①WAN 側の接続が DHCP で接続するか選択します。 「y」の場合③のメニューへ進みます。また「n」の場合は②-②-①へ進みます。 ②-②-①WAN 側の IP アドレスとサブネットマスク、デフォルトゲートウェイを登録します

	(③へ進みます) ③LAN 側の IP アドレスとサブネットマスク及び、DNS を登録します(④へ進みます) ④確認メッセージが表示されますので「y」または「n」をキー入力し Enter を押します。「n」の場合はサブメニューに戻ります。「y」の場合は Enter により再起動が実行されて設定が反映されます。	
2:System Initialize	本製品を出荷時設定に戻します。ログや設定情報などの全てのデータが失われます。 ※ 選択すると確認メッセージが表示されますので「y」または「n」をキー入力し Enter を押します。「n」の場合はサブメニューに戻ります。「y」の場合は処理を実行します。	
3:System Shutdown/Reboot	機器の再起動及び、停止を行います	
	0:Cancel	サブメニューを閉じメインメニューに戻ります
	1:System Shutdown	終了処理を行い、電源も切ります。 ※ 電源ケーブル等を抜くときは、必ず本製品の電源が切れている事(正面にあるLED(青)が消灯していること)を確認してください。故障の原因になります。
	2:System Reboot	終了処理を行い、再起動します。

第 5 章 システムログ

本章では、システムログに出力されるログの内容について記載します

1. 状態監視ログ

以下の状態監視ログが出力されます。
－本装置の状態（セッション制限、帯域制限、スパム制限）
－登録された監視対象の死活監視

【セッション制限】
＞利用者のセッション数が「オプション設定-セッション制限」の″1 利用者あたりセッション数の上限″を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46 ALERT
2	監視項目	セッション	[Router] Session
3	状態	WARNING（閾値オーバー） CRITICAL（閾値オーバー） OK（状態復旧）	Session CRITICAL-セッション制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	該当端末のセッション数	閾値オーバーを検出した時点の該当端末が張っているセッション数（セッション数がしきい値以下になった場合は表示されません）	(649)
8	装置全体のセッション数	ログ出力時点の装置全体のセッション数（TCP および UDP の合計）	(715)
9	セッション制限の閾値	セッション制限の閾値（例では 1 利用者あたりセッション数の上限(1)：500、1 利用者あたりセッション数の上限(2)：750）	(limit 500-750s/1user)

※306 号室の端末で 649 セッション使用され、セッション制限がかかっている場合
Jun 10 15:48:46 ALERT: [Router] Session | Session CRITICAL - セッション制限中[306 号室/00:19:DB:00:00:40/192.168.1.199(649)] (715) (limit 500-750s/1user)

【スパム制限】

＞利用者のメール送信数が「オプション設定-スパム制限」の″1 利用者あたりメール送信の上限″を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40 ALERT
2	監視項目	スパムメール	spam mail
3	状態	WARNING（閾値オーバー） CRITICAL（閾値オーバー） OK（状態復旧）	Spam Mail CRITICAL - スパム制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	メール送信数	閾値オーバーを検出した時点に該当端末が送信したメール送信数（初回しか表示されません）	(101)
8	スパム制限の閾値	スパム制限の閾値（例では 1 利用者あたりのメール送信数の上限：10 通／1 分）	(limit 10mail/1user)

※306 号室で 101 通の送信を行ったのでスパム制限にかかっている場合。

Jun 10 16:09:40 ALERT: spam mail | Spam Mail CRITICAL - スパム制限中 [306 号室/00:19:DB:00:00:40/192.168.1.199(101)] (limit 10mail/1user)

【帯域制限】

＞利用者の帯域量が「オプション設定-帯域制限」の″1 利用者あたり帯域使用量の上限″を超えた場合、ログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40 ALERT
2	監視項目	トラフィック	[Net] Traffic
3	状態	CRITICAL（閾値オーバー） OK（状態復旧）	Traffic CRITICAL -帯域制限中
4	部屋番号	閾値オーバーを検出した部屋番号（部屋管理設定を行っていない場合は「（未検出）」と表示）	306 号室
5	MAC アドレス	閾値オーバーによって制限中の端末の MAC アドレス	00:19:DB:00:00:40
6	IP アドレス	閾値オーバーによって制限中の端末の IP アドレス	192.168.1.199
7	トラフック量	閾値オーバーを検出した時点に該当端末が送受信したトラフィック量	(97.47Mbps) TX 97472648bps, RX 1745448bps
8	トラフィック量の閾値	帯域制限の閾値（例では 1 利用者あたりのトラフィックの上限：10Mbps／1 分）	(limit 10Mbps/1user)

※306 号室で 97.47Mbps の送信を行ったので帯域制限にかかっている場合。

Jun 10 16:09:40 ALERT: [Net] Traffic | Traffic CRITICAL -帯域制限中[TX 306 号室/00:19:DB:00:00:40/192.168.1.199(97.47Mbps)] TX 97472648bps, RX 1745448bps (limit 10Mbps/1user)

【登録された監視対象の死活監視】

監視対象から ping 応答が正常に返らない場合、ログが出力されます。（独自ログフォーマット）

No	項目名	内容	例
1	日時	ログ出力日時	Jun 15 11:51:07 ALERT
2	監視項目	PING	[ping]
3	監視対象タイプ	監視設定で登録された監視対象タイプ（英数 5 文字まで）	SWHUB
4	監視対象 IP アドレス	監視設定で登録された監視対象の IP アドレス	192.168.1.250
5	状態	CRITICAL（疎通なし） OK（状態復旧）	CRITICAL - Host Unreachable (192.168.1.250)

※192.168.1.250 のスイッチ機器に対して PING 疎通がない場合。

Jun 15 11:51:07 ALERT: [ping] SWHUB 192.168.1.250 | CRITICAL - Host Unreachable (192.168.1.250)

2. DHCP ログ

本装置上で稼動している DHCP サービスのログが出力されます。

3. メールログ

本装置上で稼働している SMTP サーバのログが出力されます。
※「オプション設定-SMTP 代理送信」が有効（使用する）の場合のみ有効です。

4. 認証ログ

接続開始（認証）、接続終了（認証切断）に関するログが出力されます。（独自ログフォーマット）
※出力項目は、接続開始、接続終了とで異なります。

No	項目名	内容	接続開始	接続終了
1	日時	ログ出力日時	○	○
2	ログ送信元	0：POPCHAT ＜固定＞	○	○
3	ログ ID	認証ログ（開始／終了）の識別 ID	○	○
4	ログ区分	0：開始、1：終了	○	○
5	POPCHAT-ID	本装置の識別 ID	○	○
6	接続ポート	利用者端末が接続されたポート	○	－
7	接続ポートラベル	利用者端末が接続されたポートのラベル ＊接続ポート設定を行っていない場合は「（未検出）」	○	－
8	（未使用）	（未使用）	－	－
9	IP アドレス	利用者端末の IP アドレス	○	○
10	（未使用）	（未使用）	－	－
11	MAC アドレス	利用者端末の MAC アドレス	○	○
12	接続開始／終了	接続開始／終了した時間	○	○
13	認証方式区分	000：「フリー認証」による接続開始 001：「ベーシック認証」による接続開始 002：認証ローミングによる接続開始 003：「アクセス ID 認証」による接続開始 004：「@Cloud 認証」による接続開始（*1） 005：「Radius 認証」による接続開始 006：自動認証設定による接続開始	○	○
14	アクセス ID	「アクセス ID 認証」にて使用されたアクセス ID、または 「Radius 認証」にて使用されたアカウント	○	－
15	エリア属性区分	（未使用）	－	－
16	郵便番号	郵便番号	○	○
17	言語コード	利用者端末（ブラウザ）の言語設定	○	－
18	国コード	利用者端末（ブラウザ）の国設定	○	－
19	ユーザエージェント	ユーザエージェント情報	○	－
20	（未使用）	（未使用）	－	－
21	（未使用）	（未使用）	－	－
22	課金金額	課金金額	○	－

23	接続アドレス区分	0:Private 接続アドレス 1:Global 接続アドレス 2:(認証ローミングによるアドレス割当)	○	○
24	接続アドレス	利用者端末に割り当てられた接続アドレス	○	○
25	認証ドメイン ID	(未使用)	−	−
26	OpenID プロバイダ	(未使用)	−	−
27	性別区分	(未使用)	−	−
28	年齢区分	(未使用)	−	−
29	(未使用)	(未使用)	−	−
30	(未使用)	(未使用)	-	-

5. アクティブログ

接続開始(認証)、接続終了(認証切断)に関するログが出力されます。(独自ログフォーマット)
※認証ローミング、@クラウドオプション利用時のみ有効。
対象機能利用時、認証ログに追加して、認証中の端末で未接続状態が 15 分間続くと接続終了の記録がされ、認証中の再接続時には、接続開始の記録がされます。

No	項目名	内容	接続開始	接続終了
1	日時	ログ出力日時	○	○
2	ログ送信元	0:POPCHAT ＜固定＞	○	○
3	ログ ID	認証ログ(開始／終了)の識別 ID	○	○
4	アクティブログ ID	アクティブ接続ログ(開始／終了)の識別 ID	○	○
5	ログ区分	0:開始、1:終了	○	○
6	POPCHAT-ID	本装置の識別 ID	○	○
7	接続ポート	利用者端末が接続されたポート	○	−
8	接続ポートラベル	利用者端末が接続されたポートのラベル ＊接続ポート設定を行っていない場合は「(未検出)」	○	−
9	(未使用)	(未使用)	−	−
10	IP アドレス	利用者端末の IP アドレス	○	○
11	(未使用)	(未使用)	−	−
12	MAC アドレス	利用者端末の MAC アドレス	○	○
13	アクティブ接続開始／終了	アクティブ状態が開始／終了した時間 あるいは接続開始／終了した時間	○	○
14	アクティブ接続ステータス区分	ログ区分が 0:開始の場合 0:開始(通常) 1:開始(再開) 2:開始(ローミングによる再開) ログ区分が 1:終了の場合 0:終了(通常) 1:終了(タイムアウト) 2:終了(ローミングによる再開)	○	○
15	(未使用)	(未使用)	-	-

6. トラフィックログ

＞POPCHAT の帯域量のログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 16:09:40
2	トラフィック量(上り)	トラフィック量（上り）: Traffic TX ※単位　bps	TX 97472648bps
3	トラフィック量(下り)	トラフィック量（下り）: Traffic RX ※単位　bps	RX 1745448bps

※例

Jun 10 16:09:40 Traffic TX 97472648bps, RX 1745448bps

7. セッションログ

＞POPCHAT の全体のセッションのログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46
2	セッション数	セッション：Session	Session　715

※例

Jun 10 15:48:46 Session 715

【セッション制限】

＞利用者のセッション数が「オプション設定−セッション制限」の″1　利用者あたりセッション数の上限″を超えた場合、ログが出力されます（独自ログフォーマット）。

8. アクティブユーザ

＞POPCHAT に接続中の利用者数のログが出力されます（独自ログフォーマット）。

No	項目名	内容	例
1	日時	ログ出力日時	Jun 10 15:48:46
2	アクティブユーザ数	アクティブユーザ数：ActiveUser	ActiveUser 15

※例

Jun 10 15:48:46 ActiveUser 15

9. パケット転送ログ （オプション）

＞ パケット転送の際にシスログサーバに記録されるログ(POPCHAT 本体には保存されません)
※例　ホスト名「auth」の POPCHAT より 9 月 2 日 10 時 44 分に IP アドレス「192.168.1.1」の端末から「203.0.113.1」のサイトへ HTTP で通信をしたとき。

Sep　2 10:44:05 auth kernel: [173283.975040] [PACKET]IN=br0 OUT=eth0 PHYSIN=eth1 SRC=192.168.1.1 DST=203.0.113.1 LEN=1434 TOS=0x00 PREC=0x00 TTL=63 ID=58421 DF PROTO=TCP SPT=45934 DPT=80 WINDOW=1222 RES=0x00 ACK URGP=0

第 6 章 トラブルシューティング

本章では、基本的なトラブルシュートを記しますが、改善が見られないときは速やかに本製品を購入された販売代理店にご相談ください。

1. 起動しない

a. 本製品と電源ケーブル及びアダプタが正しく接続されている事をお確かめください。
b. 電源ケーブルが電源コンセントに接続されている事をお確かめください。
c. 電源ボタンを押し、電源 LED（青）が、点灯する事をお確かめください。

2. 管理 PC にログイン画面が表示されない

a WAN側、LAN側ポートのコネクタに正しいLANケーブルが接続されている事をお確かめください。
b URLアドレスを正しく入力されているかお確かめください。
LAN 側からの接続する際の設定前（工場出荷時）の URL は「http://192.168.1.254:888」ですが、設定後は「192.168.1.254」を設定後のLAN側アドレスに置き換えて入力してください。
c 管理 PC のネットワークが正しく設定されている事をお確かめください。
固定 IP アドレス付与の場合、IPアドレスはLAN側アドレスと同じネットワークセグメントでなければなりません。
d DHCP の場合は、正しくIPアドレスが取得できているかお確かめください。
Windows の場合はコマンドプロンプトで「ipconfig」と入力し実行（Enter）すれば確認できます。不正なアドレスの場合は管理PCを再起動して再度確認してください。

3. 管理画面でログインできない

a 大文字小文字など間違いがないか ID、パスワードを再度入力してください。
なおパスワードが分からなくなった場合は、サポートにてパスワードを初期化するか、工場出荷時に戻さないとログインができなくなります。

4. インターネットに接続できない

a 利用者端末をネットワークに接続後、認証するまではインターネット側に出ることはできません。認証処理が完了しているかご確認ください。

5. 利用者端末に認証画面が表示されない

a 利用者端末に、本製品では利用できない設定がないかお確かめください。
この場合、DHCP でのアドレス取得に変更するなどの処置が必要です。
・認証画面を表示しない設定になっている場合
・利用者端末のデフォルトゲートウェイ又は DNS サーバの IP アドレスが空欄の場合
・IPアドレスが他の端末や本装置のアドレスと重複している場合
・利用者端末に本装置の LAN 側ネットワークと同一セグメントのアドレスが設定されており、デフォルトゲートウェイが POPCHAT の LAN 側アドレスに設定されていない場合（同一セグメントの場合はプラグ＆プレイが働きません）
・手動プロキシ設定で本製品に設定していないポート番号が使われている場合
・プロキシサーバのアドレス設定が IP アドレスではなく、ホスト名（xxx.yyy.co.jp 等）で設定されている場合

b 利用者の端末が DHCP 設定で、正しいアドレスが取得できていない。
一度、利用者端末を再起動してお確かめください。また、ファイアウォールまたはウィルス対策ソフトの影響で取得できない場合があります。

c ダイヤルアップ接続や外部の無線アクセスポイントに接続されていないかご確認ください。

d ブラウザを起動し、http://www.yahoo.co.jp 等のインターネット上のホームページに一度アクセスして下さい。

e お使いのOSやアプリケーションにより、DHCP によるアドレスの自動取得ができない場合があります。この場合、固定アドレス設定により接続を試みてください。

f 配線及び機器等、物理的な導通に問題ないかご確認ください。

g 認証解除後、約1分間は認証画面が表示されない仕様となります。

6. 利用者端末で認証は出来るがインターネットアクセスができない。

a 本製品の管理メニューのステータス表示でネットワーク情報をご確認ください。

b 管理PCや、他の端末でインターネットアクセスができているかお確かめください。
もし、同じようにインターネットアクセスができないのであれば、本製品のインターフェースのWAN側設定をご確認ください。

c 上位側配線、機器、回線等に問題や、工事の為の一時停止等がないかご確認ください。

7. メールの送受信ができない

a メールの送信ができない場合は、以下のことが考えられます。
・メール送信先のアドレスが間違っていないか確認してください。
・メールサーバの設定が何も設定されていない場合は送信できません。これまでメール送信ができた状態の端末からのみメール送信が可能です。
・プロバイダで「Outbound Port 25 Block」によるメール送信制限が行われていないか確認してください。

b メールの受信ができない場合は、以下のことが考えられます。
・メール受信サーバのアドレスが間違っていないか確認して下さい。
・設定しているメール受信サーバが、外部ネットワークからの接続を許可していない場合があります。（主に企業のイントラネットやCATVネットワークが該当します）

その他、POPCHAT シリーズに関する情報は、「http://popchat.jp」にて公開しております。

本製品の保証期間はご購入より 1 年です。
修理の依頼は購入頂いた販売店にご相談ください。

ご購入後 1 年以上経過した製品の修理、技術サポートは有償となります。
安心のための保守契約もございますので、詳しくは購入頂いた販売店にご相談ください。

第 7 章　仕様

MicroPOPCHATⅢ

チップセット System Chipset list:

Intel Bay trail-I　E3825　チップセット

LAN

Gigabit Ethernet Controller LANx2

電源容量 :

9.5W

インターフェース:

LAN ポート×2

シリアルポート(RS232 pin header)×1

USB2.0　×2(使用不可)

VGA ポート　×1(使用不可)**寸法:**

145(W) x 89.3(D) x　※35(H)mm

※ゴム足装着時 39mm,

重量:

0.7Kg

動作温度

0-50℃

動作湿度

5-95%(結露なきこと)

設定上限

セッション数:16000

(Extend ライセンス時:24000)

最大認証数:250

DHCP 割当 IP アドレス数:500

(Extend ライセンス時:750)

部屋管理数(接続ポート設定数):100

(Extend ライセンス時:150)

アクセス ID 登録数:500

(Extend ライセンス時:750)

自動認証の MAC アドレス登録数:100

セキュリティ設定(許可アドレス)数:100

ポート転送設定数:100

フィルタリング設定数:100

SecurePOPCHATⅢ

チップセット System Chipset list:

Intel® C226 チップセット

LAN

Onboard Intel® Gigabit Ethernet Controller LAN × 2

電源容量 :

76W

平均電力消費量 34W

インターフェース:

USB ポート×2

LAN ポート×2

VGA 端子×1

PS2 x 1

Serial(使用不可) x 1

寸法 Dimension:

200(W) x 350(D) x 45(H)mm

重量 Weight:

3Kg

動作温度

0-35℃

動作湿度

10-90%(結露なきこと)

設定上限

セッション数:32000

(Extend ライセンス時:48000)

最大認証数:500

(Extend ライセンス時:750)

DHCP 割当 IP アドレス数:1000

(Extend ライセンス時:1500)

部屋管理数(接続ポート設定数):250

(Extend ライセンス時:375)

アクセス ID 登録数:1000

(Extend ライセンス時:1500)

自動認証の MAC アドレス登録数:100

セキュリティ設定(許可アドレス)数:100

ポート転送設定数:100

フィルタリング設定数:100

HyperPOPCHATⅢ

チップセット System Chipset list:

Intel® C226 チップセット

LAN

Onboard Intel® Gigabit Ethernet Controller LAN × 2

電源容量 :

77W

平均電力消費量 35W

インターフェース:

USB ポート×2

LAN ポート×2

VGA 端子×1

PS2 x 1

Serial(使用不可) x 1

寸法 Dimension:

200(W) x 350(D) x 45(H)mm

重量 Weight:

3Kg

動作温度

0-35℃

動作湿度

10-90%(結露なきこと)

設定上限

セッション数:65000

最大認証数:1000

(Extend ライセンス時:1500)

DHCP 割当 IP アドレス数:2000

(Extend ライセンス時:3000)

部屋管理数(接続ポート設定数):500

(Extend ライセンス時:750)

アクセス ID 登録数:2000

(Extend ライセンス時:3000)

自動認証の MAC アドレス登録数:100

セキュリティ設定(許可アドレス)数:100

ポート転送設定数:100

フィルタリング設定数:100

■付録）認証画面：エラーメッセージについて

1）認証画面表示の際のメッセージ

・「お使いの端末からの通信が上限セッション数を超えたため、一時的に接続を制限させていただいております。」
⇒　利用者端末がセッション制限にかかっている場合に表示されます。

・「認証可能な端末の上限（XXXX）を超えています」
⇒　認証数が、最大接続数（最大認証数）を超えている場合に表示されます。

2）認証処理の際のメッセージ

・「処理が集中しています。しばらくしてから実行ください。」
⇒　複数の利用者端末から同時に認証された場合など、認証処理が重なった場合に表示されます。
　※POPCHAT 内部の認証制御処理と重なった場合も同様のメッセージとなります。

・「ERROR: (AUTH_NOROOM)」
⇒　接続ポートのポート検出をおこなう設定において、利用者端末が接続されたポートが POPCHAT に登録されていない場合やポート検出に失敗した場合に表示されます。

・「アクセス ID が正しくありません。」
⇒　認証方式：アクセス ID 認証において、入力されたアクセス ID が有効でない場合に表示されます。

・「有効な接続期間ではありません。」
⇒　接続時間（期間）外で、認証しようとした場合に表示されます。
　※POPCHAT の時刻がずれている際にも表示される場合があります。

・「お使いの端末の IP アドレスはすでに使用されています。IP アドレスを再設定（DHCP リースを更新）してください。」
⇒　利用者端末の IP アドレスが、他の利用者端末に割り当て済の場合に表示されます。

・「ID/パスワードが正しくありません。」
⇒　認証方式：Radius 認証において、入力された ID/PWD が有効でない場合に表示されます。

・「認証処理エラー（NETWORK）」

⇒　Radius 認証サーバへの問合せにて応答が返ってこない場合に表示されます。

・「只今、インターネットに接続できません。」

⇒　上位回線が指定 IP アドレスとの通信断を検知した際に表示されます。