Biz メール＆ウェブ プレミアムr3

管理者マニュアル

第 1.19.0 版
2026/2/16

NTTドコモビジネス株式会社

この度は「Biz メール＆ウェブ プレミアム」を ご契約いただき、ありがとうございます。

本書は、「Biz メール&ウェブ プレミアム」の『管理設定』『データベースやアクセス解析』等の機能について、必要事項・重要事項等をご説明しています。
快適にご運用いただく為に、ご利用開始前に必ずお読みください。

本書では「Biz メール＆ウェブ プレミアム」を全て「本サービス」と表記しています。
本サービスではお客さまのサーバー運用において、トラブルなく円滑にご利用いただく為に、様々なツールや情報を提供しておりますが、ご利用前に、あらかじめ設定していただく必要があります。
※ 設定漏れ等ないよう、ご注意ください。

本サービスの仕様変更により、本書の内容とサービスが一致しない場合がありますので、ご了承ください。

表示やマークについて

サーバーを利用する契約者、または利用者が損害を受ける可能性のある事や、サーバーが利用不可となる可能性があることを、回避法とともに記載しています。

警告	必読となります。未確認の場合、損害を負う可能性があります。
注意	ご確認をお願いいたします。未確認の場合、一時的にサービスを利用できない等の不都合が生じる可能性があります。

禁止行為は禁止マークが入っています。

	禁止事項を示しています。

その他の表示

アドバイス	知っておくと便利なこと 知っておいていただきたいこと

本書および本書以外のマニュアルについて

マニュアル名	用途・目的
セットアップマニュアル	Biz メール&ウェブ プレミアム の 初期設定に関する、**管理者向けマニュアル**です。 ■管理者の初期設定、IP アクセス制限（簡易） ■ドメインの設定、ウェブメールの初期設定 ■ユーザーの登録（新規/変更/削除） ■ホームページのディレクトリ構成、ファイル作成、公開手順 ■DNS サーバーの変更・登録申請、サーバー情報等 ■運用開始時の確認事項 ■ご契約内容の変更方法、ユーザーサポート、工事故障情報通知
管理者マニュアル	Biz メール&ウェブ プレミアム をご利用いただく上での詳細な設定に関する、**管理者向けマニュアル**です。 ※詳細は本書の「目次」をご参照ください。
利用者マニュアル	Biz メール&ウェブ プレミアム のユーザーが個別に行う設定について記載しています。 ■コントロールパネルの基本操作、パスワード変更 ■メール関連（受信設定：転送、自動返信、個別ルール） ■ファイルマネージャ―の使い方、共有ファイル、復元ファイル ■Web サイト機能関連（ディレクトリ構成、FTP 設定）
メール設定マニュアル	Biz メール&ウェブ でメールソフトを使用する場合に **管理者が行う事前確認および注意事項** と **ユーザー個別に行うメールソフトの設定** について記載しています。 ■新規利用の場合のメールご利用までの流れ・DNS 情報の設定について ■他サービスから移行した場合のメールご利用までの流れ・DNS 情報の設定について ■メールセキュリティをご利用の場合の注意事項 ■メールソフトに関する注意事項 ■メールソフトの設定
Active!mail 利用マニュアル	Biz メール&ウェブで Active! mail を利用するユーザーが個別に行う設定 について記載しています。 ■ウェブメール機能（Active!mail） の設定/利用方法
<オプションサービス> メール監査アーカイブ 設定マニュアル	メール監査アーカイブ（オプションサービス）の コントロールパネルや機能に関する、**管理者向けマニュアル**です。 ■メール監査アーカイブの概要 ■セットアップ手順 ■各種コントロールパネルの概要 ■主管理者・副管理者の登録と権限 ■送受信メールの全文保存設定 ■登録済みフィルタールール確認 ■送受信ルールの設定 ■メール管理の機能と操作方法 ■レポート閲覧方法 ■送受信ルール関連（作成・編集・削除など） ■通知メッセージ、サンプル/例（フィルタールール、通知メッセージ、SPF レコード）
<オプションサービス> 迷惑メールフィルタリング /ウイルスチェック 管理者マニュアル	オプションサービスの管理者用コントロールパネル や 機能に関する、**管理者向けマニュアル**です。 ■迷惑メールフィルタリング機能概要 ■セットアップの手順 ■管理者用コントロールパネルについて、管理者アカウント管理（ID とパスワード） ■IP アドレス制限の強制解除方法 ■フィルタリングの仕様（迷惑メール/SPF の判定・度合い付与、フィルタ処理順位など） ■ウィルスチェック機能概要、警告メール関連

<オプションサービス> 迷惑メールフィルタリング ドメイン管理者マニュアル	迷惑メールフィルタリング（オプションサービス）の コントロールパネルで行う詳細設定 に関する、**ドメイン管理者向けマニュアル**です。 ■操作概要（ドメイン全体/ドメインで管理しているアカウント個別の操作） ■アカウント管理（追加、編集、削除など…） ■隔離メール関連（検索、許可リスト登録、転送、フィードバック、削除など） ■迷惑メール受信状況レポート、誤判定メールフィードバック ■ソース IP 制限、アドレスフィルタ設定 ■ドメイン管理者のパスワード変更
<オプションサービス> 迷惑メールフィルタリング 利用者マニュアル	迷惑メールフィルタリング（オプションサービス）を利用するユーザーが個別に行う設定について記載しています。 ■隔離メール関連（検索、許可リスト登録、転送、フィードバック、削除など） ■誤判定メールフィードバック ■アカウント設定、パスワード変更 ■アドレスフィルタ設定、フィルタリングルールのエクスポート/インポート

目次とページリンクについて

本書では、目次・文中のページ誘導をクリックすると、該当ページをすぐに表示することができます。各ページから目次に戻る場合は、ページ右上の矢印マークをクリックします。

目次

MEMO

1　コントロールパネルの機能

1.1. コントロールパネルへのログイン

ここでは、コントロールパネルにログインする手順をご説明します。
メールでご案内しております、「ご利用内容のご案内」をお手元にご準備のうえ、設定を行ってください。

1）「ご利用内容のご案内」に記載されている、コントロールパネルの URL にアクセスします。

> **◆ コントロールパネルの URL**
>
> https://bizmw-login.com/ユーザ ID(管理者)/login

※ ユーザ ID(管理者) は、「ご利用内容のご案内」に記載されています。

<例>［ユーザ ID(管理者)］が「*biz123*」の場合、
コントロールパネルの URL は https://bizmw-login.com/*biz123*/login となります。

2）ログイン画面で、ID とパスワードを入力して［ログイン］をクリックします。

◆ **管理者でログインする場合**
「ご利用内容のご案内」に記載されている「ユーザ ID(管理者用) ／ユーザパスワード」を入力します。

◆ **利用者でログインする場合**
管理者が作成した「ユーザ ID(利用者用) ／パスワード」を入力します。

※ 利用者の作成方法は、『セットアップマニュアル』をご参照ください。

1.2. 管理者コントロールパネルの機能概要

ここでは、管理者でログインした際のコントロールパネルの機能概要をご案内します。
※ ログインするユーザーが「管理者」と「利用者」とでは表示される機能が異なります。

［1］ホーム画面の表示

- サーバー基本情報：ご利用サーバーの基本情報が表示されます
- リソース契約情報：CPU/メモリとディスク容量の追加状況が表示されます
- リソース使用状況：リソース負荷状況とディスク使用状況を確認できます。

  ※ ［リソース負荷状況］から、サーバーの CPU やメモリ使用量、負荷状況を確認できます。
  詳細は、本書 5.5 リソース負荷状況の確認 をご参照ください。

  ※ ［ディスク使用量詳細］から、以下のデータの数値を確認できます。
  ・メールデータ
  ・ウェブデータ
  ・アプリケーション
  ・システム
  ・空き容量
  詳細は、本書 5.6 ディスク使用量の確認 をご参照ください。

- お知らせ：サポートサイトに掲載された「お知らせ」へのリンクが表示されます
- 工事・故障情報：サポートサイトに掲載された「工事・故障情報」へのリンクが表示されます

［2］上部メニュー

- ホーム：クリックするとホーム画面に遷移します
- メール：

○ ウェブメール：Active!mail ログイン画面へのリンクが表示されます

・ お客さまのドメインで Active!mail をご利用いただく場合は、初期設定が必要です。詳細は、4.1.4 ウェブメールの初期設定について｜セットアップマニュアルをご参照ください。

・ Active!mail のご利用法方については「Active!mail 利用マニュアル」をご参照ください。

○ 迷惑メールフィルタリング設定*1：
迷惑メールフィルタリングコントロールパネルのログイン画面へのリンクが表示されます。

迷惑メールフィルタリングコントロールパネルの詳細は「迷惑メールフィルタリング ドメイン管理者マニュアル」をご参照ください。

*1 別途オプションサービス（有料）のお申し込みが必要です。
迷惑メールフィルタリング｜Biz メール&ウェブ プレミアム

○ メール受信設定：
管理者（管理者 ID@お客さまドメイン）宛のメールに対して以下の設定が可能です。

・一括転送（転送先は 4 つまで）
・一括自動返信、自動返信文の設定
・個別ルール設定

詳細は以下をご参照ください。
3.3 メール受信設定(転送/自動返信/個別ルール)｜利用者マニュアル
複数の宛先へメールを転送したい｜よくあるご質問

- ファイル：クリックするとファイルマネージャに遷移します。
詳細は以下をご参照ください。
4.2 ファイルマネージャの使い方｜利用者マニュアル
4.3 共有ファイル｜利用者マニュアル
4.4 復元ファイル｜利用者マニュアル

［3］左メニュー

- ドメイン：以下の操作が可能です。
  - ・ドメインのサーバーへの登録/削除
  - ・ドメインごとのウェブサーバー設定（ドメイン名のエイリアス設定）
  - ・ドメインごとのメールサーバー設定（受信サーバー設定）*2

  詳細は 4.1 ドメインの設定｜セットアップマニュアルをご参照ください。

  *2　外部のメールサーバーを利用する場合に、Biz メール&ウェブのサーバーでメールを受信しないようにする設定です。詳細は、本書 2.5 受信サーバー設定をご参照ください。

- ユーザー：ユーザーの作成・削除・設定変更ができます。

  詳細は「 4.3 ユーザー設定｜セットアップマニュアル」をご参照ください。

- メールサーバー：以下の設定が可能です。
  - ・メールアドレス
  - ・メーリングリスト
  - ・送信ドメイン認証
  - ・迷惑メールフィルタリング*3
  - ・ウェブメール*4
  - ・メール分析

  詳細は、本書「2.メールサーバー」をご参照ください。

  *3　クリックすると以下が表示されます。
  - ・ホスティングオプションサービス管理者用コントロールパネルへのリンク
  - ・オプションサービス管理外メールの受信制限

  詳細は「迷惑メールフィルタリング・ウイルスチェック管理者マニュアル」をご参照ください。
  この機能は、別途オプションサービス（有料）のお申し込みが必要です。
  ウィルスチェック｜Biz メール&ウェブ プレミアム
  迷惑メールフィルタリング｜Biz メール&ウェブ プレミアム

  *4　クリックすると、ウェブメール（Active! mail）管理者ログイン画面へのリンクが表示されます。
  詳細は 4.1.4 ウェブメールの初期設定について｜セットアップマニュアルをご参照ください。

- ウェブサーバー：以下の設定が可能です
  - ・SSL/TLS 証明書
  - ・サイトアクセス制限
  - ・サイト編集権限
  - ・サイトバックアップ
  - ・WAF*5
  - ・ウェブサイト分析

  詳細は、本書「3.　ウェブサーバー」をご参照ください。

*5 WAF は、別途オプションサービス（有料）のお申し込みが必要です。
WAF｜Biz メール&ウェブ プレミアム

- アプリケーション：以下の操作が可能です。
  - ・WebDAV 共有フォルダの作成、編集、削除
  - ・PHP のバージョン切り替え
  - ・WordPress、Matomo、pukiwiki のインストール
  - ・MySQL、phpMyadmin 等の有効/無効およびバージョン切り替え

  詳細は、本書「4.アプリケーション」をご参照ください。

- システム：以下の設定が可能です。
  - ・定期実行タスク
  - ・IP アクセス制限
  - ・ファイルバックアップ

  詳細は、本書「5.システム」をご参照ください。

- 管理者サポート：
  オンラインマニュアル、よくあるご質問、お問い合わせ、各種お手続き へ遷移できます。

1.3. 二要素認証設定

1.3.1. 二要素認証の概要

管理者・ドメイン管理者および一般ユーザーがコントロールパネルへログインする際に、通常のパスワードとは別のパスワード（ワンタイムパスワード）による二重の認証を行う仕組みです。パスワードの流出等が発生した場合に、不正にコントロールパネルへのログインを防ぐことが出来ます。

二要素認証のクライアントアプリについて

本サービスのコントロールパネルの二要素認証は、一般的な多要素認証の仕組みを用いているため、Google Authenticator, Authy のような一般的な二要素認証アプリやウェブブラウザの拡張機能をご利用いただけます。

本マニュアルでは、動作確認済みのアプリ「Twilio Authy（Authy）」の初期設定についてご案内しています。

※ アプリのバージョンによって、表示される画面が当マニュアル内の画像と異なる場合があります。

アプリの詳細な利用方法等については、以下の公式サイトをご参照ください。

■ **Authy - Twilio Help Center**
https://help.twilio.com/categories/19752372315419

※ 「Twilio Authy（Authy）」のデスクトップ版は、2024 年 3 月 19 日に提供元でのサポートが終了（EOL）となります。

注意

コントロールパネルに二要素認証を設定した状態で以下を行った場合、コントロールパネルにログインできなくなりますので、ご注意ください。

- クライアントアプリを設定した端末の紛失・交換
- クライアントアプリの削除
- クライアントアプリに設定した認証アカウントの削除

1.3.2. 二要素認証を有効にする

1） 二要素認証の設定をする［ユーザーID］と［パスワード］で、コントロールパネルにログインします。

- ログイン方法は「1.1 コントロールパネルへのログイン」を参照してください。

2） 画面右上の「ユーザーID ボタン」のプルダウンから［二要素認証］をクリックします。

3） 「二要素認証設定」画面に、QR コード等、設定に必要な情報が表示されます。

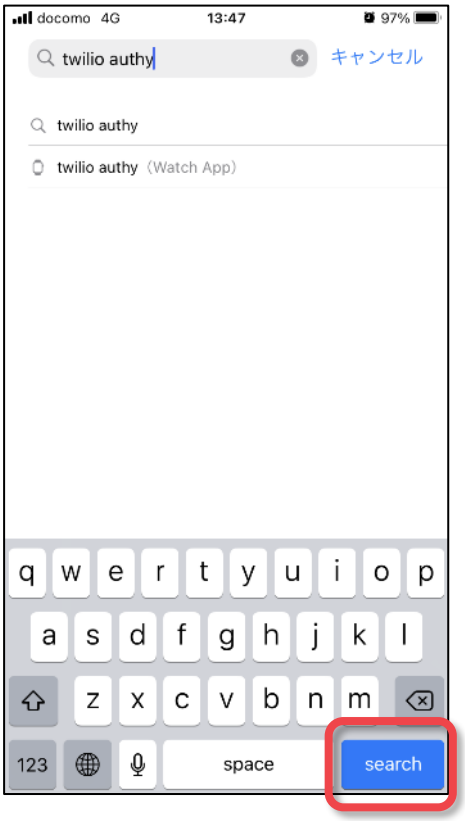
続けてクライアントアプリの設定に移ります。

1.3.3. クライアントアプリのインストール(iPhone)

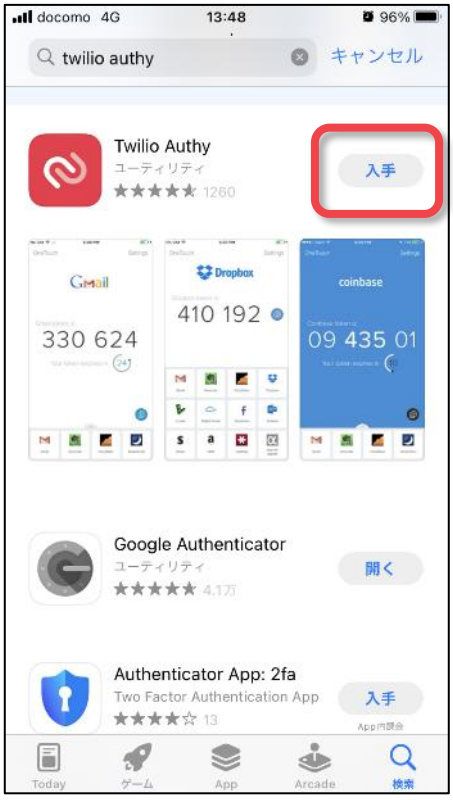
1） App Store を起動して、［検索］をタップします。

2） 検索欄に「twilio authy」と入力します。

3）　右下の［Search］をタップします。



4）　検索結果が表示されたら、［入手］をタップします。



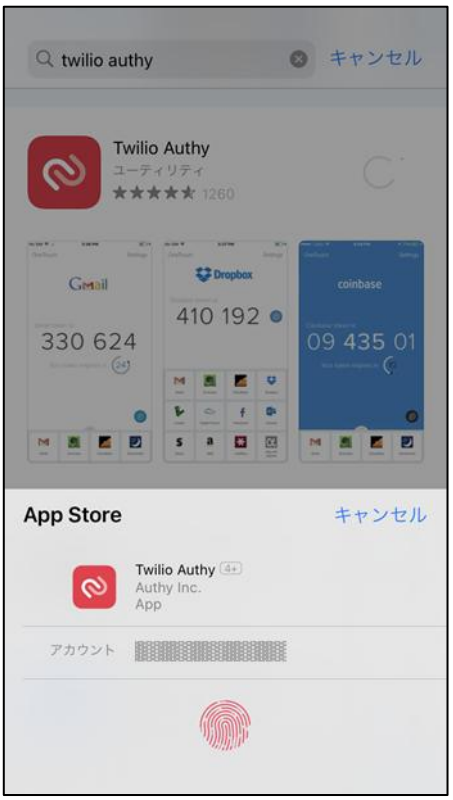
注意

アイコンおよび名称は、提供元により変更される場合があります。
見つからない場合はサポート窓口までお問い合わせください。

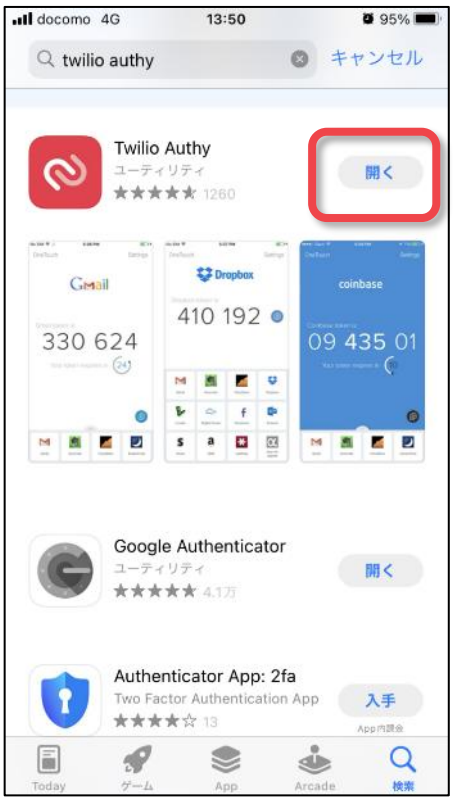
5）　アプリをインストールするための認証を行います。

※ 右図は Touch ID（指紋認証）の例です。

※ 認証を設定していない場合は
［インストール］をタップしてください。

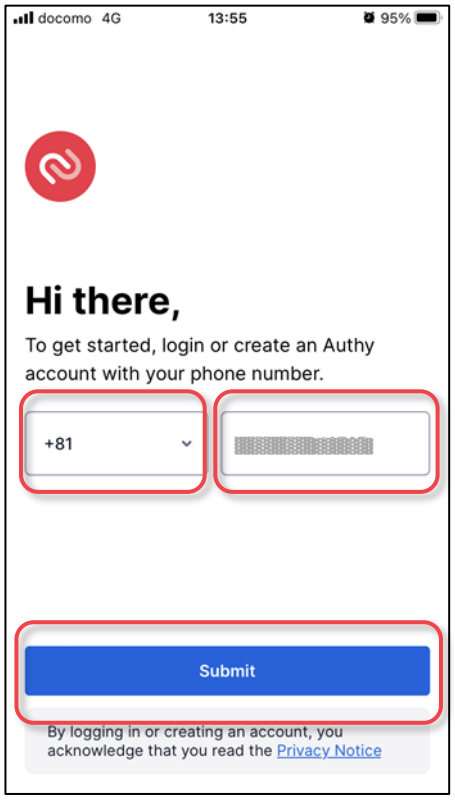


6）　インストールが完了したら、［開く］をタップします。

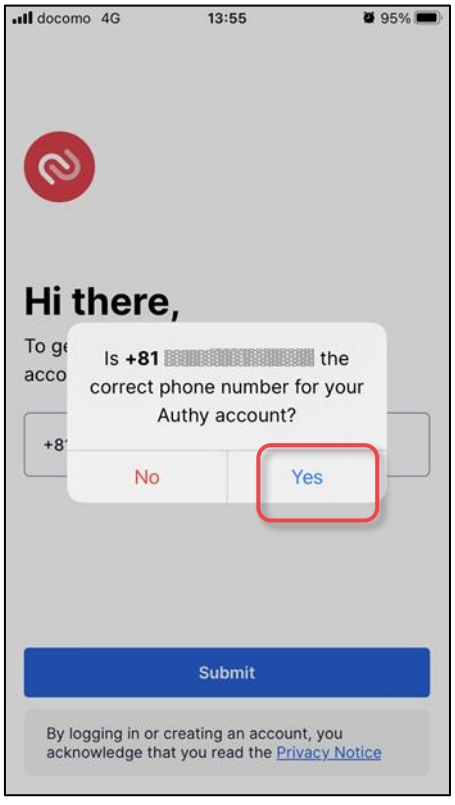


7）　セットアップ画面が開いたら、
［Country Code］と［Phone number］を入力し、
［Submit］をタップします。

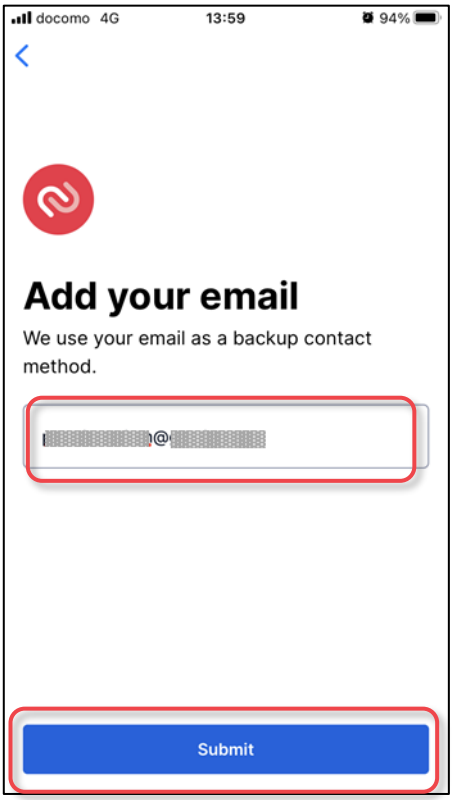
- ［Country Code］：日本国際電話コード「+81」を選択
- ［Phone number］：携帯電話の番号
  ※　電話番号を入力する際は、先頭の「0」を省略します。
  例)「090-1234-5678」の場合は「9012345678」



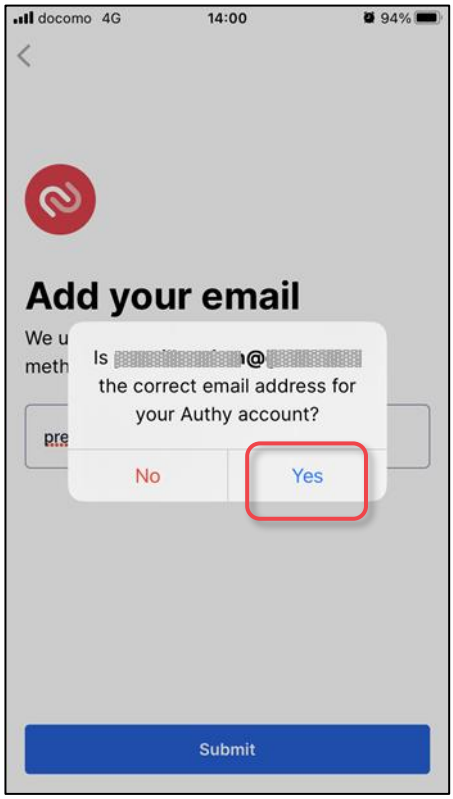
8）　入力した電話番号を確認するポップアップが表示されます。間違いがないことを確認のうえ、［Yes］をタップしてください。



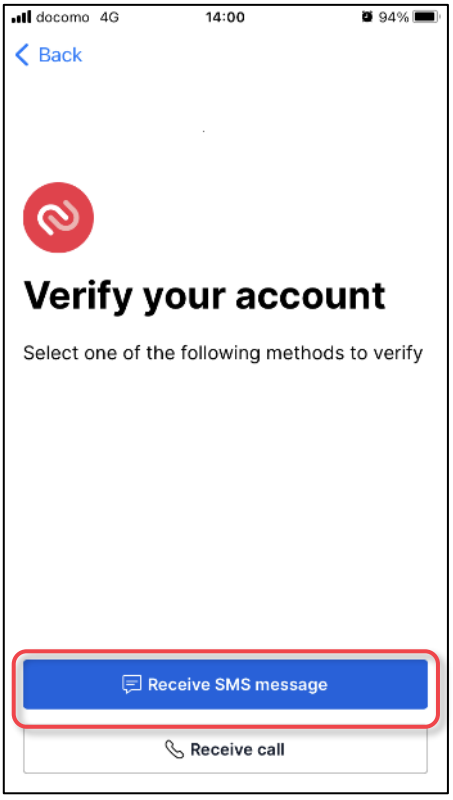
9）　［Email Adress］に、お客さまのメールアドレスを入力し、[Submit] をタップします。



１０）　入力したメールアドレスを確認するポップアップが表示されます。間違いがないことを確認のうえ、［Yes］をタップしてください。



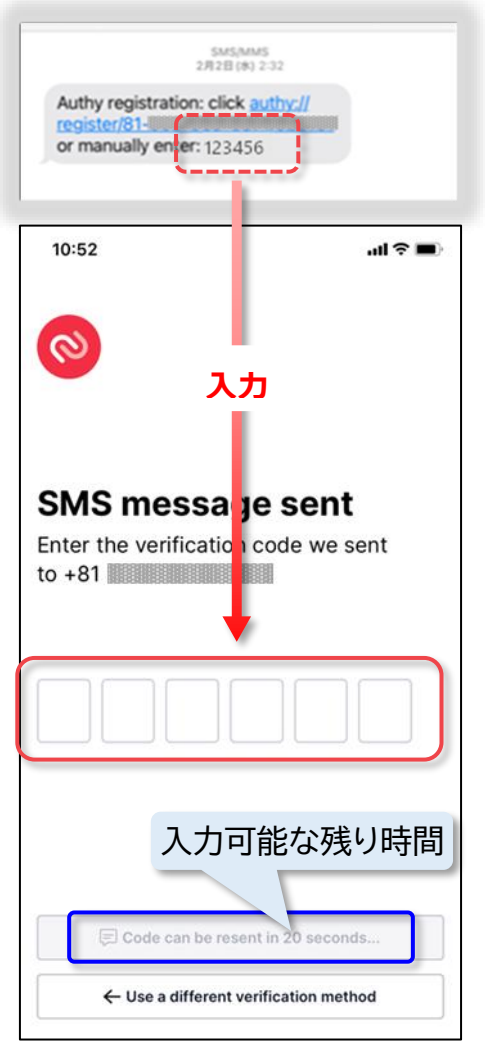
１１）　「SMS(ショートメッセージ)認証」か「電話認証」かを選択する画面が開きます。（当マニュアルでは「SMS認証」を例にご説明します）［Receive SMS Message］をクリックしてください。



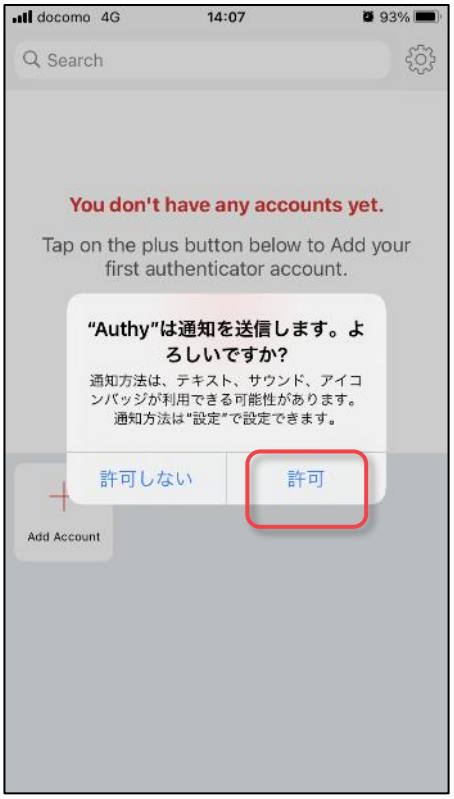
１２）　SMS に記載されている「6 桁の認証番号」を入力してください。

※　入力の有効時間は 30 秒程です。残り時間は［Code can be resent in ** seconds...］の箇所に表示されます。

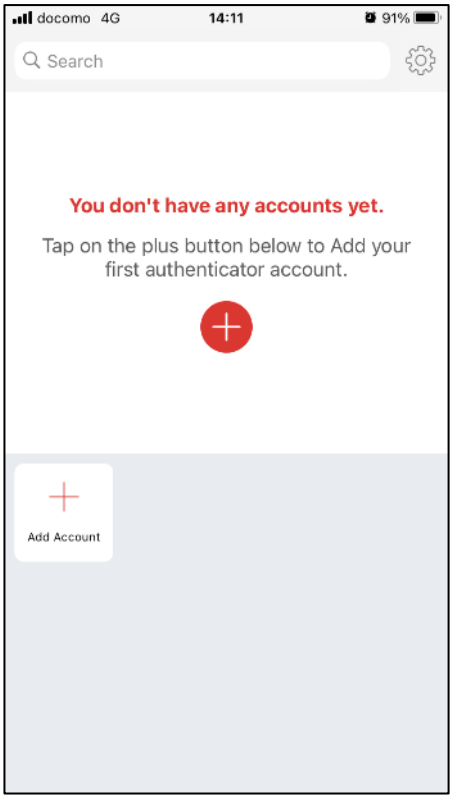
※　6 桁の数字を入力すると自動的に認証が開始されます。



１３） 通知の許可を確認するポップアップが表示されたら、[許可]をタップしてください。

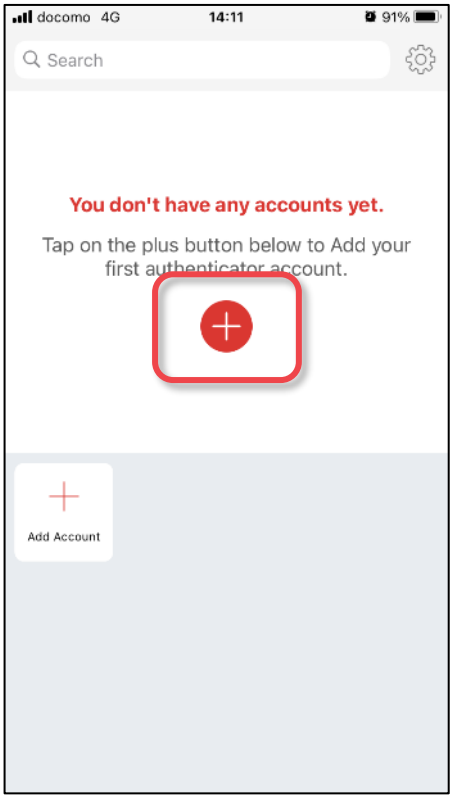


１４） 下図の画面が表示されたら、次は、**二要素認証を有効化**します。

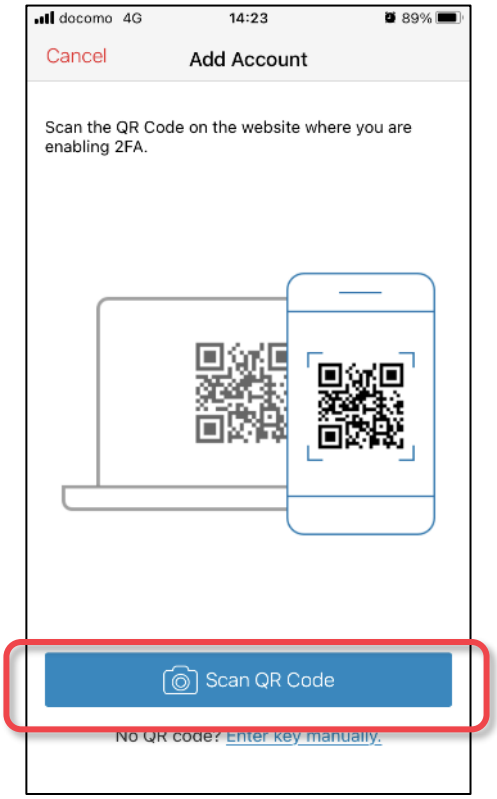


1.3.4. 二要素認証の有効化(iPhone)

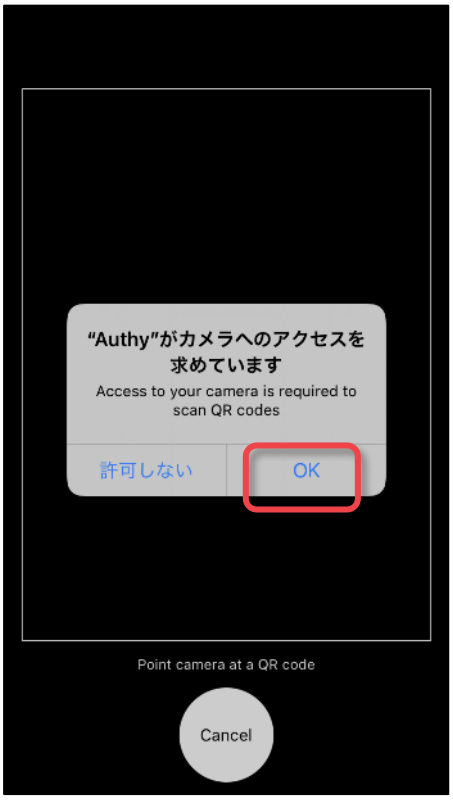
1） Authy を起動して、[＋] をタップします。



2） [Scan QR Code] をタップします。



3）　カメラへのアクセスを求める確認画面が表示されたら、［OK］をタップします。



4）　コントロールパネルに表示されている QR コードをスキャンします。

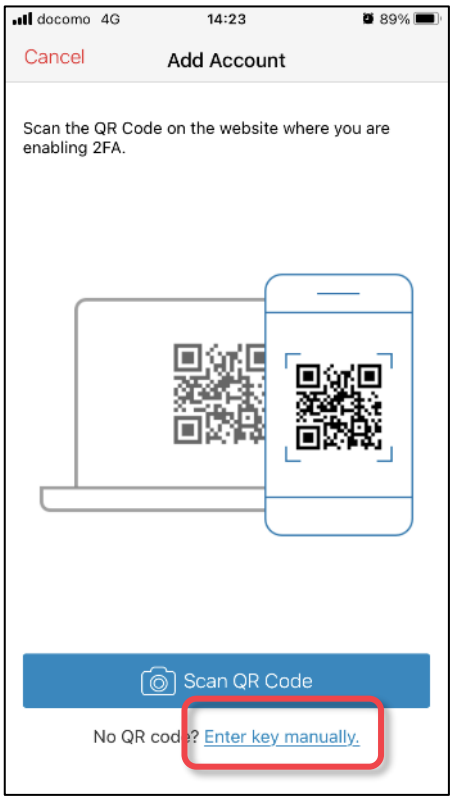
注意

二要素認証の有効化が完了するまで、コントロールパネルの画面を遷移したりブラウザを閉じたりしないでください。ページを離れると、初期設定用認証キーが更新されてしまいます。

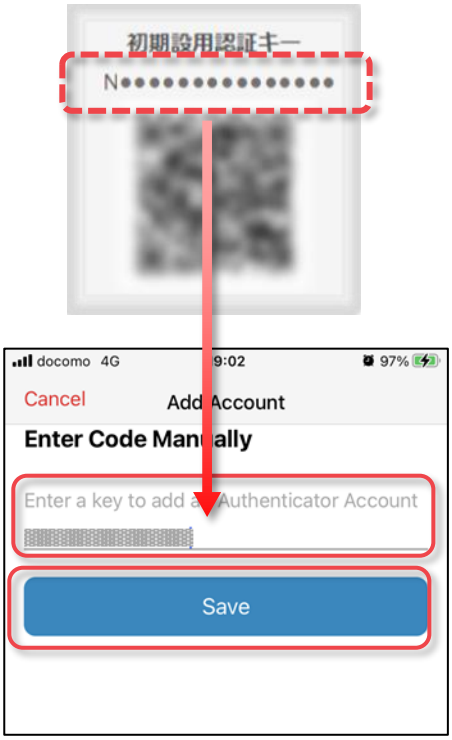
◆ **QR コードがスキャンできない場合は、後段の方法で、初期設定用認証キーを手入力できます。**

QR コードが正常にスキャンできない場合

① ［Enter key manually］をタップします。

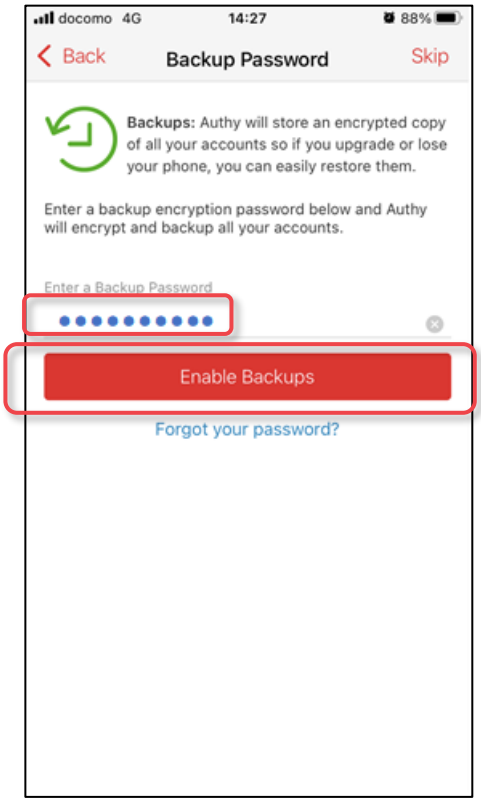


② コントロールパネルに表示されている初期設定用認証キーを入力して、［Save］をタップします。



5）　「Backups Password」を設置画する画面が表示されます。任意のパスワードを入力して、[Enable Backups]をタップします。

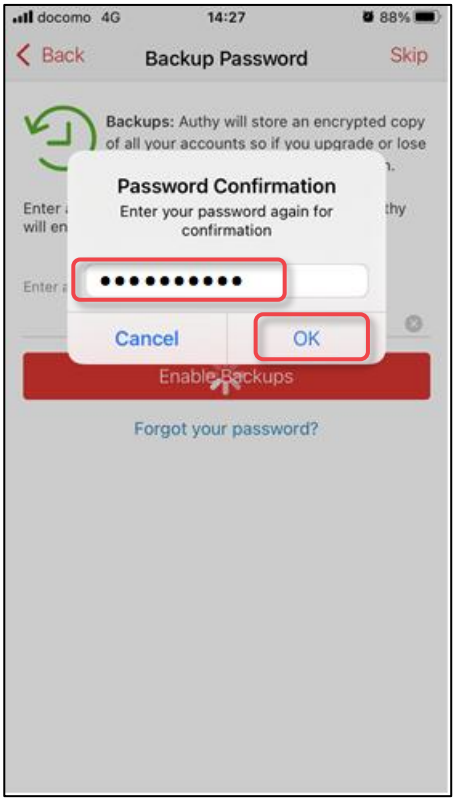
※　「Backups Password」を設定しておくと、スマートフォンを紛失した際に設定を復元できますので、設定することを推奨します。



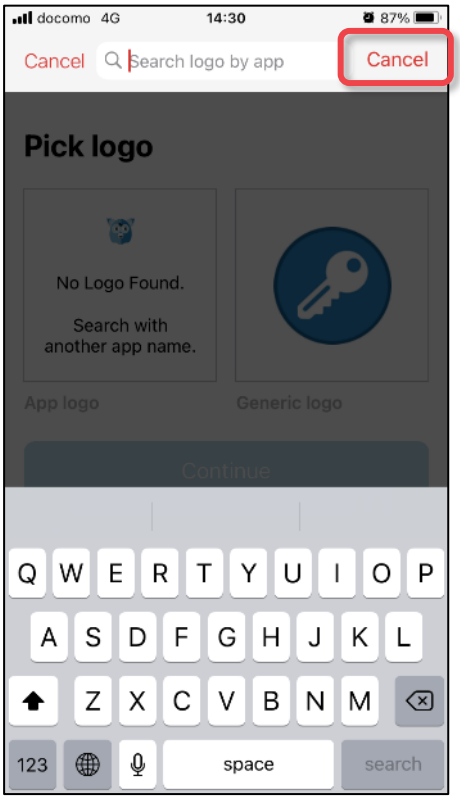
注意

アカウントのリカバリ（例: 3 回以上のパスワード誤入力でのロック時、一定期間の未使用時）の際にも、「Backups Password」の入力が必要になる場合があります。「Backups Password」を紛失・忘れる事のないようご留意ください。

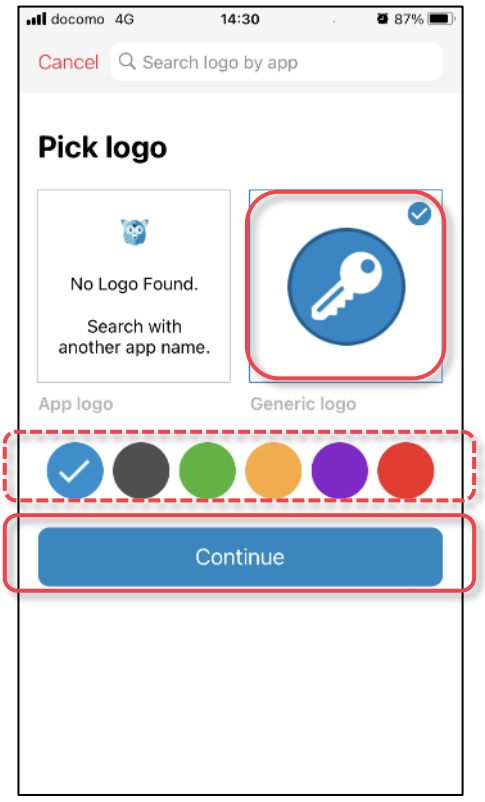
6）　パスワードの確認画面が表示されたら、パスワードを再入力して、[OK]をタップします。



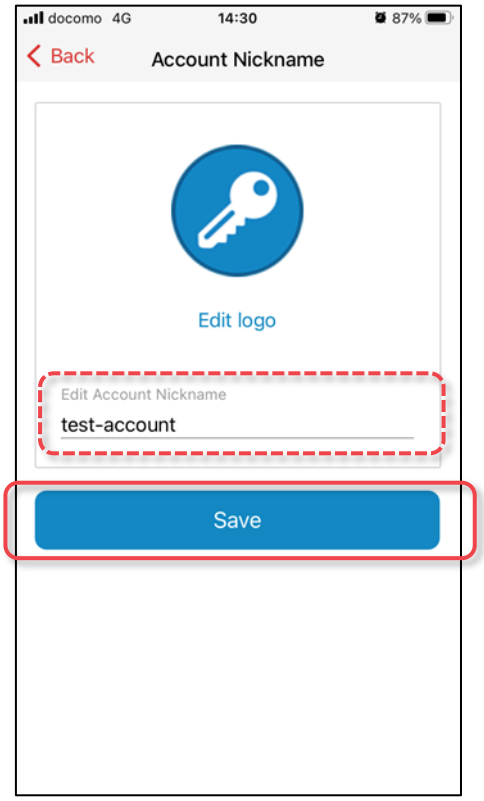
7）　Search logo by app 画面では、［Cancel］をタップします。



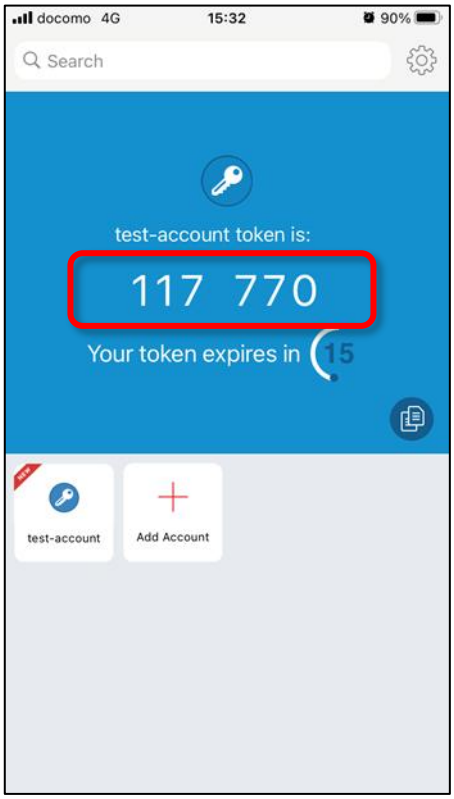
8）　Pick logo 画面で「Generic logo」を選択した後、任意のテーマカラーを選択して［Continue］をタップします。



9）　任意の［Account Nickname］を入力して、［Save］をタップします。

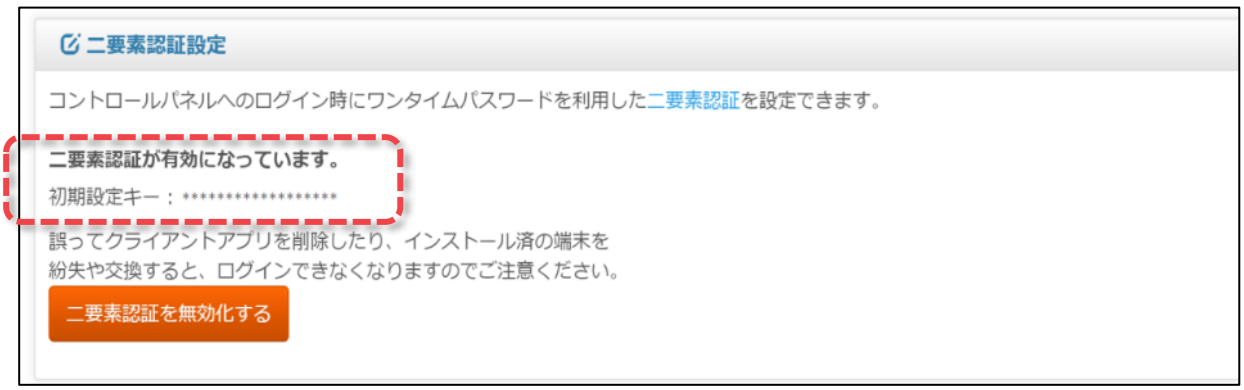


１０）　画面に 6 桁の数字（token）が表示されます。



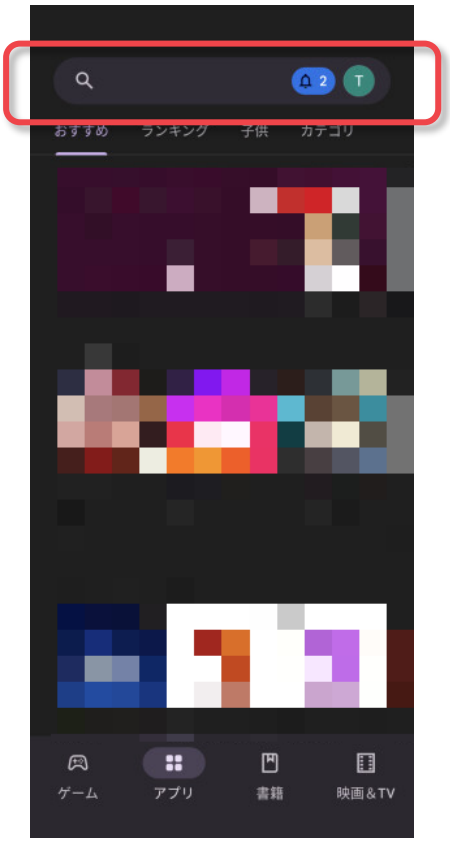
１１） Authy に表示されている 6 桁の数字（token）を、コントロールパネルの［ワンタイムパスワード］に入力して、［登録して有効化する］をクリックします。

１２） 「二要素認証が有効になっています。」と表示されたら、二要素認証の設定は完了です。

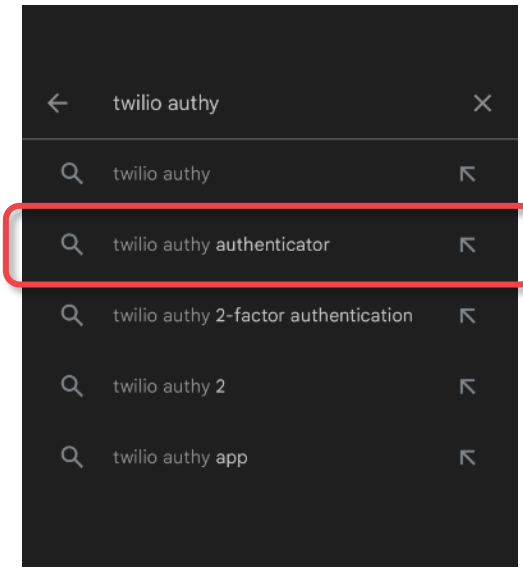


1.3.5. クライアントアプリのインストール(Android)

1） Play ストア(Google Play)を起動して、検索欄に「twilio authy」と入力します。



2） 「Twilio Authy Authenticator」を選択します。

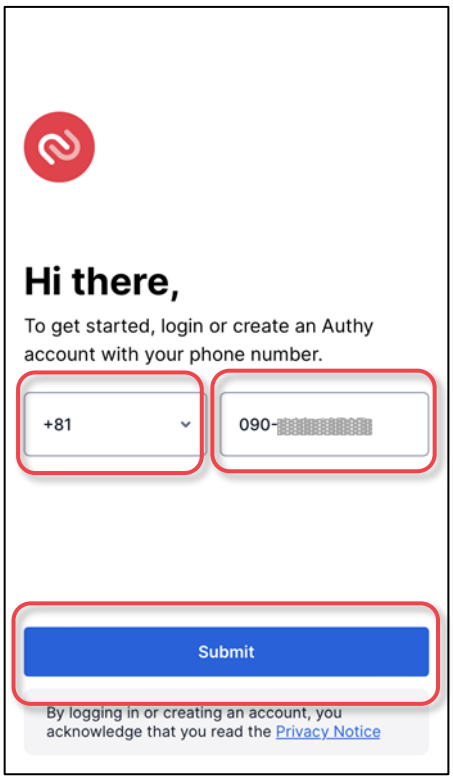


3） 検索結果が表示されたら、Twilio Authy Authenticator の［インストール］をタップします。

> **注意**
>
> アイコンおよび名称は、提供元により変更される場合があります。見つからない場合は、サポート窓口までお問い合わせください。

4） インストールが完了したら、［開く］をタップします。

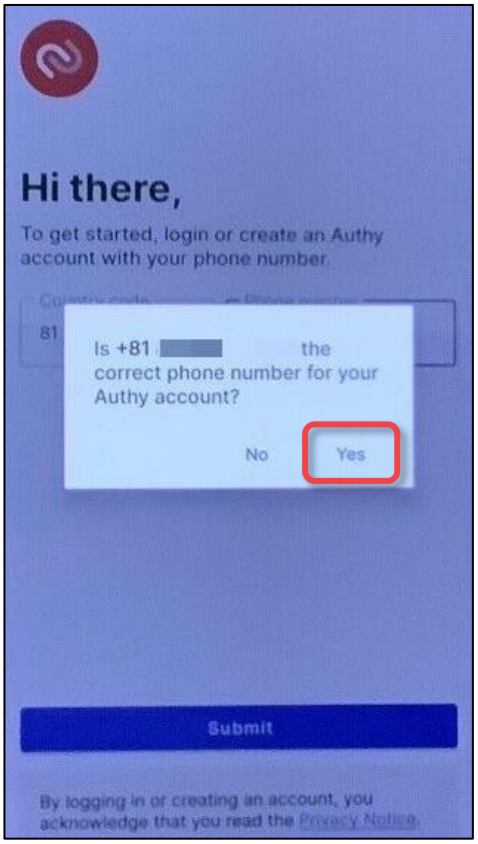
5） セットアップ画面が表示されたら、［Country Code］と［Phone number］を入力し、
［Submit］をタップします。



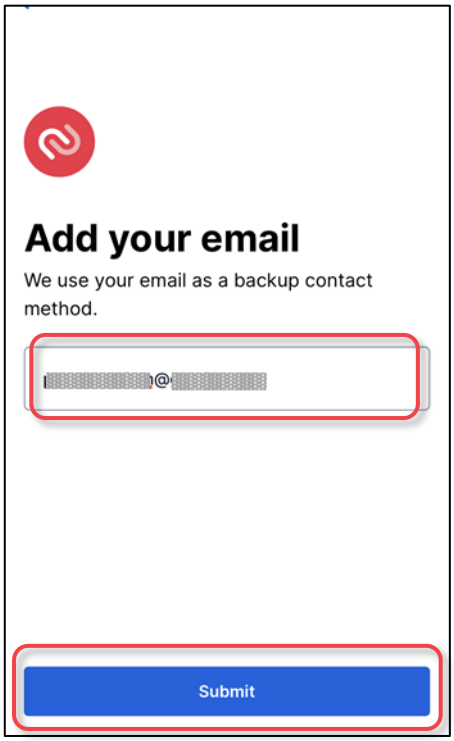
- ［Country Code］: 日本国際電話コード「+81」を選択
- ［Phone number］: 携帯電話の番号

※ 電話番号を入力する際は、先頭の「0」を省略します。
例)「090-1234-5678」の場合は「9012345678」

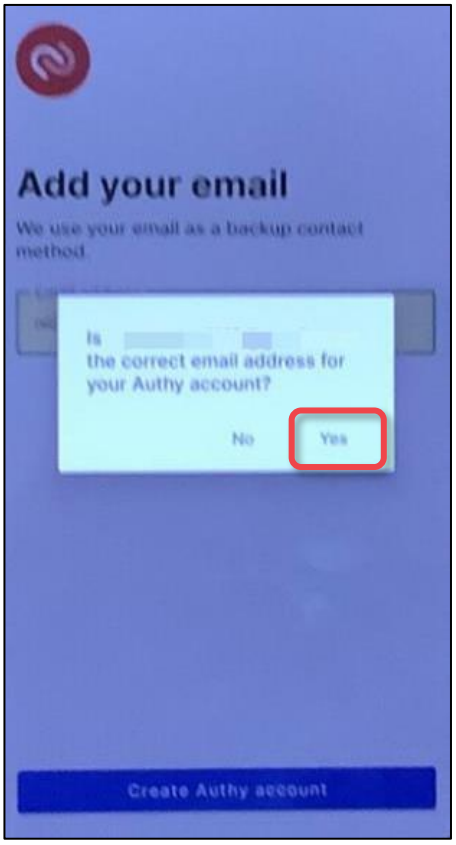
6） 入力した電話番号を確認するポップアップが表示されます。
間違いがないことを確認のうえ、［Yes］をタップしてください。



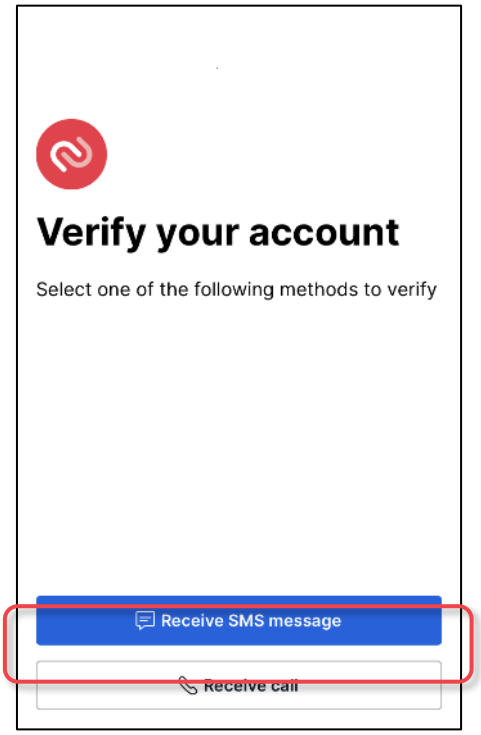
7） ［Email Adress］に、お客さまのメールアドレスを入力し、[Submit] をタップします。



8） 入力したメールアドレスを確認するポップアップが表示されます。間違いがないことを確認のうえ、［Yes］をタップしてください。



9） 「SMS(ショートメッセージ)認証」か「電話認証」かを選択する画面が開きます。（当マニュアルでは「SMS 認証」を例にご説明します）［Receive SMS Message］をクリックしてください。



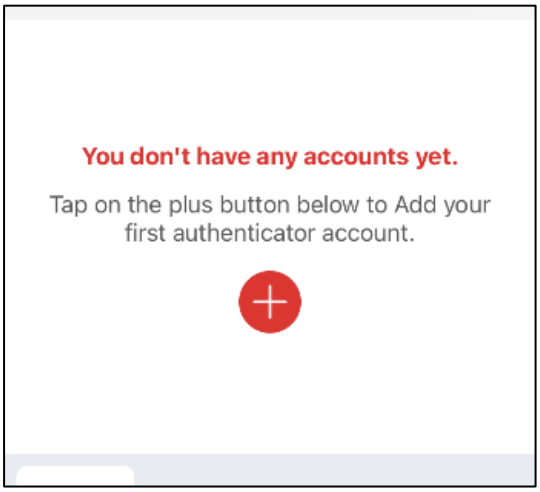
１０） SMS に記載されている「6 桁の認証番号」を入力してください。

※ 入力の有効時間は 30 秒程です。残り時間は［Code can be resent in ** seconds...］の箇所に表示されます。

※ 6 桁の数字を入力すると自動的に認証が開始されます。

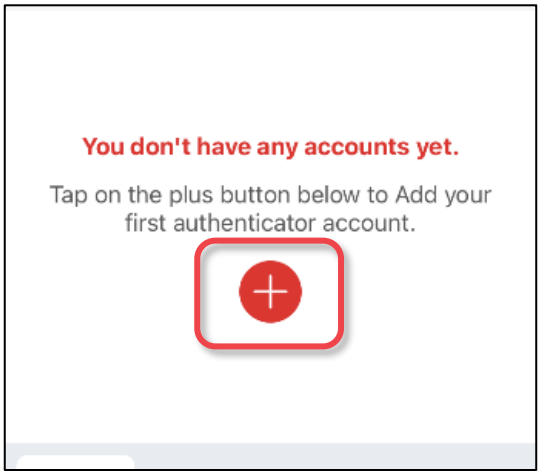
１１） 通知の許可を確認するポップアップが表示されたら、［許可］をタップしてください。

１２） 下図の画面が表示されたら、次は、**二要素認証を有効化**します。



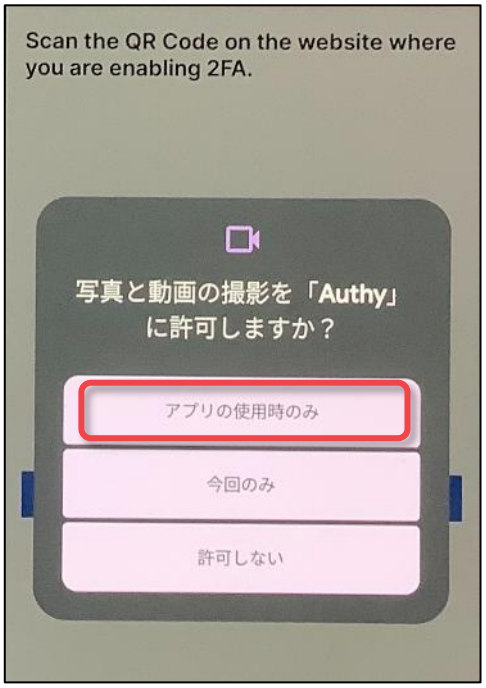
1.3.6. 二要素認証の有効化(Android)

1） Authy を起動して、[＋] をタップします。



2） [Scan QR Code] をタップします。

3）　カメラへのアクセスを求める確認画面が表示されたら、[アプリの使用時のみ] をタップします。



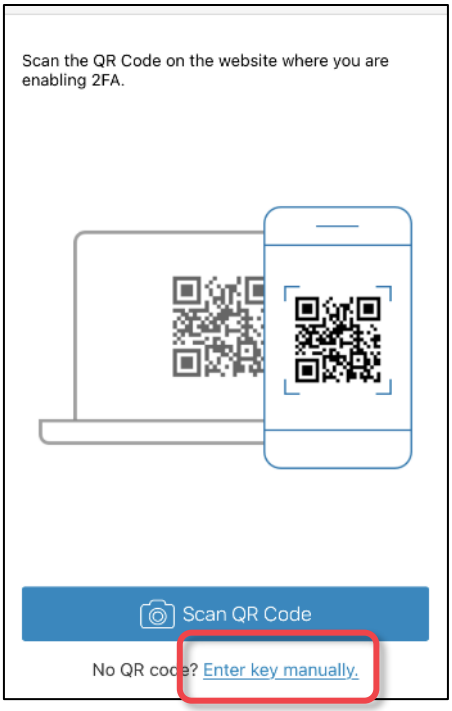
4）　コントロールパネルに表示されている QR コードをスキャンします。

> ⚠ 注意
>
> 二要素認証の有効化が完了するまで、コントロールパネルの画面を遷移したりブラウザを閉じたりしないでください。ページを離れると、初期設定用認証キーが更新されてしまいます。

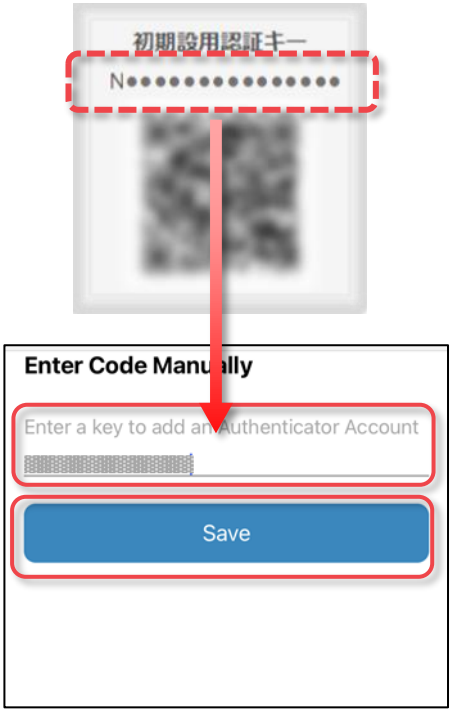
◆ **QR コードがスキャンできない場合は、後段の方法で、初期設定用認証キーを手入力できます。**

QR コードが正常にスキャンできない場合

① ［Enter key manually］をタップします。

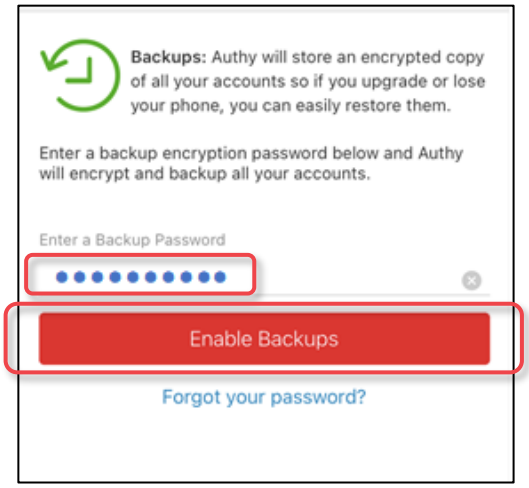


② コントロールパネルに表示されている初期設定用認証キーを入力して、［Save］をタップします。



5）　「Backups Password」を設置画する画面が表示されます。任意のパスワードを入力して、[Enable Backups]をタップします。

※　「Backups Password」を設定しておくと、スマートフォンを紛失した際に設定を復元できますので、設定することを推奨します。

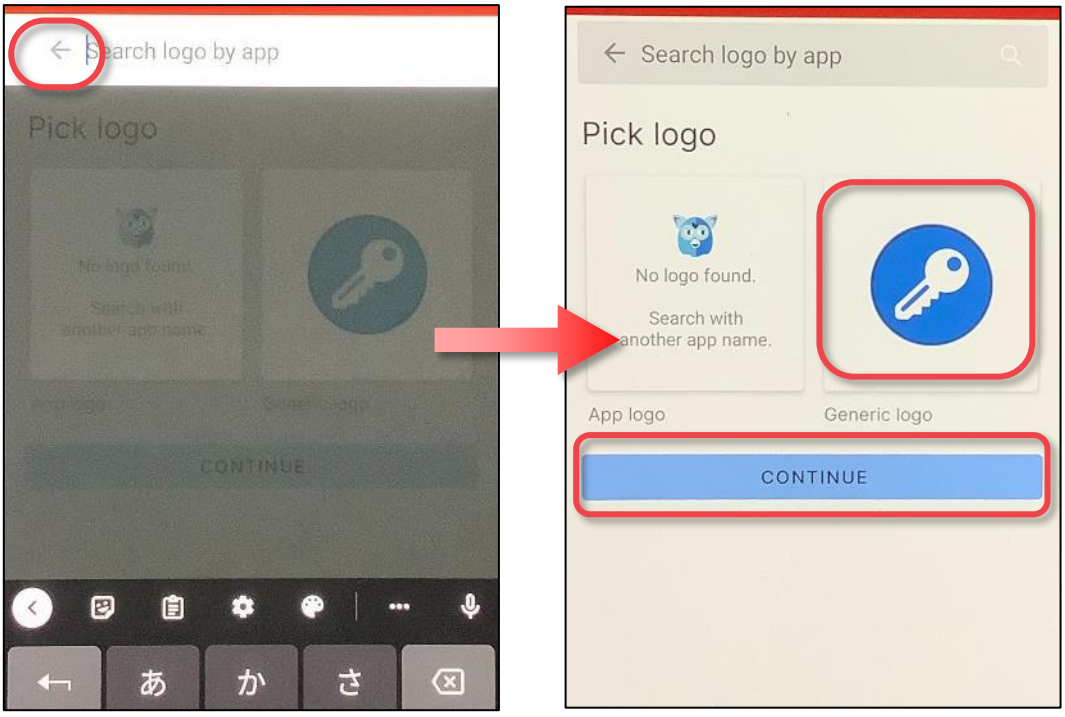


注意

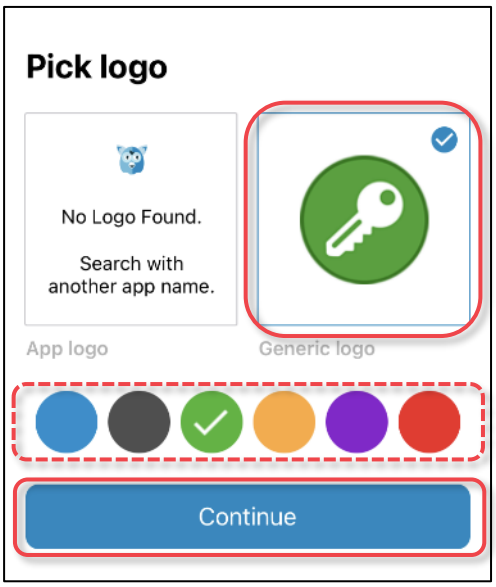
アカウントのリカバリ（例: 3 回以上のパスワード誤入力でのロック時、一定期間の未使用時）の際にも、「Backups Password」の入力が必要になる場合があります。「Backups Password」を紛失・忘れる事のないようご留意ください。

6）　パスワードの確認画面が表示されたら、手順 5）と同じパスワードを入力して、[OK]をタップします。

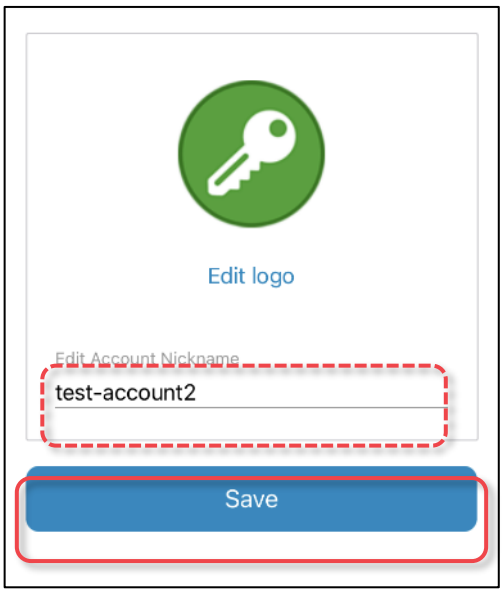
7）　Search logo by app 画面では、左上の矢印[←]をタップしてキーボードを非表示にしてから、「Generic logo」を選択して[Continue]をタップします。



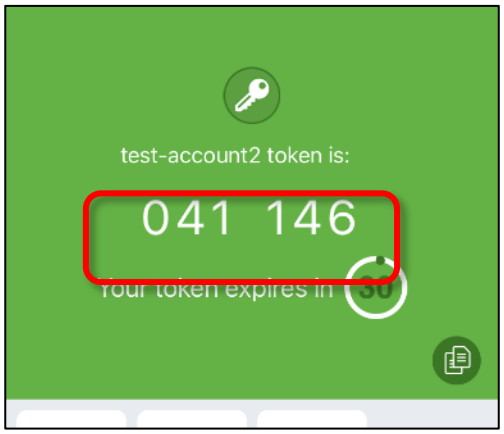
8） Pick logo 画面で「Generic logo」を選択した後、任意のテーマカラーを選択して［Continue］をタップします。



9） 任意の［Account Nickname］を入力して、［Save］をタップします。

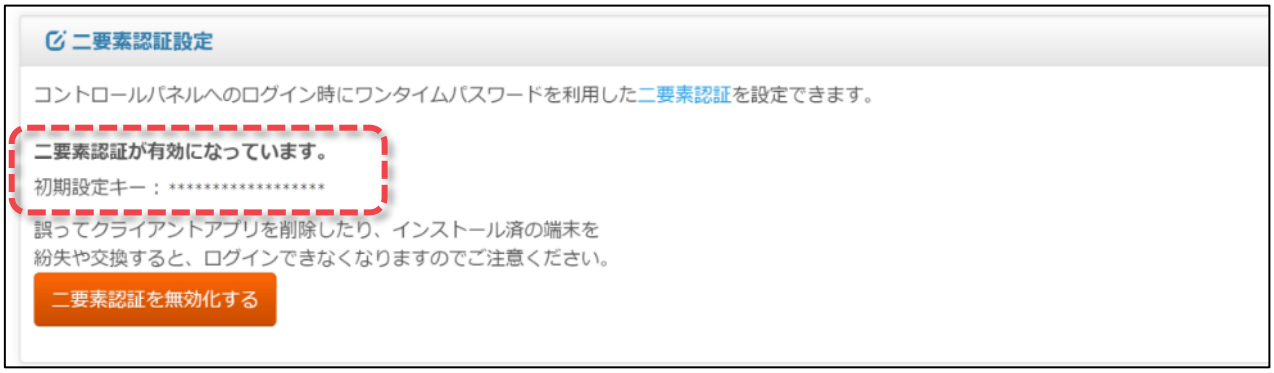


１０） 画面に 6 桁の数字（token）が表示されます。



１１） Authy に表示されている 6 桁の数字（token）を、コントロールパネルの［ワンタイムパスワード］に入力して、［登録して有効化する］をクリックします。

１２） 「二要素認証が有効になっています。」と表示されたら、二要素認証の設定は完了です。



1.3.7. PC 用のクライアントアプリについて

デスクトップ版 Authy（Windows、Mac、Linux 向け）は 2024 年 3 月 19 日にサポート終了（EOL）となります。
詳細は、以下の公式サイトをご確認ください。

User guide: End of Life (EOL) for Twilio Authy Desktop app - Twilio Help Center（英文）
https://help.twilio.com/articles/22771146070299-User-guide-End-of-Life-EOL-for-Twilio-Authy-Desktop-app

コントロールパネルのログイン時にデスクトップ版 Authy を使用している場合は、
EOL の期日までに、モバイル版 Authy に切り替えるか、別のデスクトップ版アプリに移行する必要があります。

※ EOL 後は、デスクトップ版 Authy は機能しなくなります。

※ モバイル版 Authy と同期して使用している場合は、EOL の期日までに、モバイル版 Authy でログインできるか確認しておくことをお勧めします。

■ モバイル版 Authy に切り替える

- バックアップ機能を有効にしている場合は、デバイス間で同期されます。

  参照） Enable or Disable Backups and Sync in Authy - Twilio Help Center
  https://help.twilio.com/articles/19753577267355

※ 同期するには、『デスクトップ版 Authy』に登録したものと同じ電話番号を『モバイル版 Authy』に登録する必要があります。

- モバイル版 Authy のインストール～初期設定については、以下をご参照ください。
  1.3.3 クライアントアプリのインストール（iPhone）
  1.3.4 二要素認証の有効化（iPhone）
  1.3.5 クライアントアプリのインストール（Android）
  1.3.6 二要素認証の有効化（Android）

■ 別のデスクトップ版アプリに移行する

- 事前にコントロールパネルの二要素認証を無効化してください。
  ※ 無効化の手順は「1.3.9 二要素認証の無効化」をご参照ください。

- デスクトップ版アプリはお客さまでお選びいただき、設定方法等は各アプリ提供元の案内をご確認ください。

注意

EOL 期日までに上段の対応ができず、コントロールパネルへ**管理者としてログインができなくなった場合**は、「管理者のパスワード変更」の手続きが必要となります。

※ 変更申込書の「申込内容」で［二要素認証解除］を選択してください。
※ お手続きの詳細は、以下の弊社サイトをご参照ください。

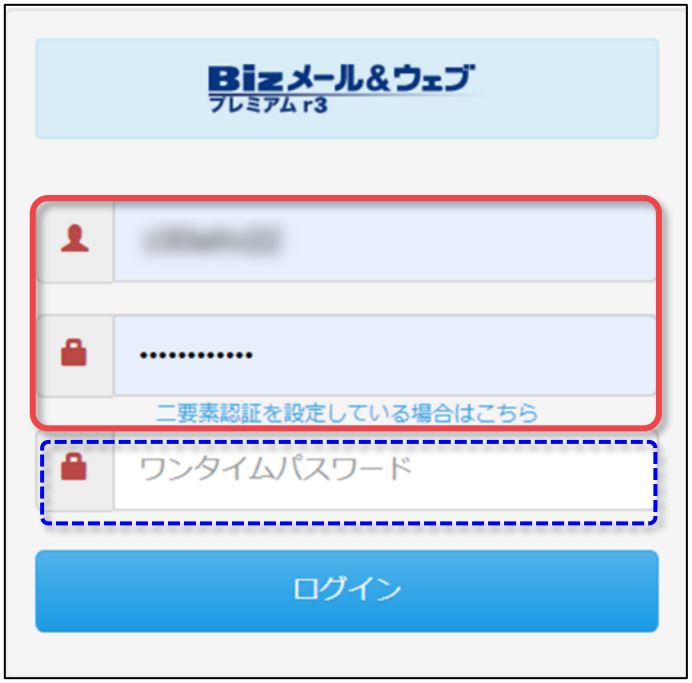
<パスワードの変更｜Biz メール&ウェブ プレミアム>
https://www.ntt.com/business/services/cloud/rental-server/vps/change_pass_02.html

※ 一般ユーザーがログインできなくなった場合は、管理者が該当ユーザーの二要素認証を無効化できます（参照：1.3.9 二要素認証の無効化 ＞他ユーザーの二要素認証を無効化する）。
二要素認証を無効化するとセキュリティリスクが高くなります。無効化した後は早めに有効化することをお勧めします。

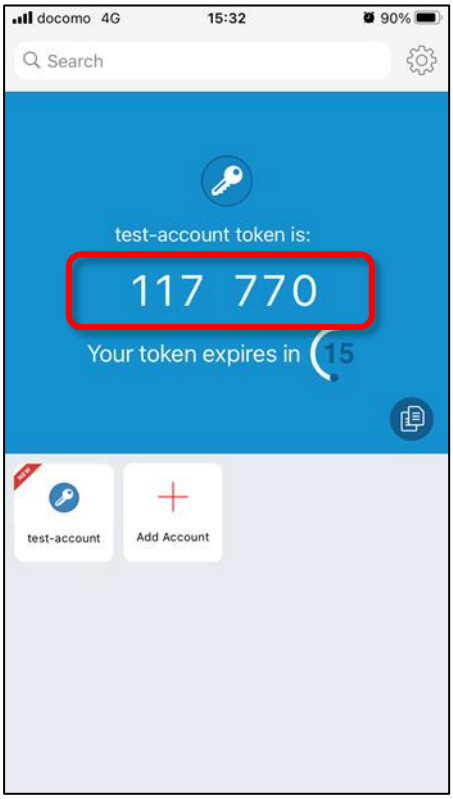
1.3.8. 二要素認証を利用したコントロールパネルへのログイン

1） コントロールパネルにアクセスします。

2） ［ユーザーID］［パスワード］を入力して、「二要素認証を設定している場合はこちら」をクリックすると、［ワンタイムパスワード］欄が表示されます。



3） クライアントアプリ(Authy)に表示されている6 桁の数字（token）を、手順２）で表示された［ワンタイムパスワード］欄に入力して、[ログイン]をクリックします。



4）　正常にログインできれば、二要素認証は設定されています。

アドバイス

コントロールパネルへログインするための二要素認証は、全てのユーザー（管理者、ドメイン管理者、一般ユーザー）において設定できます。

注意

- コントロールパネルの二要素認証を有効化している場合、クライアントアプリ(Authy)を紛失・破損すると、ログインできなくなります。

※　一般ユーザーがログインできなくなった場合は、管理者が該当ユーザーの二要素認証を無効化できます（参照：1.3.9 二要素認証の無効化 ＞他ユーザーの二要素認証を無効化する）。

※　管理者を変更する場合（前任者の異動・退職等）は、事前に二要素認証を無効化してください。ワンタイムパスワードを受け取ることができず、ログインできなくなります。
（参照：1.3.9 二要素認証の無効化 ＞管理者の二要素認証を無効化する）。

※　管理者がログインできなくなった場合は、「管理者のパスワード変更」の手続きが必要となります。手続きに関しては、以下の弊社サイトをご参照ください。

<パスワードの変更｜Biz メール&ウェブ プレミアム>
https://www.ntt.com/business/services/cloud/rental-server/vps/change_pass_02.html

- ワンタイムパスワードの有効期限は **30 秒**です。

1.3.9. 二要素認証の無効化

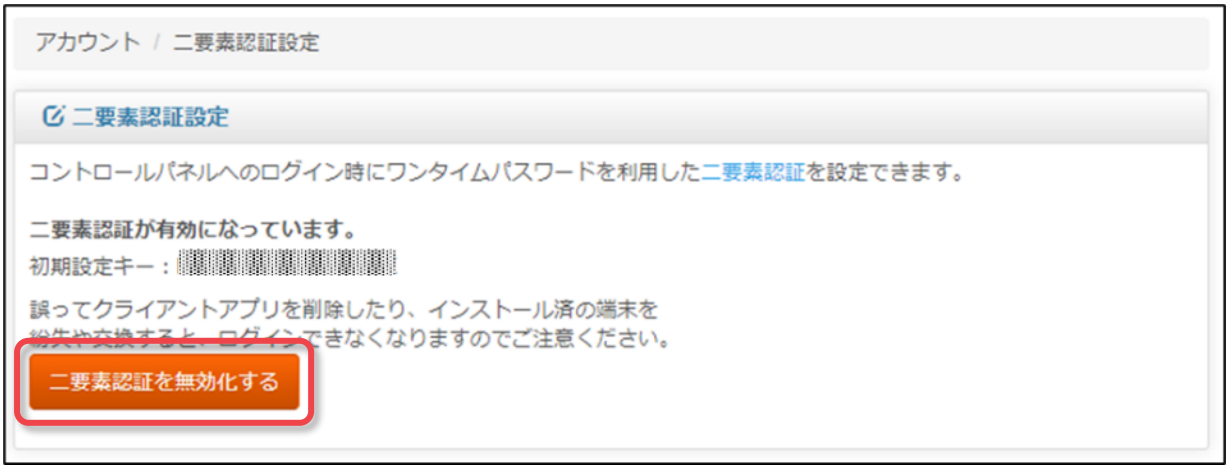
管理者の二要素認証を無効化する

ここでは、「管理者」自身の二要素認証を無効化する手順をご案内します。

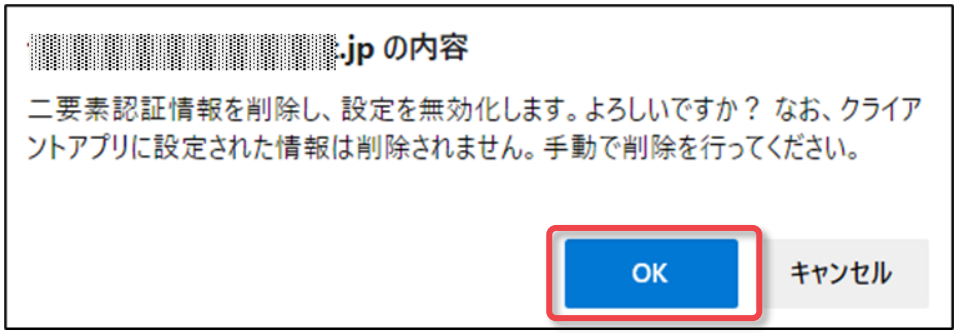
1） 管理者アカウントで、コントロールパネルにログインします。

2） 右上のユーザーID のボタンから、［二要素認証］をクリックします。

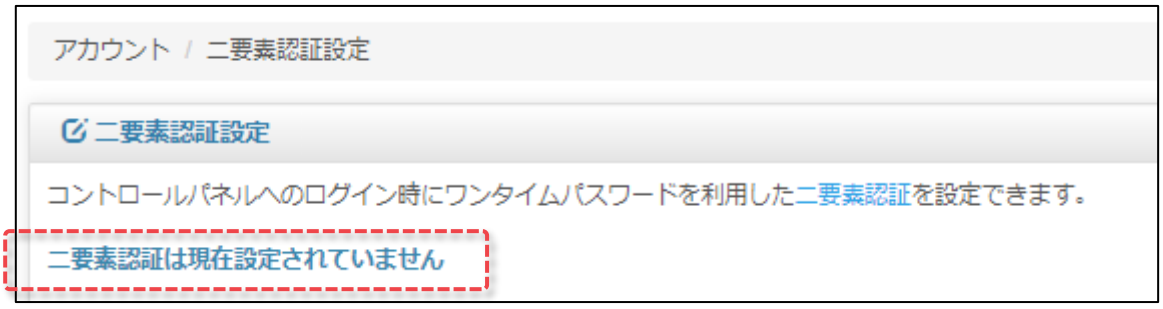
3） 「二要素認証設定」画面の、［二要素認証を無効化する］をクリックします。



4）　確認のダイアログが表示されたら、OK をクリックします。



5）「二要素認証設定」画面に、「二要素認証は現在設定されていません」と表示されていれば完了です。



他ユーザーの二要素認証を無効化する

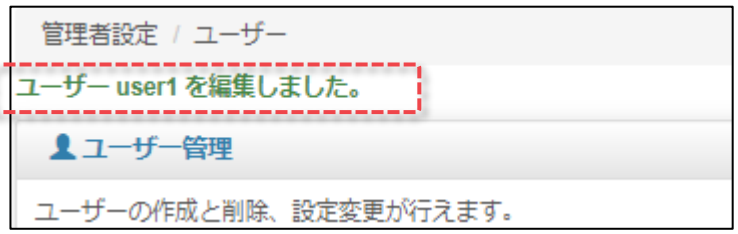
ここでは、「管理者」が、ドメイン管理者や一般ユーザーの二要素認証を無効化する手順をご案内します。

1）　管理者アカウントでコントロールパネルにログインします。

2）左メニューの［ユーザー］から「ユーザー管理」画面を開き、該当ユーザーの［設定］をクリックします。

3）「ユーザー設定」画面で、画面下部にある「二要素認証ログイン設定の解除」の［設定を解除する］にチェックを入れて［保存］をクリックします。

4）　「ユーザー○○○を編集しました。」と表示されたら完了です。



※　二要素認証の設定を無効化されたユーザーは、ワンタイムパスワードなし（ユーザーID とパスワードのみ）でログイン可能になります。

2　メールサーバー

2.1. メールサービスの概要

2.1.1. メールサーバー機能

本サービスのメールサーバー機能は、以下の内容となります。

機能	内容
提供プロトコル	・SMTP (port587) ・STARTTLS (port587) ・POP3(port110) ・POP3s(POP3 over SSL: port995) ・IMAP(IMAP4: port143) ・IMAPs(IMAP over SSL: port993)
インターフェース	・コントロールパネル上のウェブメール ・POP3/IMAP ・SMTP(認証方式は SMTP Auth)

注意

- SMTP(Port 25)はご利用いただけません。

2.1.2. メール送受信の暗号化

本サービスでは、次に示すプロトコルを使用いただくことで、本サービスとメールソフト間の送受信を暗号化する事ができます。

- POP over SSL (Port 995)
- IMAP over SSL (Port 993)
- STARTTLS (Port 587)

注意

- **本サービスでは、TLS1.0 と TLS 1.1 が無効化されています。**

※ Outlook2010・Outlook エクスプレス・Live メールは、「暗号化された接続(SSL)」が使用できません。

※ 非暗号化接続も使用可能ですが、Biz メール＆ウェブでは暗号化を推奨しているため、**暗号化接続可能なメールソフト**をご利用いただきますようお願い致します。

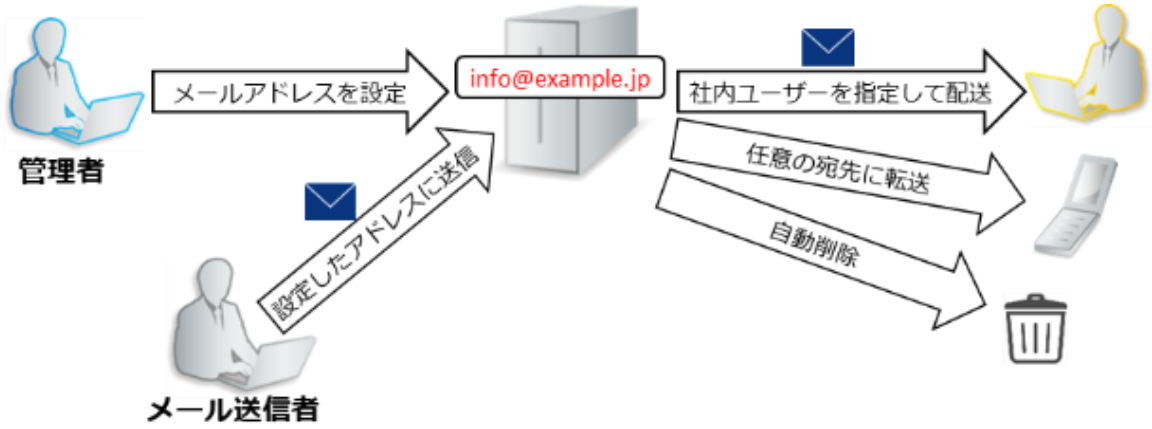
※ 動作確認済みのメールソフトや設定については、『**メール設定マニュアル**』をご参照ください。

- 上記のプロトコルを使用する場合は、本サービスにインストール済みの証明書の利用が必要となります。お客さまがご利用するメールソフト内のメールサーバー欄には、「c******.mwprem.net」を設定してください。

※「c******」は、『ご利用内容のご案内』に記載されている［ユーザ ID(管理者)］です。

2.2. メールアドレス

「管理者」または「ドメイン管理者」がメールアドレスを設定する事で、1 ユーザーが複数のメールアドレスを所有できるようになります。また、設定したメールアドレスには、「任意のアドレスへの転送」や「自動削除」等の動作を指定する事ができます。



2.2.1. メールアドレスの新規作成

1） ［メールサーバー］から、［メールアドレス］をクリックします。

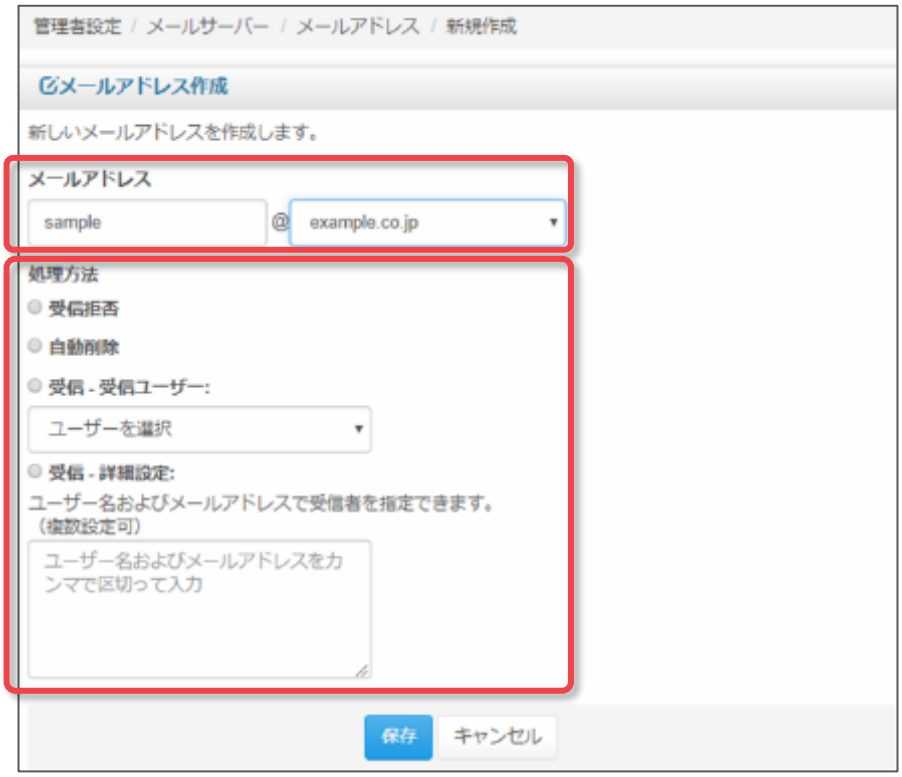
「メールアドレス管理」画面に「amanda@c15***.mwprem.net」という、覚えのないメールアドレスが表示されている場合**

このメールアドレス（amanda@テンポラリドメイン）は、旧環境からシステム上で登録（コントロールパネル上は非表示）されていましたが、 新環境へ「全て同期」して移行しているため、コントロールパネル上に表示された状態になっています。

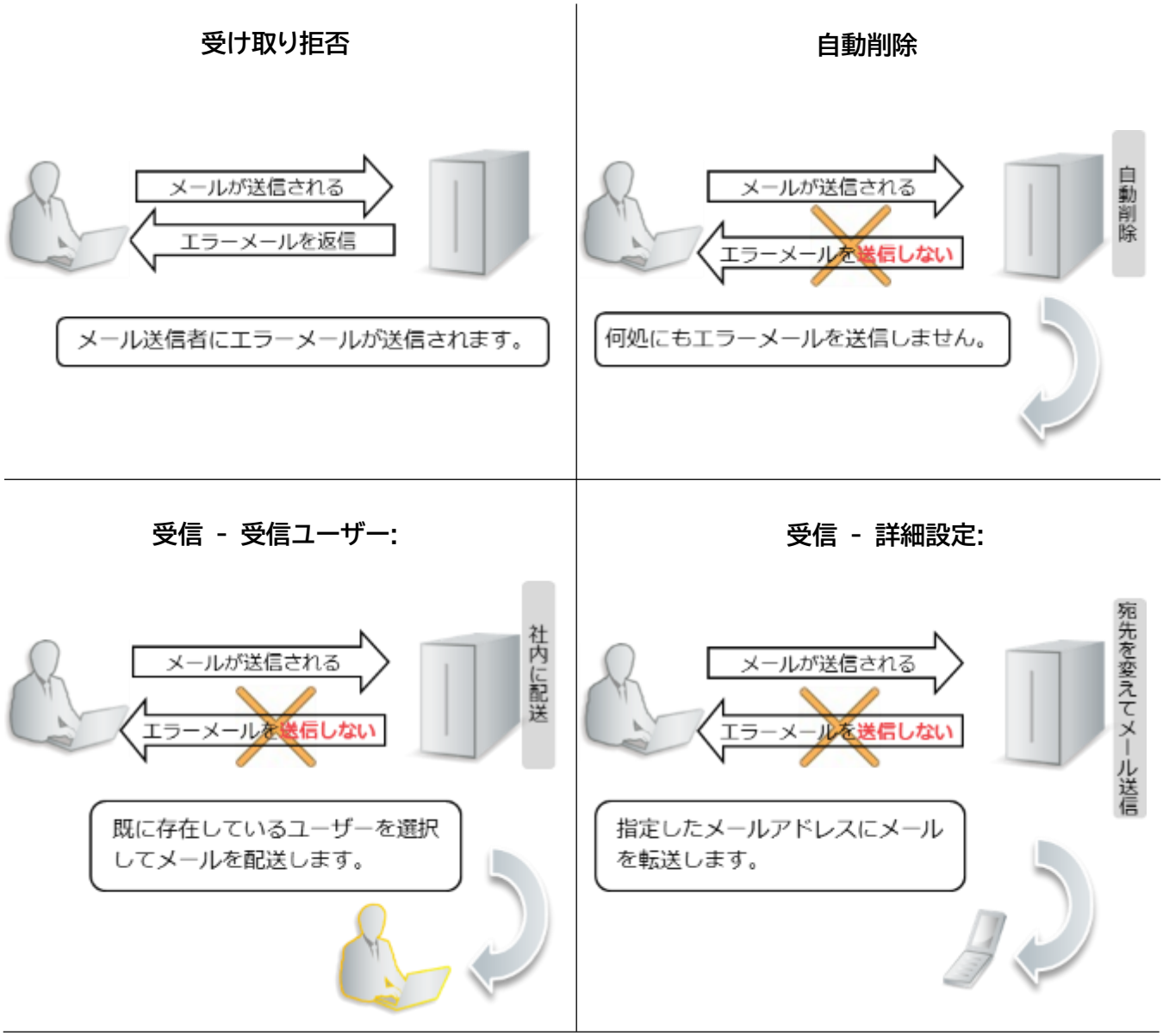
システム側でも特に決まった用途で用いてはいないため、不要であれば削除していただいて問題ありません。

2） ［新規作成］をクリックします。

3） ［メールアドレス］の「@から左側」を入力して、ドメインを選択した後、［処理方法］を選択します。



［処理方法］の選択について



- 上図をご確認の上、利用したい選択肢にチェックを入れてください。

※ ［受信 - 詳細設定:］を選択した場合は、転送先のメールアドレス（複数の場合は, [カンマ]で区切る）を入力します。

注意

［受信 - 詳細設定:］に入力する際は、社内（コントロールパネルで設定されたドメイン）を転送先に指定する場合でも必ず、@から右側のドメインも入力してください。

例: sample1 ×　　sample@example.co.jp　○

※自分自身のアドレスに転送する場合は、@から右側が不要です。

4） ［処理方法］の内容に間違いがないことを確認して、［保存］をクリックします。メールアドレスを追加した旨のメッセージが表示されたら、完了です。

2.2.2. メールアドレスの設定変更・削除

設定変更について

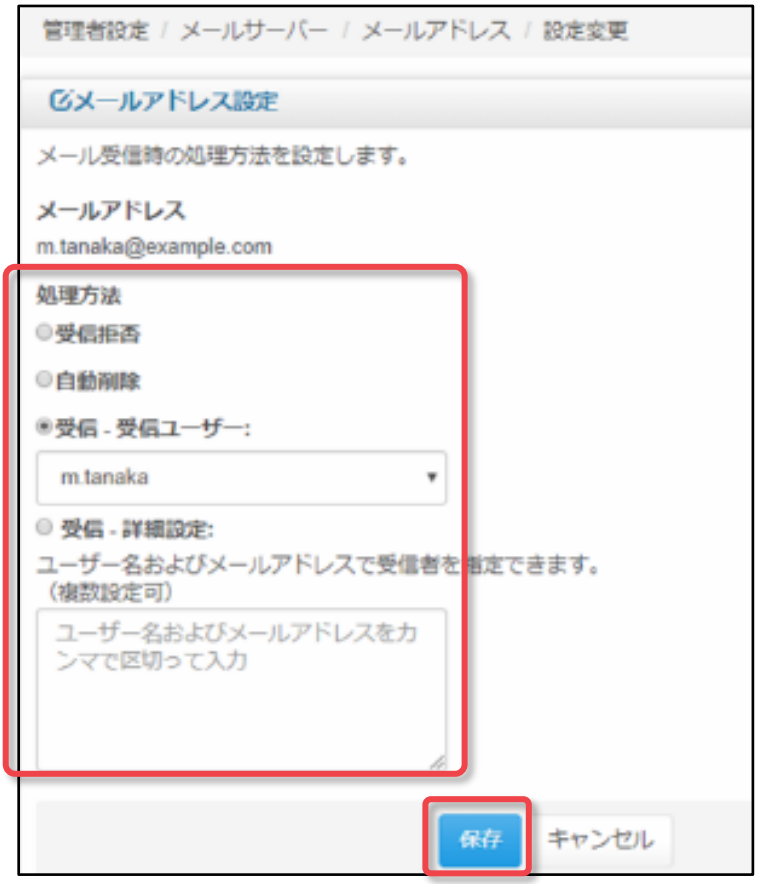
1） ［メールサーバー］から、［メールアドレス］をクリックします。

2） 設定変更したいメールアドレスの、［設定］をクリックします。

注意

メールアドレス自体の変更は行えません。
別途、別の文字列で［新規作成］する必要があります。

3）　［処理方法］を任意の設定に変更して、［保存］をクリックして設定変更完了です。



削除について

1） ［メールサーバー］から［メールアドレス］をクリックした後、削除したいメールアドレスの、［削除］をクリックします。

2） 確認画面が表示されたら［削除］をクリックします。

3） 削除された旨のメッセージが表示されたら、メールアドレス削除の完了です。

注意

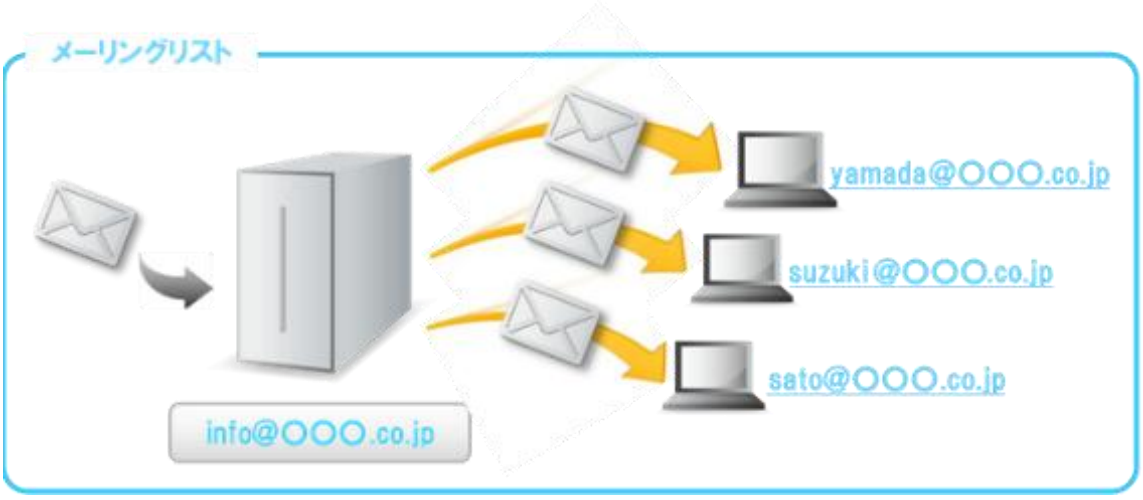
メールアドレスの削除以降は、そのメールアドレスでのメール受信は出来なくなります。
ただし、サーバーに保存済のメールデータが削除される事はありません。

2.3. メーリングリスト

2.3.1. メーリングリストの概要

メーリングリストとは、複数のメールアドレスに向けて一斉にメール配信する機能のことです。

たとえば、組織内の「営業担当」「開発担当」といったチームに対して、それぞれメーリングリストを作成し、そこに該当するメンバー全員のメールアドレスを登録すると、１つのメールアドレスにメールを送信する操作で、登録メンバー全員に向けてメールを送信できます。



※ メーリングリストの管理は、コントロールパネルで行います。

本サービスで作成できるメーリングリストの概要は、以下になります。

基本機能	
作成できるメーリングリスト数	最大 400 件
メーリングリストに登録できるアドレス数	最大 4000 メールアドレス
送信可能なメールのサイズ	添付ファイルを含めて、最大約 30MB

注意

- メーリングリストの中に、更にメーリングリストのアドレスを登録すると、**正常に動作しない**場合があります。

2.3.2. メーリングリストの作成

メーリングリストの機能をご利用になるには、「メーリングリストの作成」と「メンバー登録」の２つの設定が必要となります。以降で設定手順についてご説明します。

1） コントロールパネルの左メニュー「メールサーバー」から［メーリングリスト］をクリックして、［新規作成］をクリックします。

2） メーリングリスト作成の画面が表示されたら、各項目を入力し、［保存］をクリックしてください。

※ 入力規則等は、後段の表と注意事項 をご参照ください。

入力項目について

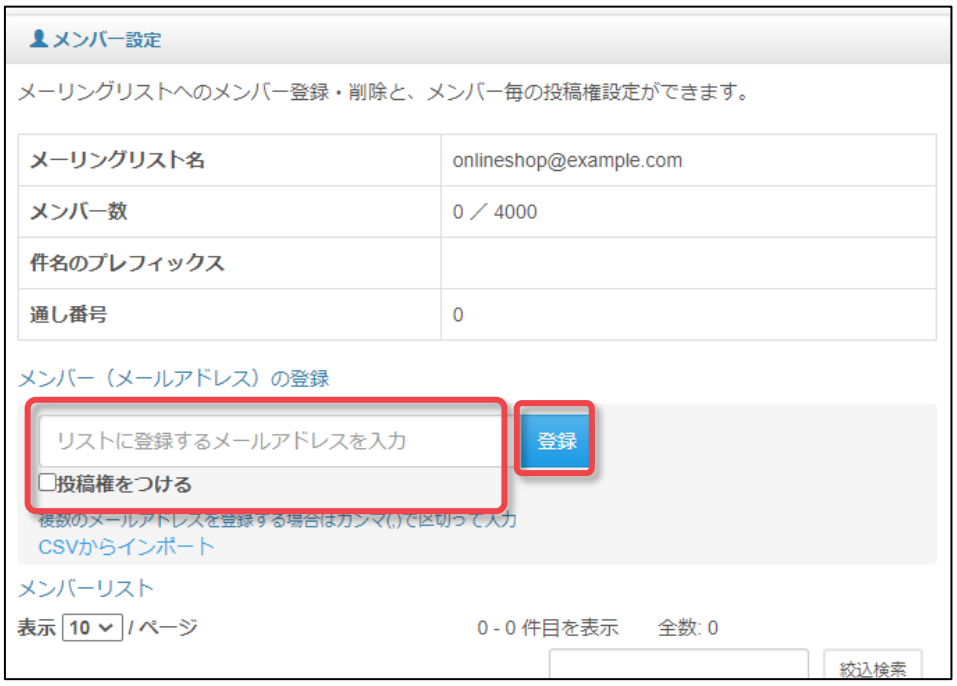
<table>
<tr><th>#</th><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>1</td><td>メーリングリスト名</td><td colspan="2">■登録するメーリングリスト名を入力します。
【使用できる文字種】※ 最大 64 文字
半角英小文字（a-z)、　半角の数字、(0-9)、　一部の半角記号(- 　_　 .)</td></tr>
<tr><td>2</td><td>件名のプレフィックス</td><td colspan="2">■必要に応じて、メーリングリストに投稿した際に件名の先頭に追加される「文字列」を指定できます。(空欄のままでも保存可能です)
【使用できる文字種】※ 最大 64 文字
半角英数字(a-z, A-Z, 0-9)、　半角記号(# [ ] / ¥ < > を除く)</td></tr>
<tr><td>3</td><td>通し番号の表示</td><td colspan="2">■このチェックボックスを選択すると、メーリングリストに投稿したときに、件名の先頭に「通し番号」を付与します。
※「通し番号の表示」を選択しない場合でも、番号のカウントは実施されます。</td></tr>
<tr><td rowspan="4">4</td><td rowspan="4">投稿可能なメンバー</td><td colspan="2">■メーリングリストへの投稿を許可する送信者を指定します。</td></tr>
<tr><td>メンバーであれば誰でも投稿可能</td><td>メーリングリストに登録されているメールアドレスから、メーリングリストへの投稿が可能になります。</td></tr>
<tr><td>管理者に承認されたメンバーのみ</td><td>登録済みのメールアドレスで、「許可された投稿者」に指定されたメールアドレスのみ、メーリングリストへの投稿が可能になります。</td></tr>
<tr><td>メンバーに関わらず誰でも投稿可能</td><td>メーリングリストへの登録状況に関係なく、あらゆるアドレスから、メーリングリストへの投稿が可能になります。ただし、登録している全メンバーが「投稿権あり」に設定されている必要があります。
※「投稿権なし」のメンバーを追加、もしくは既存メンバーを「投稿権なし」に変更すると、メーリングリストの設定が「管理者に承認されたメンバーのみ」に変更されます。
この場合は、全メンバーを「投稿権あり」に設定した後で、メーリングリストの設定を「メンバーに関わらず誰でも投稿可能」に変更してください。
※ 全メンバーを「投稿権あり」に設定しただけでは、メーリングリストの設定は「メンバーであれば誰でも投稿可能」となります。</td></tr>
<tr><td rowspan="4">5</td><td rowspan="4">メールの返信先</td><td colspan="2">■メーリングリストから配信されたメールの返信先を選択します。</td></tr>
<tr><td>メーリングリスト名</td><td>メーリングリストが指定されます。</td></tr>
<tr><td>送信者</td><td>メーリングリストへの投稿者が指定されます。</td></tr>
<tr><td>特定のアドレス</td><td>プルダウン下のテキストボックスに入力したメールアドレス宛に送信されます。
【使用できる文字種】※ 最大 64 文字
半角英小文字（a-z)、　半角の数字(0-9)
一部の半角記号(- 　_　 .)</td></tr>
</table>

注意

- メーリングリスト名は、登録済のユーザーID と重複して作成することはできません。
- メーリングリスト名に、**英大文字** は使用できません。

3） メーリングリスト管理画面に、作成したメーリングリストが表示されます。
続けて、作成したメーリングリストに「メールを受信するメンバー」を登録する為、［メンバー］をクリックしてください。

4） 「メンバー設定」画面が表示されたら、［メンバー（メールアドレス）の登録］に登録したいメールアドレスを入力して、［登録］をクリックします。
※ 必要に応じて、［投稿権をつける］にチェックを入れてください。



※ 入力規則等は、次ページ をご参照ください。

項目	説明
メンバー(メールアドレス)の登録	● メールアドレスを入力して、[登録]をクリックすると、該当のメーリングリストにメールアドレスを追加できます。 ● [投稿権をつける]にチェックを入れると、追加するメールアドレスに「許可された投稿者」の権限を付与できます。 **【使用できる文字種】** 半角英字(a-z) ，半角数字(0-9) ，一部の半角記号(_ - .) 最大 64 文字

アドバイス

「投稿権」とは

メーリングリストを作成する際に[投稿可能なメンバー]を[管理者に承認されたメンバーのみ]に設定した場合は、メンバー登録時に[投稿権]を付与したメンバーのみが、メーリングリストへの投稿が可能となります。
投稿権が付与されていないメールアドレスからメーリングリストに送信された場合は、送信元にエラーが返ります。

5） 「受信者が追加されました。」と表示され、メンバー(メールアドレス)欄に、登録したメールアドレスが表示されたら完了です。

注意

- メールアドレスを登録する際は、メールがループしないようご注意ください。
  ループとなった場合、エラーとなり正しく送信されない可能性があります。
- メーリングリストの中に、更にメーリングリストのアドレスを登録すると、正常に動作しません。
- メンバー（メールアドレス）の登録する際は、お間違えのないようご注意ください。

2.3.3. メーリングリストの設定変更

1） コントロールパネルの［メーリングリスト］から、設定変更を行うメーリングリストの［設定］をクリックします。

2） メーリングリスト編集の画面が表示されたら、設定を変更し、［保存］をクリックしてください。
各項目の内容については、「2.3.2 メーリングリストの作成」をご参照ください。

注意

一度作成されたメーリングリストの名前を変更することはできません。
該当のメーリングリストを削除の上、再作成が必要です。

2.3.4. メンバーの編集

（1）投稿権の編集について

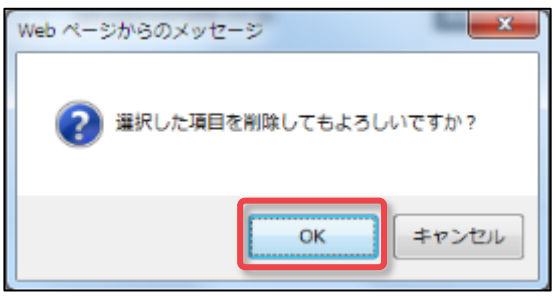
① コントロールパネルの [メーリングリスト] から、設定変更を行うメーリングリストの [メンバー] をクリックします。

② ［操作］の［投稿権をはずす/投稿権をつける］をクリックすると、投稿権を変更できます。

（2）メンバーの削除

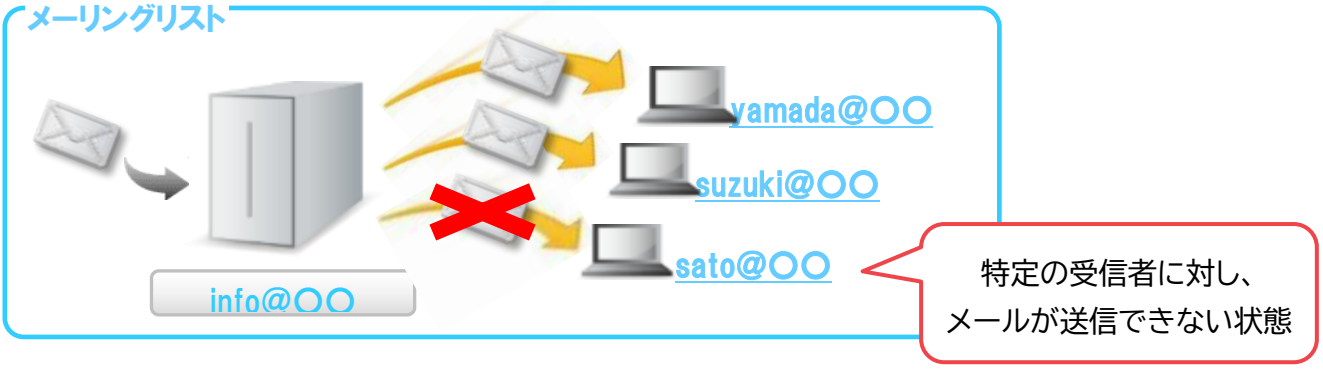
削除したいメンバーの［削除］ボタンをクリックするか、チェックボックスで複数のメンバーを選択して一括削除ができます。

※ 削除の確認メッセージが表示されたら［OK］をクリックしてください。



2.3.5. メール不達時の動作

メールアドレスの登録ミスや削除などにより、メーリングリストの受信者に対して正常にメールが送信されない場合、該当のアドレスは、メーリングリストの受信メンバーから自動的に停止されます。



■アドレス停止の流れ

メール送信に失敗した回数がカウントされ、一定数に達すると該当アドレスへの配送を一時停止し、警告メールを 7 日おきに 3 回送付します。

■停止アドレスの復元について

該当アドレスを復元にするには、以下いずれかの作業を実施してください。

停止アドレスの復元	
[1] 受信者による作業	該当アドレス宛に送付された警告メールに対し、**件名や内容を変更せずにそのまま返信**します。 ※この方法は、受信者が警告メールを受信できた場合のみ可能です。 **警告メール内容サンプル>** *onlineshop* メーリングリストでの会員権が,一時的に停止されています. 停止解除の操作を行わなければ，このリストからのメールは受け取れません．あと 3 回これと同じ通知を発送しますが，それ以降は退会措置をとらせていただきます． 停止を解除するには，このメールに返信（ただし, Subject: 行は変更しないでください)してください． 問題や質問があれば，リスト管理者宛にご連絡ください．
[2] 管理者による作業	コントロールパネルの「受信者リストの編集」画面で、該当メールアドレスを受信者から削除した後、再度登録してください。

アドバイス

受信者の一時停止時とメンバー削除時には、管理者宛にメールで通知されます。

2.4. 送信ドメイン認証

送信ドメイン認証（DKIM）に関する以下の確認と操作が可能です。

- DKIM 認証のステータスの確認
- DKIM 認証の有効化/停止
- DKIM レコードに設定する情報の確認

※ コントロールパネルに登録済みのドメインが対象となります。
※ テンポラリドメイン（c*******.mwprem.net）には DKIM 認証を設定できません。

2.4.1. DKIM 認証のステータス確認

DKIM 認証のステータスを確認するには、左メニューの「メールサーバー」から［送信ドメイン認証］をクリックして「DKIM」画面を開きます。

［1］コントロールパネルに登録したドメインが表示されます。

［2］DKIM 認証の［有効化］［停止］を切り替えることができます。

※ 詳細は「2.4.2 DKIM 認証の有効化/停止」をご参照ください。

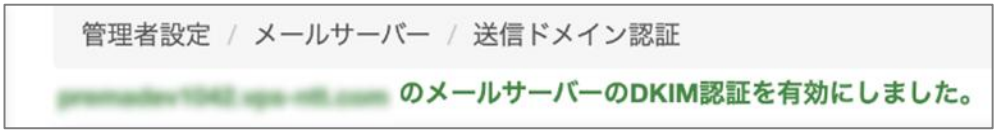
［3］DKIM レコードのステータス（以下 3 種類）が表示されます。

- ⊘ 設定済 ：問題なく設定されている
- ⊘ 設定されていません ：未設定
- ⊘ 公開鍵が正しくありません ：設定されている公開鍵が異なる

2.4.2. DKIM 認証の有効化/停止

DKIM 認証を有効化/停止するには、左メニューの「メールサーバー」から［送信ドメイン認証］をクリックして、「DKIM」画面を開きます。

- ステータスが「停止中」の場合は［有効化］できます。
  ※ 処理後は、有効化した旨のメッセージが表示されます。



- ステータスが［認証中］の場合は［停止］できます。
  ※ 処理後は、停止した旨のメッセージが表示されます。

■有効化までの手順

1） コントロールパネルにドメインを登録する
参照）セットアップマニュアル「4.1 ドメインの設定」

2） DNS に DKIM レコードを設定する
※ Biz メール＆ウェブプレミアムの DNS をご利用の場合は、DKIM レコードは標準で設定されます。
※ お客さまで用意した DNS をご利用の場合は、「2.4.3 DKIM レコードに設定する情報の確認」をご参照のうえ設定してください。

3） 「DNS サーバーの DKIM レコード設定」のステータスが［設定済］なことを確認する

4） DKIM 認証を「有効化」する

2.4.3. DKIM レコードに設定する情報の確認

1） 左メニュー「メールサーバー」の［送信ドメイン認証］から「DKIM」画面を開き、該当ドメインの［設定］をクリックします。

2） 「DKIM レコードの設定」画面が開きます。

■ **STEP 1** ：DNS サーバーに設定する DKIM レコードの情報を確認できます。

- **NAME（レコード名）** ：「bizmw._domainkey.*ドメイン名*」です。［コピー］が可能です。
- **TTL** ：数値は任意です（3600 は設定例）
- **VALUE（公開鍵）** ：［コピー］が可能です

■ STEP 2 ：DKIM レコードの設定状況を確認できます。

DNS に DKIM レコードを追加した後に［DKIM レコードを確認する］をクリックすると、ステータスが表示されます。

ステータスは以下の 3 種類です。

- 問題なく設定されている場合
  DKIM レコードが正しく設定されています。
- 未設定の場合
  DKIM レコードを確認できません。DNS サーバーの設定をご確認ください。
- 設定されている公開鍵が異なる場合
  DKIM レコードに設定されている公開鍵が正しくありません。DNS サーバーの設定をご確認ください。

> ⚠ 注意
>
> DKIM レコードを追記した後、DNS の設定が有効に機能するまで時間がかかる場合があるため、追記した後すぐに［DKIM レコードを確認する］を押すと、上記の**未設定の場合のステータス**が表示される可能性があります。

2.5. 受信サーバー設定

2.5.1. 受信サーバー設定の概要

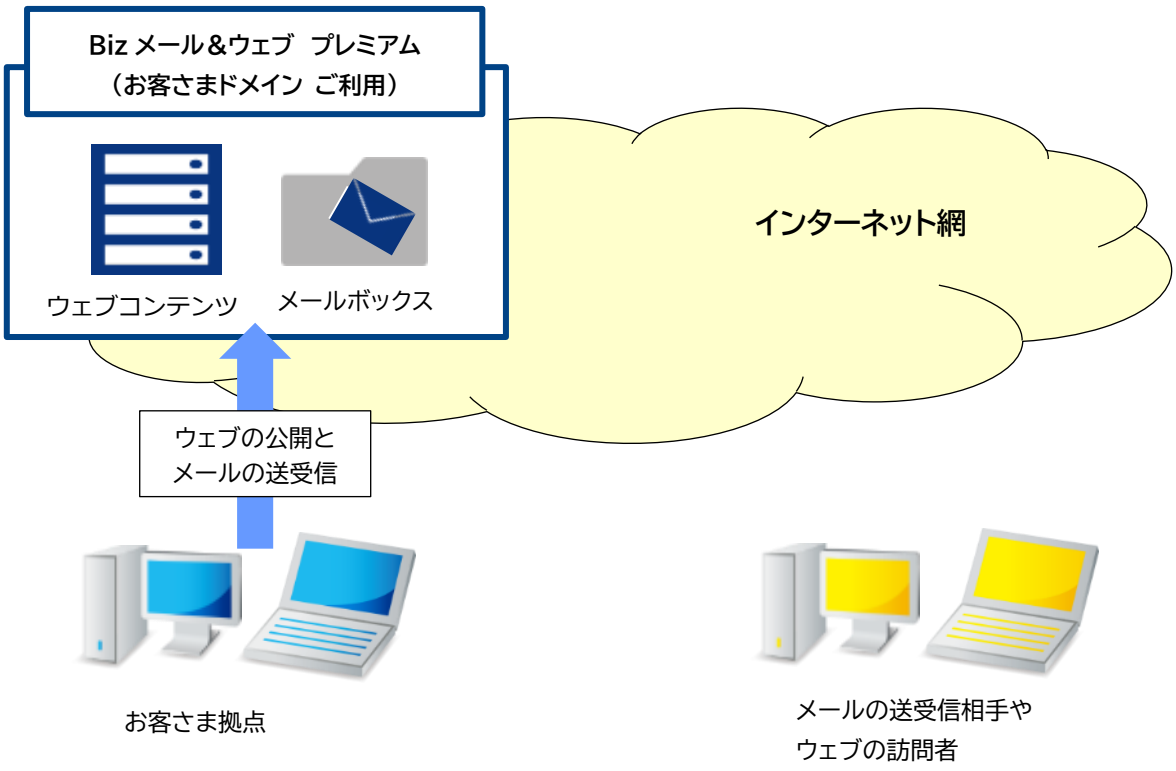
「受信サーバー設定」は、Biz メール＆ウェブ プレミアム サーバーのメール受信方法を変更する機能です。

メールサーバーを、本サービス以外（外部）のメールサーバーで利用する場合、本機能を利用して、Biz メール＆ウェブ プレミアム サーバーでメールを受信しないように設定することができます。

※ 本機能は、オプションサービス「迷惑メールフィルタリングサービス」をご使用でない場合に限り、有効になります。

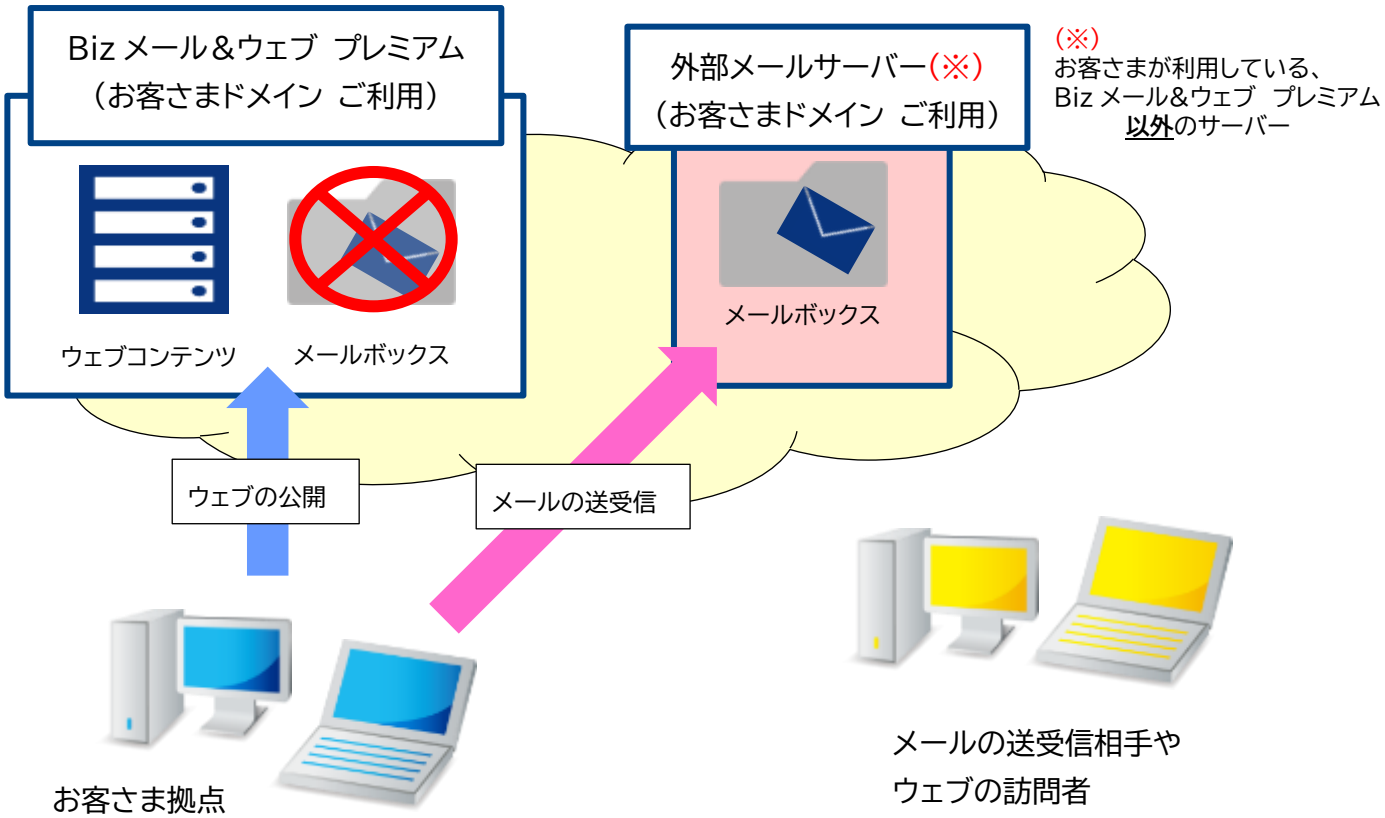
■ 通常のご利用時

Biz メール＆ウェブ プレミアムでは、標準で、ウェブコンテンツおよびメール送受信が利用できるように設定されています。このまま利用される場合は、設定の変更は必要ありません。



■ **設定変更が必要な場合**

Biz メール＆ウェブ プレミアム上でウェブサイトを運用し、メールは外部のメールサーバー(※)で運用する場合は、設定の変更が必要です。



アドバイス

外部のメールサーバーを利用する場合は、設定代行サービス「DNS ゾーン編集」のご利用をご検討ください。

※ DNS ゾーン編集の設定代行サービスのお申込み・よくあるご質問・注意事項については、以下のオフィシャルサイトをご参照ください。

※ お申込みの前に「よくあるご質問」を必ずご確認ください。

◆Biz メール＆ウェブ プレミアム　DNS ゾーン編集（設定代行サービス）

https://www.ntt.com/business/services/cloud/rental-server/vps/service25_03.html

または、別途お客さまにて DNS サーバーをご用意いただき、MX レコードの設定を変更していただく必要があります。

2.5.2. メール受信設定の変更

本機能で「ドメイン宛メール受信設定」を変更すると、外部のメールサーバーでメールの受信ができるようになります。設定手順を以下でご説明します。

※ 設定にあたり、以下の注意事項を必ずご確認ください。

注意

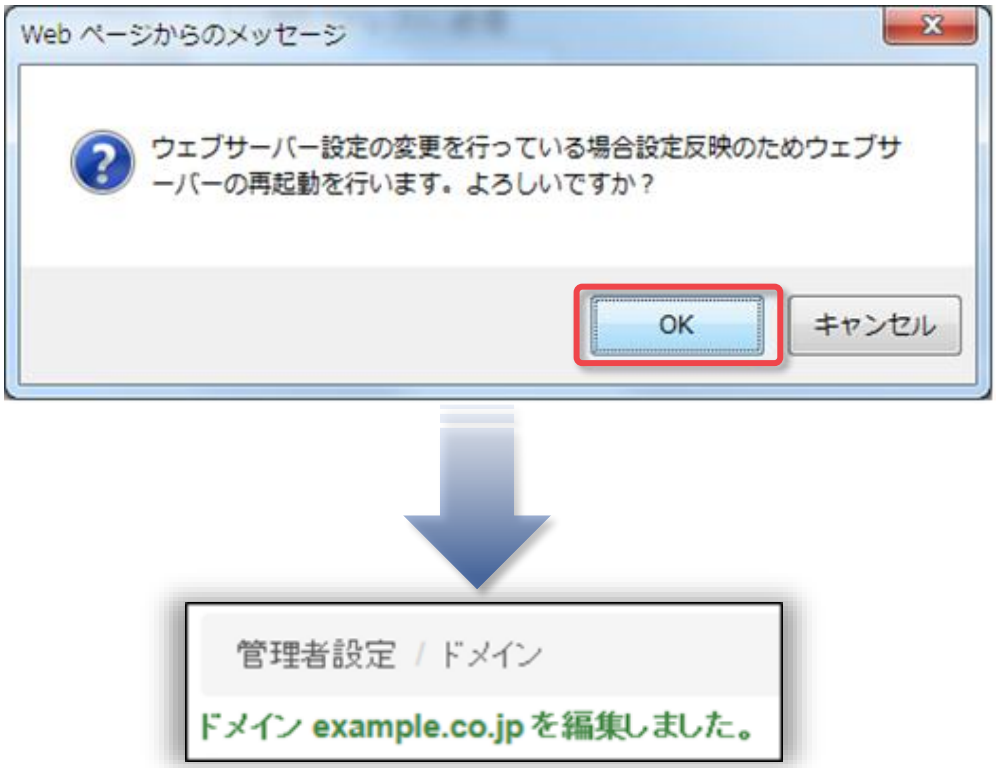
- 誤って本設定を実施した場合、本サービスのサーバーでメールの受信ができなくなります。内容をよくご理解いただいたうえ、十分ご注意ください。
- **外部メールサーバーを利用してメールを受信**する場合は、「本サービスのコントロールパネル」に登録している該当のメールアドレスを削除してください。
- **通常は外部メールサーバーを利用していて、Web フォーム（本サービスのウェブサーバー）からメールを送信**する場合は、「本サービスのコントロールパネル」に差出人のメールアドレスが存在している必要があります。

※ メールアドレスの削除/作成手順は「2.2 メールアドレス」をご参照ください。

1） コントロールパネル左メニューの［ドメイン］から「ドメイン管理」画面を開き、設定変更したいドメインの［設定］をクリックします。

2） 「メールサーバー設定」欄で、「ドメイン宛メール受信設定」の［ドメイン宛のメールを受信する］のチェックを外して、［保存］をクリックします。

3） ウェブサーバーの再起動を行う旨のダイアログが表示されたら、［OK］をクリックしてください。
「ドメイン～を編集しました。」と表示されたら、設定変更完了です。



2.6. メール分析

2.6.1. メール分析の概要

設定したキーワードをもとに集計と分析を行い、結果を表示させることによって業務推進やリスクなどの把握が可能です。

項目	種類	説明
傾向分析	分析ワード出現数の推移	設定した分析ワードが含まれていた出現数の推移を表示します。
	関連ワード	分析ワードのいずれかと一緒に出現する語句を、関連ワードとして表示します。
	関連ワードの出現分布	関連ワードの出現数の分布をカレンダーで表示します。
ページ分析	最近の関連メール一覧	分析ワードを含むメールの概要を表示します。 （日時・送信者・宛先・件名・マッチ分析ワード）
訪問者分析	メール送受信の関係者マップ	分析ワードを含むメールの送受信関係図を表示します。

アドバイス

各項目の詳細な解説は、［解説］をクリックする事で確認できます。

2.6.2. メール分析のインストール

1） コントロールパネルの左メニュー「メールサーバー」から、[メール分析]をクリックします。

2） [ドメイン選択]のプルダウンから、メール分析をしたいドメインを選択します。

3） ドメインを選択した後、画面下部の［MySQL 管理パスワード］を入力してから、［インストール］をクリックしてください。

注意

- MySQL のパスワードが不明な場合は、MySQL のパスワードを変更してから、メール分析のインストールを行ってください。（参照：4.3.5 MySQL のパスワード変更）

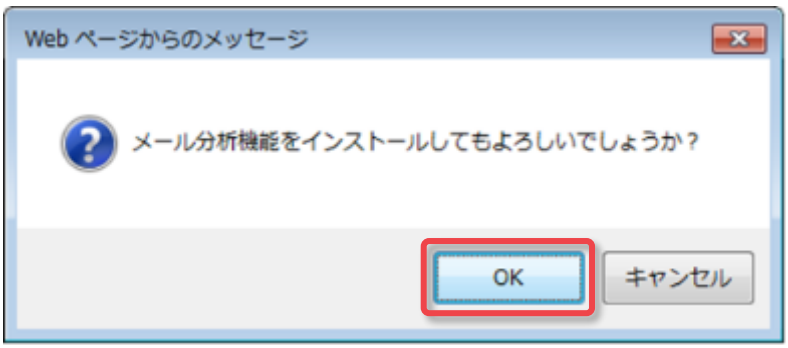
※ すでに MySQL を利用しているアプリケーションがある場合は、該当のアプリケーション側に設定している MySQL のパスワードも、変更後の新しいパスワードに修正する必要があります。

- メール分析機能のインストールを行う前に、MySQL を起動する必要があります。

※ MySQL が停止している状態でインストールをしようとすると、「MySQL is not running」と表示されます。
参照）4.3.2 MySQL の利用開始（初期化） *はじめて MySQL を起動する場合
4.3.3 MySQL の利用開始 *停止中の MySQL を起動する場合

- MySQL のバージョンについては 4.3.1 利用可能なデータベースをご参照ください。

4） 確認メッセージが表示されたら、［OK］をクリックしてください。
メール分析設定（分析ワードの設定）画面が表示されたら、インストールは完了です。



2.6.3. メール分析の設定

1） 「分析ワードの設定」画面の各設定項目を入力して、[保存]をクリックしてください。

	設定項目	説明
1	分析軸の名称設定	登録する分析軸名を入力します。 【登録可能数】5 つまで
2	分析ワード設定	受信メール本文中から抽出するワードを入力します。 【登録可能数】1 つの分析軸につき 5 つまで
3	関連ワード分析設定	登録した分析ワードと共に出現するワードを取得して、関連ワードとして分析結果に表示します。 ウェブやニュースなどで出る「新語や流行語」も関連ワードとして取得したい場合は、[追加の固有名詞辞書を利用する]にチェックを入れてください。
4	分析対象ユーザー選択	選択されたユーザーを対象に、メール着信時に分析が行われます。

2） 「分析軸の保存が完了しました。」と表示され、「分析軸」欄に、登録した名称が表示されたら完了です。

2.6.4. 分析軸の追加

ここでは、メール分析軸の追加方法をご説明します。

1） コントロールパネルの左メニュー「メールサーバー」から、[メール分析]をクリックして、右上の[設定]をクリックします。

2） メール分析設定画面で、[分析軸と分析ワードの追加]をクリックしてください。
各設定項目の内容については、「2.5.3 メール分析の設定」をご参照ください。

2.6.5. 分析軸の削除

ここでは、メール分析軸の削除方法をご説明します。

1） コントロールパネルの左メニュー「メールサーバー」から、[メール分析]をクリックして、右上の[設定]をクリックします。

2） メール分析設定画面が表示されたら、該当の「分析軸」のチェックボックスを選択して、[削除]をクリックします。

3） 確認メッセージが表示されたら、[OK] をクリックします。

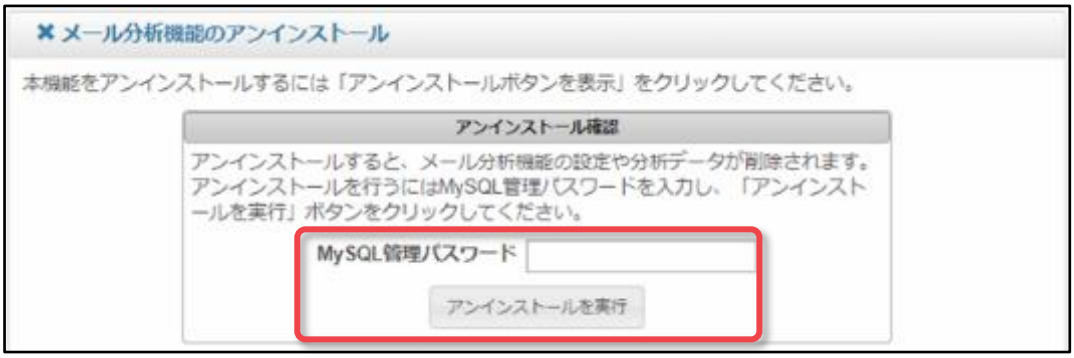
4） 「分析軸を削除しました。」と表示されたら、完了です。

2.6.6. メール分析のアンインストール

1） メール分析の画面で、アンイストールをするドメインを選択し、画面右上の［設定］をクリックします。

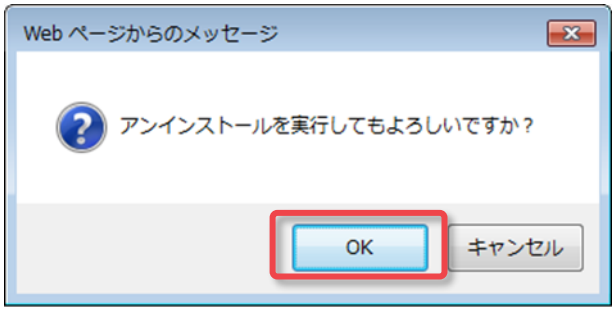
2） メール分析の設定画面で、［アンインストールボタンを表示］をクリックします。

3） アンインストール確認の［MySQL 管理者パスワード］を入力してから、［アンインストールを実行］をクリックします。



4） 確認メッセージが表示されたら、［OK］をクリックします。

5） 初期インストール画面が表示されたら完了です。



注意

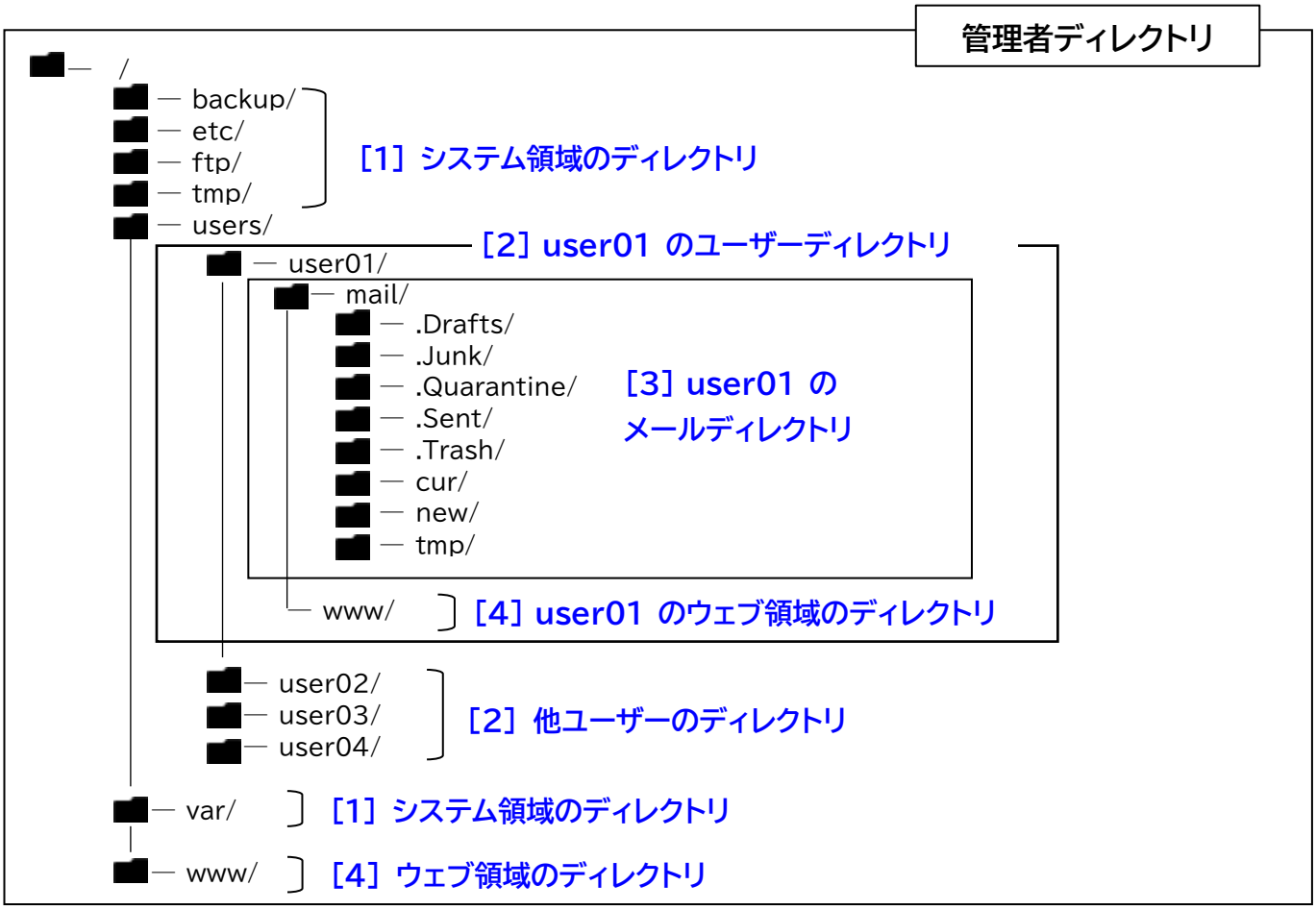
- メール分析ツールをアンインストールすると、それまで蓄積した分析データも削除されます。
- 本機能は、お客様のメール利用方法によってデータの表示分析結果が異なります。
  また、参考値となるため、データの精度を保証するものではありません。

3　ウェブサーバー

3.1. ディレクトリ構成

3.1.1. ディレクトリの概要

本サーバー内のディレクトリ構成を、次に示します。



- **システム領域のディレクトリ・・・[1]**
  サーバー運用上、必要なファイルが格納されるディレクトリです。

- **ユーザー領域のディレクトリ・・・[2]**
  利用者（ユーザー）固有のファイルが格納されるディレクトリです。

- **メールディレクトリ・・・[3]**
  利用者（ユーザー）のメールが格納されるディレクトリです。

- **ウェブ領域のディレクトリ・・・[4]**
  ウェブのコンテンツファイルをアップロードするディレクトリです

アドバイス

- ユーザーID(管理者用) でログインした場合は、全ての領域にアクセス可能です。
- 利用者のユーザーID でログインした場合は、**/user/<利用者のユーザーID>以下**のディレクトリのみ参照可能です。

注意

var 配下の領域に関しては、お客さまにて独自に操作は行えません。

3.1.2. システム領域のディレクトリ

システム領域の各ディレクトリについてご説明します。

- **/**
  システム領域の最上位のディレクトリ指定は / になります。
- **/backup/**
  「ウェブサーバー」の「サイトバックアップ」でバックアップしたファイルが格納されます。
  「サイトバックアップ」に関しては、「3.5 サイトバックアップ」を参照してください。
- **/etc/**
  各種アプリケーション(個別ルールなど) の設定ファイルが格納されています。
- **/tmp/**
  サーバー内で稼動する各種アプリケーションが、一時ファイルを作成するディレクトリです。
- **/var/**
  主に MySQL 関連のデータが格納されています。

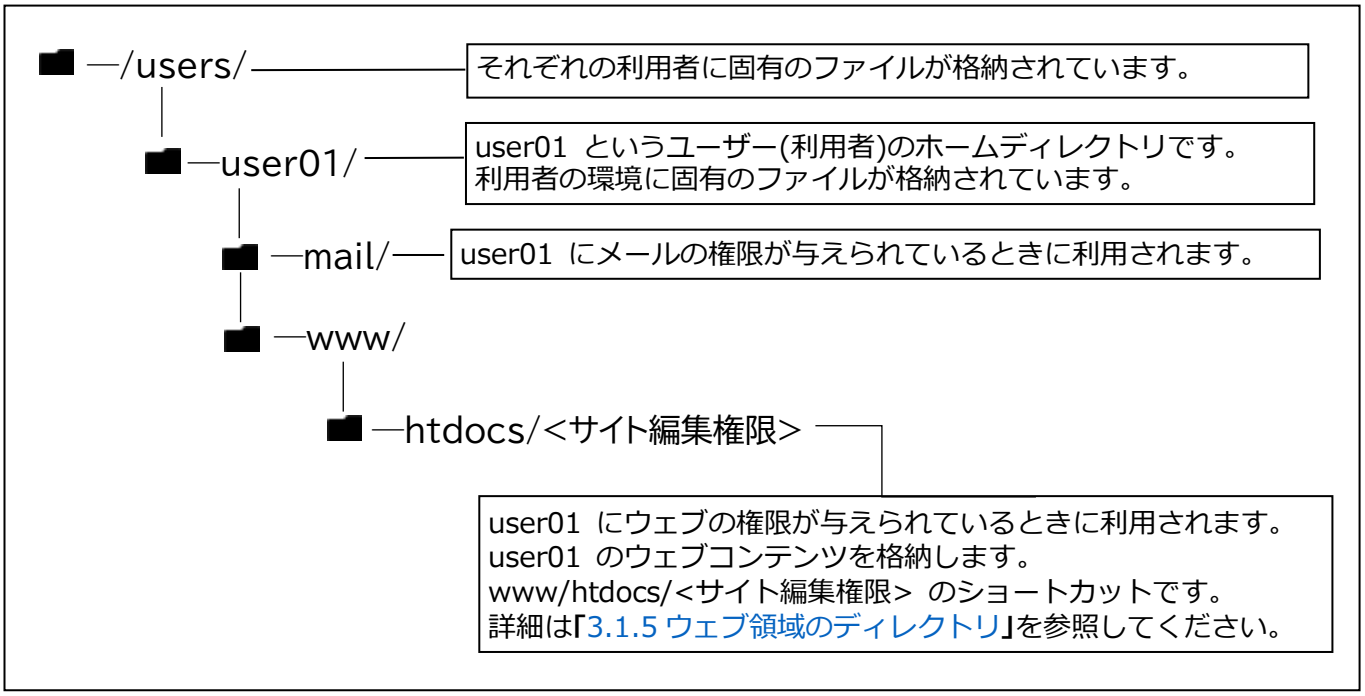
注意

- システム領域のディレクトリ、もしくはディレクトリ内のファイルを誤って削除・編集した場合、システムが正常に動作しなくなることがあります。
  FTP や、コントロールパネルの各種ツールにある「ファイルマネージャ」を使用してシステム領域のディレクトリにアクセスする場合には、十分に注意してください。
- 誤って削除・編集をして、システムの修復が必要になった場合は、ファイルマネージャの［復元ファイル］ からファイルを復元できる可能性があります。

※ ［復元ファイル］で復元されるのは、本サービスの日次バックアップ時点(午前 1 時～5 時ごろ) のファイルです。「復元ファイル」についての詳細は、『**利用者マニュアル**』を参照してください。

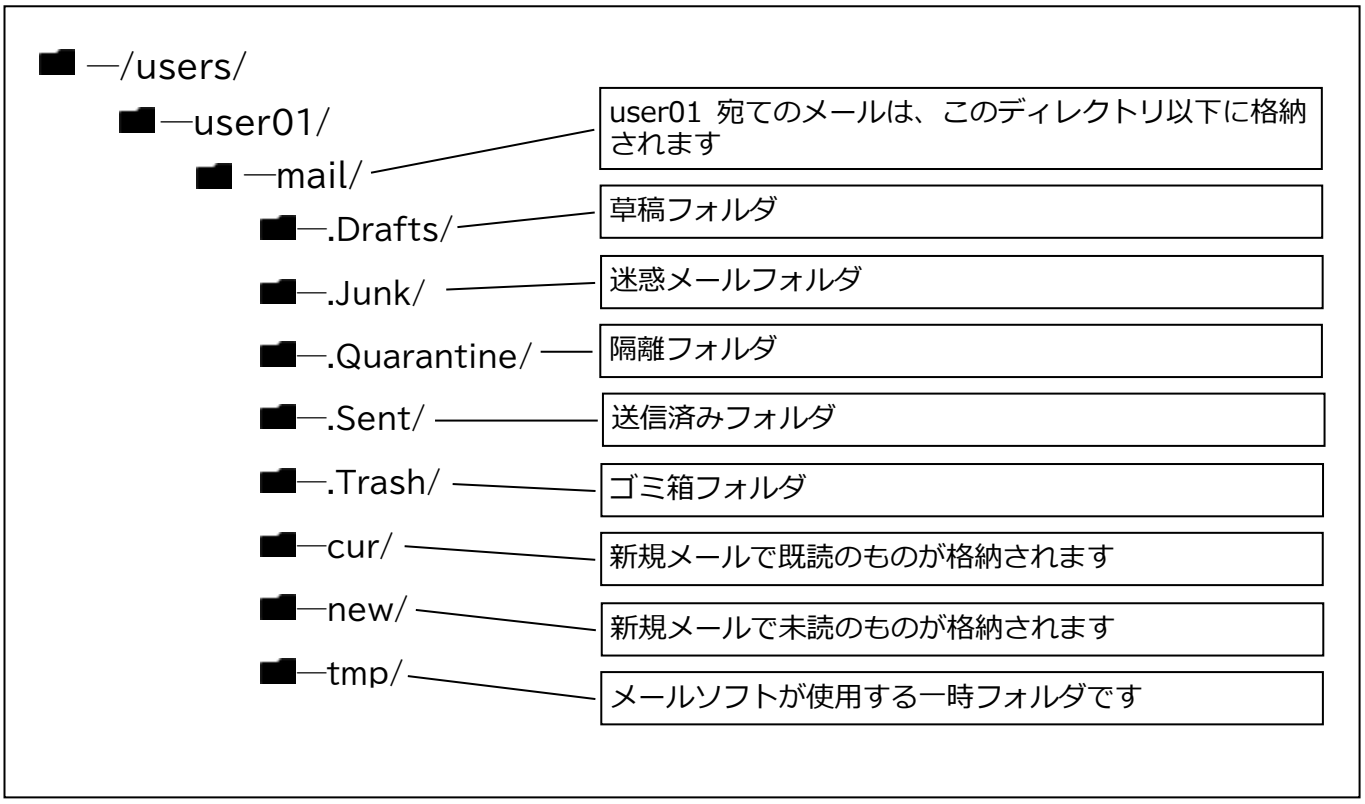
3.1.3. ユーザー領域のディレクトリ

ユーザー領域の各ディレクトリについてご説明します。



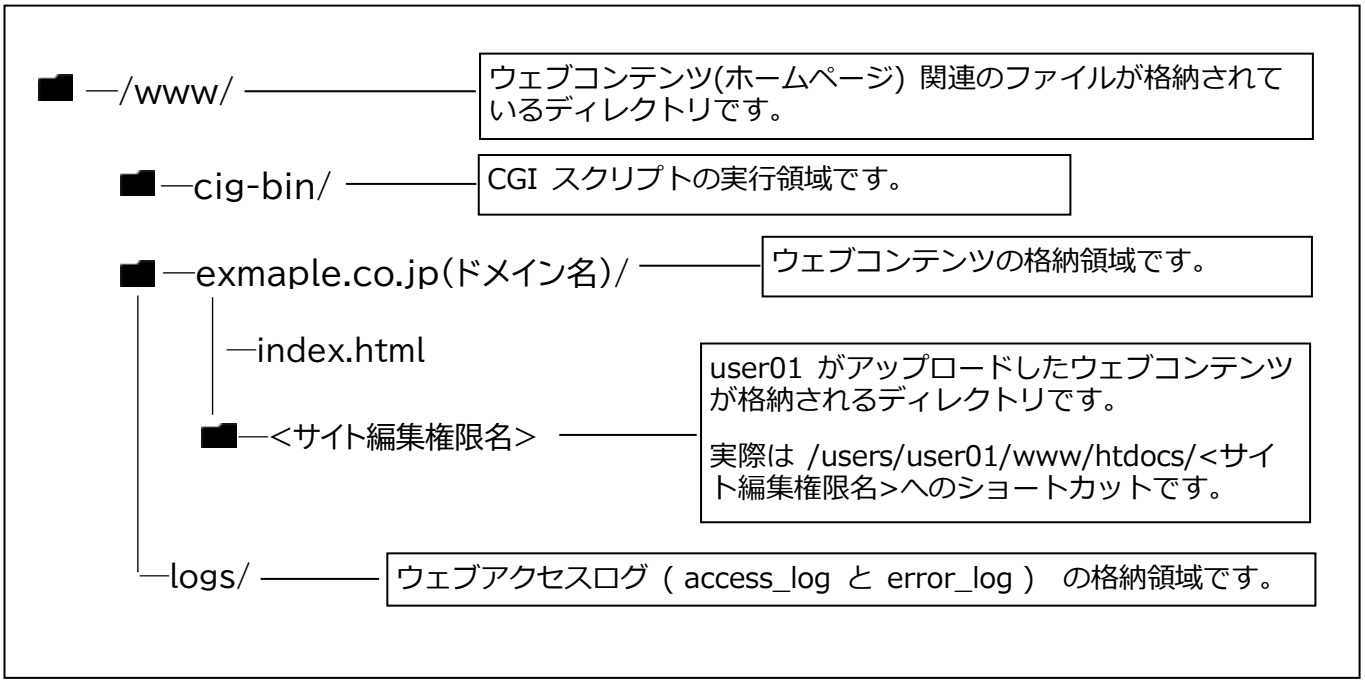
3.1.4. メールディレクトリ

メールディレクトリ内の各ディレクトリについてご説明します。



3.1.5. ウェブ領域のディレクトリ

ウェブ領域の各ディレクトリについてご説明します。



注意

- 各ディレクトリを削除された場合、正常にウェブコンテンツが表示されなくなりますので、削除しないでください。
- logs ディレクトリを削除された場合、ウェブに関するログが正しく生成されなくなりますので、削除しないでください。

「サイト編集権限」を持つ利用者のディレクトリについて

利用者にサイト編集権限が付与された場合、該当のユーザーディレクトリに、ウェブコンテンツを格納する領域が作成されます。

例えば、利用者「example」のサイト編集権限名を「example2」と設定した場合のウェブコンテンツディレクトリは、/users/example/www/htdocs/example2　となります。

また、 **/www/htdocs/<サイト編集権限名>** というシンボリックリンクが 作成されます。このショートカットは、**/users/ <ユーザーID> /www/htdocs/<サイト編集権限名>** へ格納されます。

※ サイト編集権限については、「3.4 サイト編集権限」をご参照ください。

アドバイス

サイト編集権限名が「test」、アップロードしたウェブコンテンツ名が「index.html」の場合、http://<お客さまドメイン>/test/ で閲覧することができます。

3.2. SSL/TLS 証明書

3.2.1. SSL/TLS 証明書 の概要

本サービスでは、お客さまのウェブサイトを SSL 通信でご利用いただくことができます。

SSL はインターネット上で安全にデータの送受信を行うための暗号化技術です。
SSL 通信とデジタル証明書を組み合わせることにより、お客さまサーバーとウェブブラウザ間で送受信されるデータを保護し、ウェブサイトから送信されるデータの送信元情報（ ウェブサイトの企業実在証明 *1 ） や、そのデータが送信中に改竄されていないかどうかを確認できます。

*1 グローバルサイン社のクイック認証 SSL は、企業実在証明はありません。

本サービスのサーバーには、c******.mwprem.net (例：biz123.mwprem.net ） に対応する証明書が、標準でインストールされています。
このため、クライアントコンピュータと各アカウントのコントロールパネルとの間では、証明書を活用した https による通信が可能です。

※「c******」は、『ご利用内容のご案内』に記載されている［ユーザ ID(管理者)］です。

※ マルチドメイン証明書/ワイルドカードなどはご利用できません。

注意

インストール済みの証明書は、mwprem.net の証明書であるため、お客さまが作成したウェブコンテンツの有効性や サイト運用する組織の信頼性を保証するものではありません。

お客さまドメインに対応するデジタル証明書を購入し、サーバーにインストールすることで、**お客さまドメインで https プロトコルによる通信環境**を確保し、**第三者による保証を受けたサイト**を運用することができます。

3.2.2. 利用可能な SSL/TLS 証明書

本サービスでは、次に示す証明書をご使用いただけます。

ドメインタイプ	内容	サーバー証明書	月額費用
本サービスで用意したホスト名	あらかじめ設定されたホスト名で SSL アクセスが可能です。 https://c******.mwprem.net/	**JPRS**	無料
独自ドメイン名(ホスト名) *1	お客さまの独自ドメイン名(ホスト名)で SSL アクセスが可能です。 https://独自ドメイン名(ホスト名)/	**デジサート** *3 ・セキュア・サーバ ID ・セキュア・サーバ ID EV ・グローバル・サーバ ID **ジオトラスト** *4 ・クイック SSL プレミアム **JPRS** *5 ・JPRS 組織認証型 ・JPRS ドメイン認証型 **グローバルサイン** *6 ・クイック認証 SSL ・企業認証 SSL	*2

*1 表にある証明書以外は、**サポート対象外**となります。

*2 本サービスではコントロールパネルを使用して、証明書をインストールできます。
コントロールパネルからのインストールに費用の発生はありませんが、証明書取得の費用については各証明書会社にお問い合わせください。

*3 デジサート 公式サイト：https://www.digicert.com/jp/
※ マネージド PKI 2048bit には対応していません

*4 ジオトラスト 公式サイト：https://www.geotrust.com/jp

*5 JPRS 公式サイト：https://jprs.jp/pubcert

*6 グローバルサイン 公式サイト：https://ocngs.globalsign.com/
※ グローバルサイン社が提供する各種オプション（ワイルドカード/イントラネット/期間カスタマイズ/グローバル IP など）には対応していません。

3.2.3. SSL/TLS 証明書のインストール作業について

デジタル証明書を本サーバーにインストールするには、以下３通りの方法があります。

1. 弊社に「セキュア・サーバ ID」「セキュア・サーバ ID EV」「クイック SSL プレミアム」「JPRS 組織認証型」「JPRS ドメイン認証型」の取得代行＋インストールをお申し込みいただく方法

   参照）3.2.4 SSL/TLS 証明書インストール（取得/設定代行）

2. 下表８種類のいずれかの証明書をお客さま自身で取得して、弊社にインストール作業をお申込みいただく方法

   参照）3.2.5 SSL/TLS 証明書インストール（設定代行）

3. 下表８種類のいずれかの証明書をお客さま自身で取得＋インストールする方法
   参照）3.2.6 SSL/TLS 証明書のインストール（お客さま作業による設定）

サーバー証明書		特長		導入手順の実施者		
証明書発行会社	製品名	暗号化強度	企業実在証明	CSR作成	発行会社申請	証明書設定
デジサート	セキュア・サーバ ID/セキュア・サーバ ID EV	最大256bit	○	弊社	弊社	弊社
				お客さま	お客さま	お客さま
	グローバル・サーバ ID	最大256bit	○	お客さま	お客さま	お客さま
ジオトラスト	クイック SSL プレミアム	最大256bit	×	弊社	弊社	弊社
				お客さま	お客さま	お客さま
グローバルサイン	クイック認証 SSL	最大256bit	×	お客さま	お客さま	お客さま
	企業認証 SSL	最大256bit	○	お客さま	お客さま	お客さま
JPRS	組織認証型	最大256bit	○	弊社	弊社	弊社
				お客さま	お客さま	お客さま
	ドメイン認証型	最大256bit	×	弊社	弊社	弊社
				お客さま	お客さま	お客さま

3.2.4. SSL/TLS 証明書インストール（ 取得/設定代行)

「CSR 作成」「証明書発行会社への申請」「証明書のインストール」などの面倒な手続きを、弊社がワンストップでご提供します。

各お申し込みの流れ等は、以下のページをご参照ください。

- デジサート SSL 証明書代行取得設定お申し込み｜Biz メール＆ウェブ プレミアム
  https://www.ntt.com/business/services/cloud/rental-server/vps/change_ssl_02.html

- ジオトラスト SSL 証明書代行取得設定お申し込み｜Biz メール＆ウェブ プレミアム
  https://www.ntt.com/business/services/cloud/rental-server/vps/change_ssl_03.html

- JPRS SSL 証明書代行取得設定お申し込み｜Biz メール＆ウェブ プレミアム
  https://www.ntt.com/business/services/cloud/rental-server/vps/change_ssl_04.html

3.2.5. SSL/TLS 証明書インストール（設定代行）

お客様にて証明書発行会社への申請を行っていただき、「CSR 作成」「証明書のインストール作業」を、弊社が代行いたします。

お申し込みの流れ等は、以下のページをご参照ください。

- SSL サーバー証明書代行設定お申し込み｜Biz メール＆ウェブ プレミアム
  https://www.ntt.com/business/services/cloud/rental-server/vps/change_ssl_01.html

「証明書の種類」「代行サービスの料金」「注意事項」等については、以下のページをご参照ください。

SSL サーバー証明書｜Biz メール＆ウェブ プレミアム
https://www.ntt.com/business/services/cloud/rental-server/vps/service11.html

3.2.6. SSL/TLS 証明書のインストール(お客さま作業による設定)

SSL/TLS 証明書の取得、設定を行う場合の手順について説明します。

（1）コントロールパネルから CSR の生成
（2）(1)の CSR を元に、SSL/TLS 証明書の購入
（3）コントロールパネルから SSL/TLS 証明書のインストール

（1）コントロールパネルから CSR の生成

① コントロールパネルの左メニュー「ウェブサーバー」から、[SSL/TLS 証明書] をクリックします。

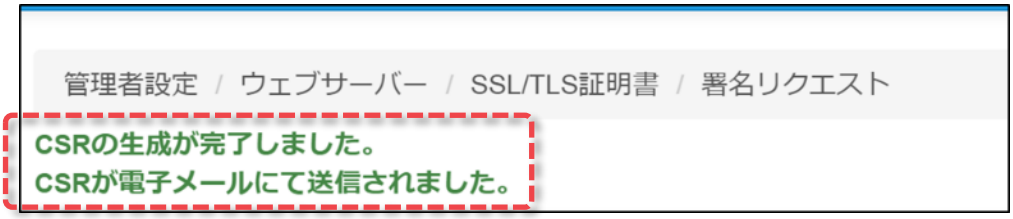
② インストールするドメインを選択して、「新しい証明書インストール」欄の、ステップ 1［署名リクエスト(CSR)生成］をクリックします。

③ 各項目を入力した後、［次へ］をクリックします。

注意

- 半角英数字および一部の記号「 -.,+/() 」以外は、ご利用いただけません。
- 日本語は使えません。

④ CSR の生成が完了して電子メールで送信された旨のメッセージが表示され、
作成済み CSR は、管理者のメールアドレスに送付されます。



※ ［送信先メールアドレス］に任意のメールアドレスを入力して、［CSR の内容を電子メールで送信する］をクリックすると、管理者以外のメールアドレスにも CSR 情報を送付できます。

⑤ 画面下部の［CSR 生成を終了］をクリックします。これで、CSR の作成は完了です。

アドバイス

- 作成された CSR のうち、デジタル証明書の手配に必要な部分は
「-----BEGIN CERTIFICATE REQUEST-----」(この行自身を含む)
から
「-----END CERTIFICATE REQUEST-----」(この行自身を含む)
までです。
- CSR の例は、次ページの「■作成された CSR」を参照してください。
- 証明書の手配に必要な CSR の要件については、各証明書会社に ご確認ください。
- Subject Alternative Name(SAN・SANs)を利用する際は、プルダウンメニューから対象のドメインを選択します。

(例) 「example.co.jp」と「www.example.co.jp」の両方で利用する場合は、
www.example.jp を選択します。

■作成された CSR

以下は、コントロールパネルで表示される、または管理者宛にメール送信される CSR 情報の例です。必要な部分について、紛失等しないようご注意ください。

```
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=JP、 ST=Tokyo、 L=Minato-Ku、 O=Verio APAC、
 CN=vjtest002.tempdomainname.com、 OU=Internet Section
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit) :
                    00:a9:91:82:07:22:c6:d3:8e:f7:38:99:e9:2e:bf:
                    7f:96:c7:c2:7a:5b:81:31:eb:66:a9:c7:6e:b9:91:
                    c4:39:68:34:01:3c:5f:26:71:28:87:ae:3d:3b:bd:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
                    15:25:09:63:a4:af:a0:7e:52:87:6e:75:02:22:9a:
                    4d:f0:13:46:47:d2:a2:e5:81:0f:9e:ff:c3:c1:57:
                    39:8f
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Algorithm: md5WithRSAEncryption
        a7:0d:8f:3a:97:ef:45:e8:a2:ef:6f:79:7d:a2:c6:73:eb:10:
        d1:41:7b:25:a8:77:50:2c:b3:88:8c:42:b2:cc:c9:6e:05:50:
        36:97:03:9b:78:bb:a7:ce:66:a4:2e:c1:2e:ad:0f:a7:31:b5:
        15:2a:45:21:bd:9b:a3:df:cd:6e:a9:27:b0:a4:a1:1b:bd:5d:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:XX:
        da:1a:b8:6d:d7:33:37:be:b0:5f:d8:cb:59:e5:4b:eb:2a:df:
        72:d4:7f:91:e6:ac:8c:e6:5b:46:45:67:ef:89:68:b1:87:11:
        65:da:49:c1:d0:61:88:31:b3:aa:0c:b7:aa:1f:da:8e:34:9a:
        ae:83:da:11
```

デジタル証明書の手配に必要な部分


```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwgYgxCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVUb2t5bzESMBAG
A1UEBxMJTWluYXRvLUt1MRMwEQYDVQQKEwpWZXJpbyBBUEFDMSUwIwYDVQQDExx2
anRlc3QwMDIudGVtcGRvbWFpbm5hbWUuY29tMRkwFwYDVQQLExBJbnRlcm5ldCBT
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
YGtfjwpmqMhkfjqI9t2fim4P+MUgKmNc3/Y8AF+sviPDfLEgpqcI49oauG3XMze+
sF/Yy1nlS+sq33LUf5HmrIzmW0ZFZ++JaLGHEWXaScHQYYgxs6oMt6of2o40mq6D
2hE=
-----END CERTIFICATE REQUEST-----
```

（2）デジタル証明書の購入

「(1)コントロールパネルから CSR の生成」で作成した CSR を元に、証明書会社から、デジタル証明書を購入します。証明書会社によっては、デジタル証明書のことを「サーバー証明書」と呼ぶことがあります。

購入したデジタル証明書の例を、次に示します。

◆サーバー証明書

[オーダーID]　　CE200911225659
[コモンネーム]　www.example.com

インストールに必要な部分

```
-----BEGIN CERTIFICATE-----
MIIEeTCCA2GgAwIBAgILAQAAAAABJRn2bmgwDQYJKoZIhvcNAQEFBQAwbDEkMCIG
A1UECxMbT3JnYW5pemF0aW9uIFZhbGlkYXRpb24gQ0FUMRMwEQYDVQQKEwpHbG9i
YWxTaWduMS8wLQYDVQQDEyZHbG9iYWxTaWduIE9yZ2FuaXphdGlvbiBWYWxpZGF0
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
L+MTvU8QX1f/SXXvAyMu/AHQwndvZi5ZyjsAWkUwm2Oy8T8WBe3mzJrWE4qkykQr
os6qgJQWW6DT5GFYlf7zSa1RBTfLIv4haHAJ0IhKOSYjn/eGdgVY300Eaegcapvv
4vGeuJjFKym50hU1hbu+If05u5bhq3EOc9i6sqkT3pGcAPTWcPUbP2RcjNGq
-----END CERTIFICATE-----
```

アドバイス

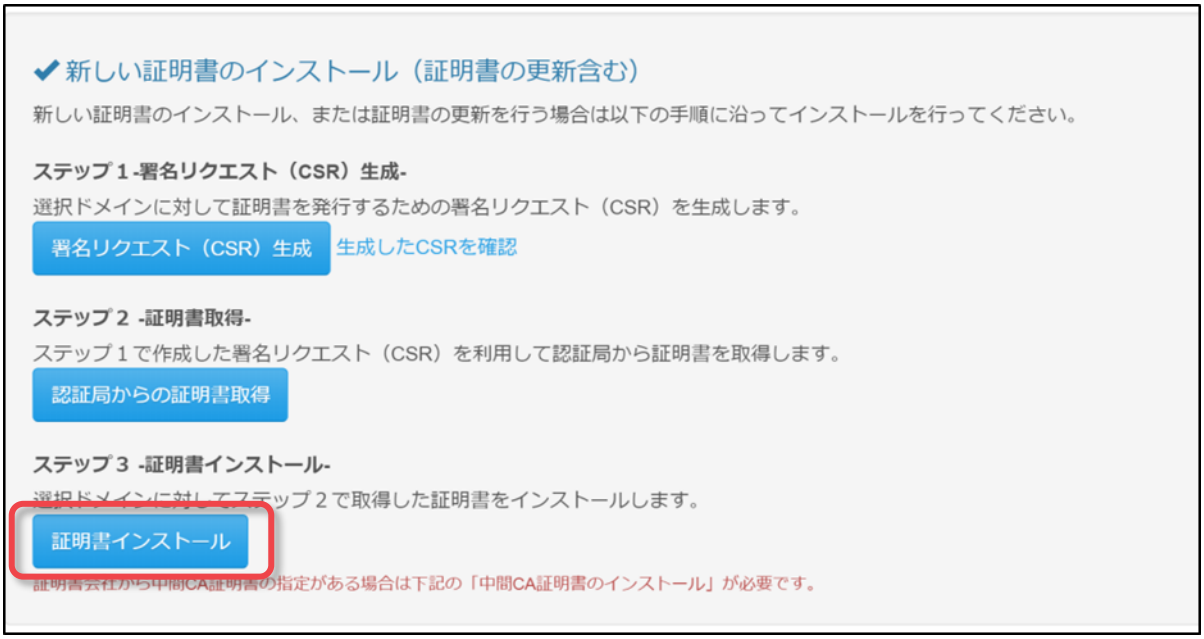
- デジタル証明書のインストールに必要な部分は
  「-----BEGIN CERTIFICATE -----」(この行自身を含む)
  から
  「-----END CERTIFICATE -----」(この行自身を含む)
  までです。

入手した証明書に該当する記述が見あたらない場合は、手配先の証明書会社にご確認ください。

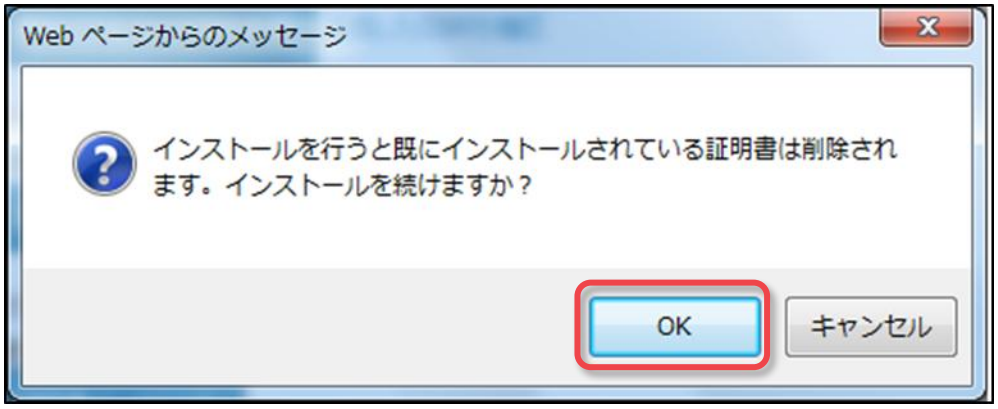
（3）デジタル証明書のインストール

「(2)デジタル証明書の購入」で入手したデジタル証明書を、本サーバーにインストールする手順をご説明します。

① コントロールパネル左メニュー「ウェブサーバー」から、「SSL/TLS 証明書」の画面を開き、ステップ 3 の［証明書インストール］をクリックします。



② 確認メッセージが表示されたら、［OK］をクリックします。



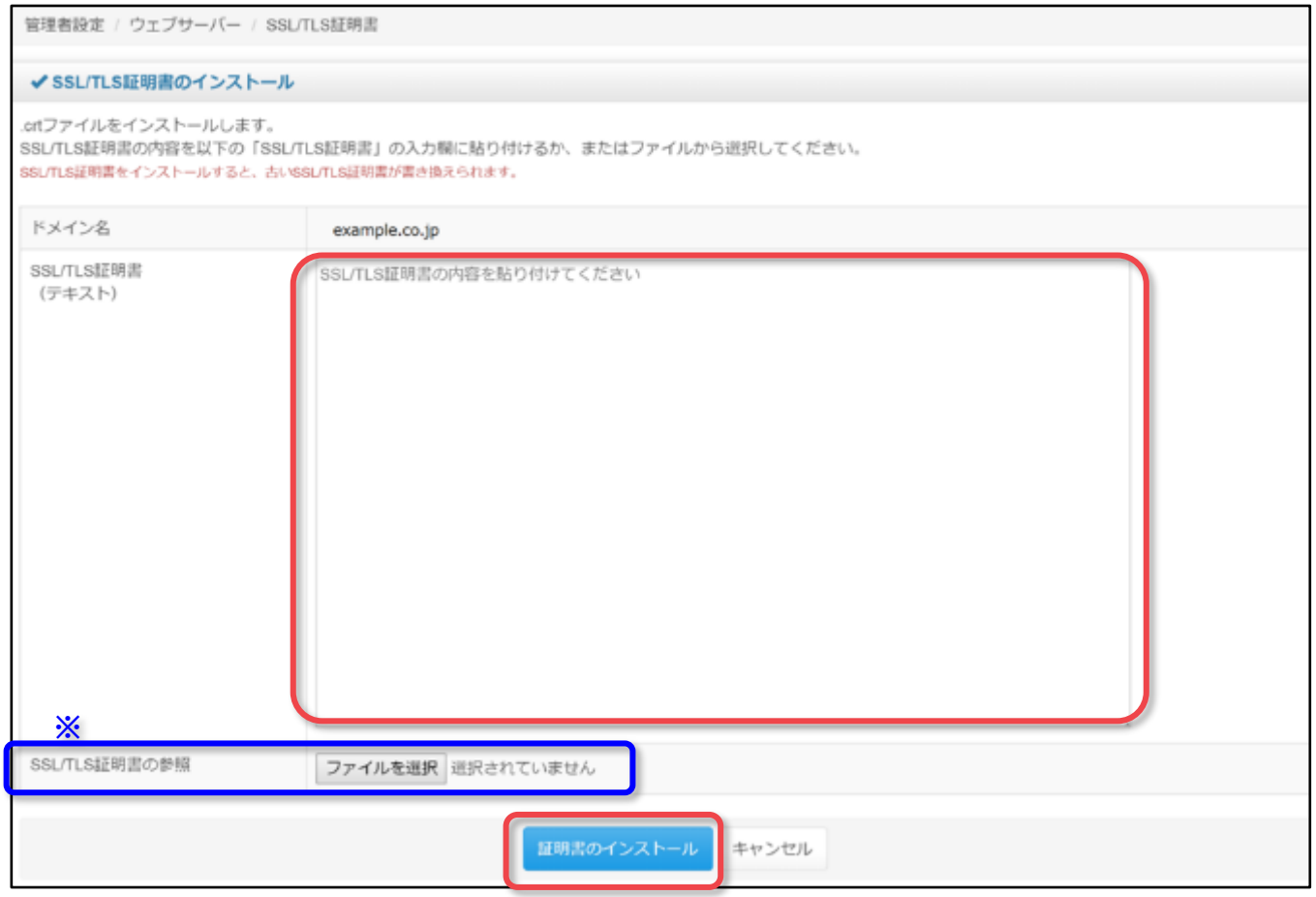
注意

インストールを行うことで、既にインストールされている証明書は削除されますので、十分に注意してください。

③ デジタル証明書を「SSL/TLS 証明書（テキスト）」欄に貼り付けます。

※ 「SSL/TLS 証明書の参照」の［ファイルを選択］から、デジタル証明書を選択することもできます。

デジタル証明書を入力/選択したら、［証明書のインストール］をクリックします。



アドバイス

- 送られてきた証明書に、「◆証明書◆中間証明書◆証明書＋中間証明書(PKCS7 形式)」の３つが存在する場合は、「証明書」のみを、インストール時に利用します。
- サーバー証明書の拡張子は、**.crt** または **.cer** です。
- サーバー証明書は、テキストエディタを利用して内容を確認できます。

④ 「SSL/TLS 証明書のインストールが完了しました。」と表示されたら、作業は完了です。
［ステータス］が「有効」となっている事を確認してください。

3.2.7. SSL/TLS 証明書の更新(お客さま作業による設定)

SSL/TLS 証明書には、有効期限が設定されています。継続してご利用される場合は、更新のお手続き、および更新費用が必要となります。また、更新を行う際は、再度コントロールパネルでの CSR の取得、サーバー証明書のインストールを行っていただく必要があります。

デジタル証明書の更新を行う場合の流れは次の通りです。

（1）コントロールパネルから CSR の生成
（2）(1)の CSR を元に、SSL/TLS 証明書の購入
（3）コントロールパネルから SSL/TLS 証明書のインストール

（1）コントロールパネルから CSR の生成

① コントロールパネルの左メニュー「ウェブサーバー」から、[SSL/TLS 証明書]をクリックします。

② インストールするドメインを選択してください。次に、「新しい証明書インストール」欄の、ステップ 1［署名リクエスト(CSR)生成］をクリックします。

注意

既に CSR を生成済みで、再度［CSR の生成］をクリックすると、以下のようなダイアログが表示されます。新しい CSR の生成を行うには、［OK］をクリックしてください。

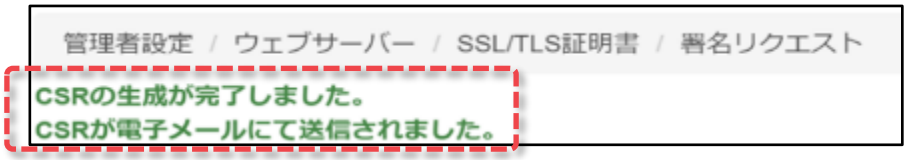
これにより、古い CSR は破棄されます。

③ 各項目を入力した後、［次へ］をクリックします。

注意

- 半角英数字および一部の記号「 -.,+/() 」以外は、ご利用いただけません。
- 日本語は使えません。

④ CSR の生成が完了して電子メールで送信された旨のメッセージが表示され、作成済み CSR は、管理者のメールアドレスに送付されます。



※ ［送信先メールアドレス］に任意のメールアドレスを入力して、［CSR の内容を電子メールで送信する］をクリックすると、**管理者以外のメールアドレスにも CSR 情報を送付**できます。

⑤ 画面下部の、［CSR 生成を終了］をクリックします。これで、CSR の作成は完了です。

アドバイス

- デジタル証明書の手配に必要な記述部分については、「3.2.6　SSL/TLS 証明書 インストール 」の「■作成された CSR」を参照してください。
- 証明書の手配に必要な CSR の要件については、各証明書会社に ご確認ください。

（2）デジタル証明書の購入

「3.2.6 SSL/TLS 証明書のインストール」の「(2)デジタル証明書の購入」を参考に、デジタル証明書の購入を行ってください。

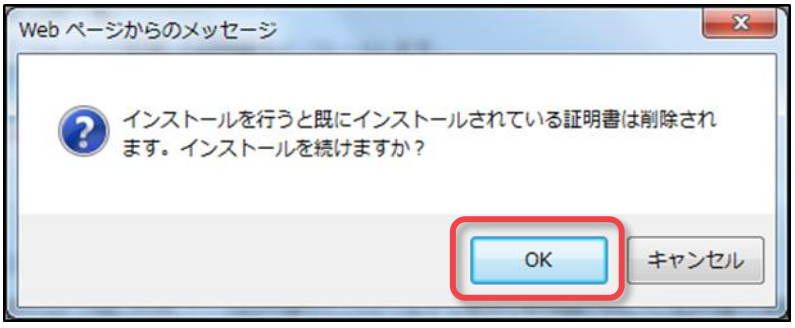
（3）デジタル証明書のインストール

「(2) デジタル証明書の購入」で入手した証明書を、本サーバーにインストールします。

① コントロールパネル左メニューの「ウェブサーバー」から、「SSL/TLS 証明書」の画面を開き、ステップ 3 の［証明書インストール］をクリックします。

注意

［署名済み証明書のインストール］をクリックすると、以下のようなダイアログが表示されます。新しい証明書のインストールを行うには、［OK］をクリックしてください。
これにより、古い証明書は破棄されます。



② 「3.2.6 SSL/TLS 証明書インストール」の「(3)デジタル証明書のインストール」を参考に、インストール作業を完了させてください。

3.2.8. 中間 CA 証明書について

Biz メール＆ウェブでは、当マニュアルに記載されている認証局から発行された証明書をご利用の場合は、中間証明書のインストールは不要ですが、
各社中間 CA 証明書の変更時期と、SSL 証明書を発行するタイミングとによっては、後段の手順で、お客さまご自身でインストールして頂く必要があります。

※ 中間 CA 証明書は、発行時に届く通知書のリンク先でダウンロードできますが、 ダウンロード先の記載が確認できない場合等は、以下の各社公式サイトをご参照ください。

- **デジサート** --- セキュア・サーバ ID/セキュア・サーバ ID EV、グローバル・サーバ ID
  https://knowledge.digicert.com/ja/jp/solution/SOT0009.html
- **ジオトラスト** --- クイック SSL プレミアム
  https://knowledge.digicert.com/ja/jp/solution/SOT0009.html

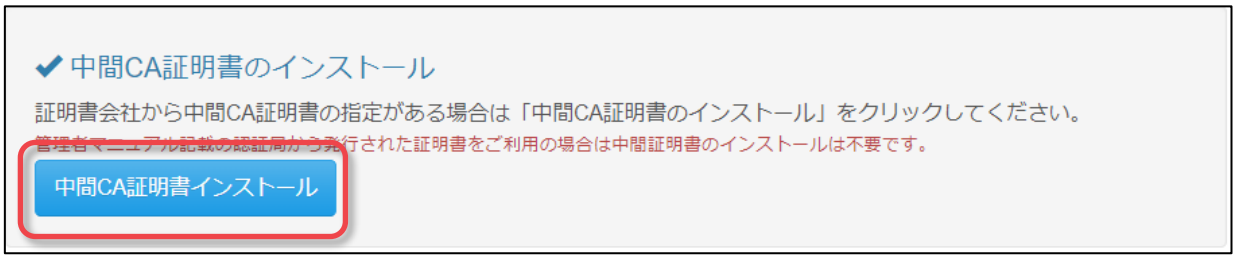
参考情報）中間 CA 証明書のダウンロードページ URL 変更のお知らせ｜デジサート
https://knowledge.digicert.com/ja/jp/alerts/ALERT2749.html

- **JPRS** --- 組織認証型、ドメイン認証型
  https://jprs.jp/pubcert/service/certificate/
- **グローバルサイン** --- クイック認証 SSL、企業認証 SSL
  https://jp.globalsign.com/repository/#root

中間 CA 証明書のインストール手順

① コントロールパネルの左メニュー「ウェブサーバー」から［SSL/TLS 証明書］をクリックして、「SSL/TLS 証明書の設定」画面でドメインを選択します。

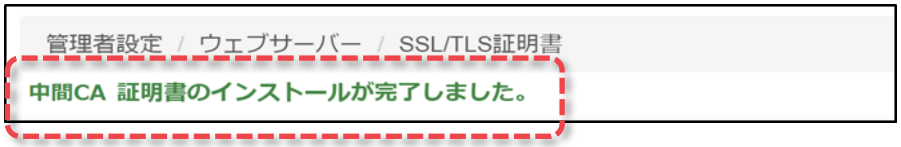
② 「SSL/TLS 証明書の設定」画面下部の［中間 CA 証明書のインストール］をクリックします。



③ 中間 CA 証明書を「中間 CA 証明書の入力」欄に貼り付け、［中間 CA 証明書のインストール］をクリックします。

※「中間 CA 証明書の参照」の［ファイルを選択］から、中間 CA 証明書を選択することもできます。

④ 「中間 CA 証明書のインストールが完了しました。」と表示されたら、作業は完了です。



3.3. サイトアクセス制限

3.3.1. アクセス制限の設定

本サービスでは、ホームページにアクセス制限をかけて、パスワードによるユーザー認証をご利用いただけます。
ユーザー認証を行うことで、会員専用のホームページなどを作成することができます。
アクセス制限を設定可能な領域は、htdocs 及び htdocs 配下の各サブディレクトリです。

ここでは、アクセス制限の設定方法をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイトアクセス制限] をクリックします。

2） 「ディレクトリ選択」プルダウンから、アクセス制限をかけるディレクトリを選択して、[ユーザー作成]をクリックします。

注意

ディレクトリ名やファイル名に利用できない文字種(日本語等)を利用していた場合は、プルダウンに目的のディレクトリ名等が表示されません。

※ 作成規則については『**セットアップマニュアル**』を参照してください。

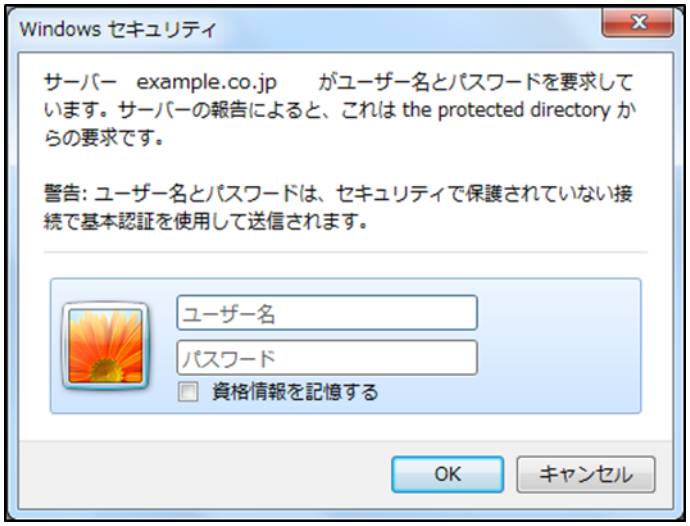
3）　［ユーザーID］と［パスワード］を入力して、［保存］をクリックします。

パスワードで利用可能な文字種や記号は以下の通りです。

・パスワードは８～３２文字の長さが必要です。
・英大文字、英小文字、数字、記号をそれぞれ１文字以上含む必要があります。
・パスワードに利用可能な記号は、次のとおりです。
　@ # $ % ^ * ( )　 _ + = - &

4） 「<ユーザーID>が現在のディレクトリに作成されました」と表示され、「ユーザーID」欄に作成したユーザーID が表示されていれば、完了です。

5） ウェブブラウザで該当ディレクトリの URL にアクセスすると、認証画面が表示されるので、正常にログイン出来ることを確認してください。



3.3.2. アクセス制限の解除

アクセス制限を解除する手順を、ご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、「サイトアクセス制限」画面を開きます。次に、［ディレクトリ選択］プルダウンから、アクセス制限を解除したいディレクトリを選択します。

2） 「ユーザーID」欄に、現在設定されているアクセス制限が表示されます。
［ステータス］が「利用中」となっている、制限を解除したいユーザーID を選択して、「操作」欄の［停止］ または［削除］をクリックします。

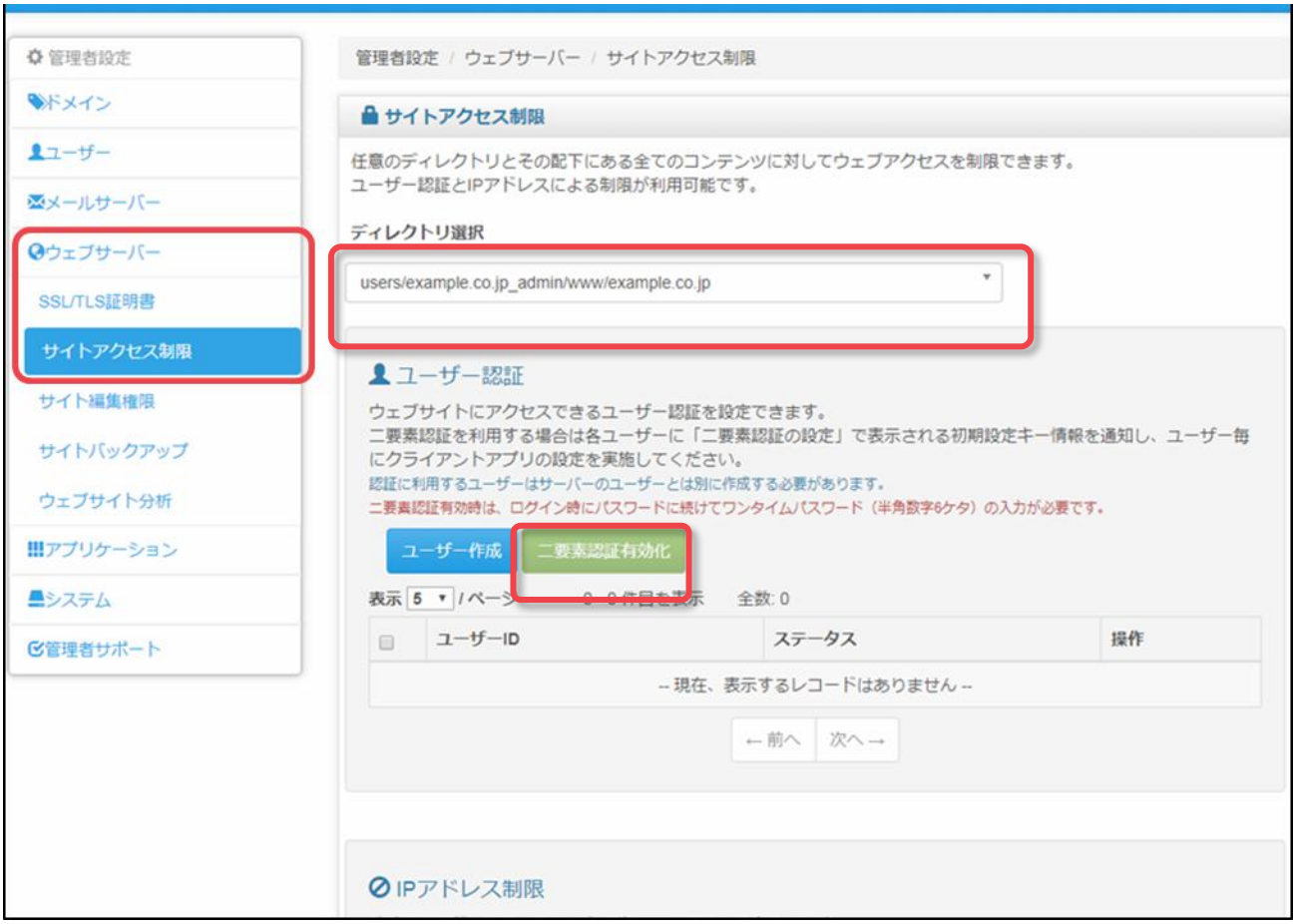
停止	該当ユーザーID でのアクセスを停止します。 必要な際には、再度有効化して利用することができます。
削除	該当ユーザーID が削除されます。

注意

アクセス制御を完全に解除するためには、ディレクトリに対して作成したユーザーID を全て「削除」します。ユーザーを「停止」するだけでは、認証画面が表示され、アクセス制御は解除されません。

3.3.3. 二要素認証による Web アクセス設定をする

1） コントロールパネルの左メニュー「ウェブサーバー」から、「サイトアクセス制限」画面を開きます。次に、[ディレクトリ選択] プルダウンから、二要素認証の設定を適応したいディレクトリを選択して、[二要素認証有効化] をクリックします。



2） 「3.3.1 アクセス制限の設定」で設定したユーザーの「操作」欄に追加された、[二要素認証の設定] をクリックします。

3） 通知先のメールアドレスを入力して、[指定したメールアドレスに案内を送信] をクリックします。

4） 「指定されたアドレスへメールを送信しました。」と表示されます。

アドバイス

メールによる通知機能を利用する事を推奨しますが、口頭やメモ等で通知して頂く方法でも、設定上の問題はありません。

5） 利用者の方に、クライアントアプリのインストールと設定を行っていただきます。
設定の手順は、それぞれ以下のページをご参照ください。

<iphone>
1.3.3 クライアントアプリのインストール(iPhone)
1.3.4 二要素認証の有効化(iPhone)

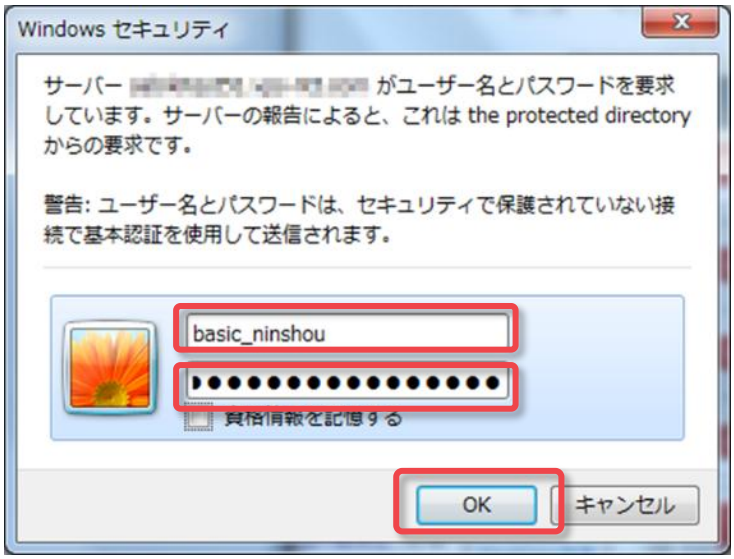
<Android>
1.3.5 クライアントアプリのインストール(Android)
1.3.6 二要素認証の有効化(Android)

注意

- 二要素認証を設定された利用者が iPhone/Android で「二要素認証の有効化」をする際、リンク先の手順２）～４）の「QR コードスキャン」はできません。
「QR コードが正常にスキャンできない場合」の方法で、本項の手順３）～４）で通知した『初期設定用認証キー』を入力するようお伝えください。

※ QR コードの読み取りができないクライアントアプリで「二要素認証の有効化」をする場合も、本項の手順３）～４）で通知した『初期設定用認証キー』を入力するようお伝えください。

6） 二要素認証を設定した Web サイトへ、正常にアクセスが可能か確認します。
ウェブブラウザでアクセスすると、下図のようにユーザー名とパスワードを要求する画面が表示されます。



次ページの「パスワード条件について」をご確認のうえ、**［ID］と［パスワード＋ワンタイムパスワード６桁］**を入力して、［OK］をクリックしてください。

パスワード条件について ※必ずご確認ください

二要素認証においては、「**3.3.1 アクセス制限の設定**」で設定した［ユーザーID］と［パスワード］に加えて、［ワンタイムパスワード 6 桁］を入力していただく必要があります。

==========

ID： 3.3.1 アクセス制限の設定 で作成した **ユーザーID**

パスワード: 3.3.1 アクセス制限の設定 で設定した パスワード ＋ ワンタイムパスワード 6 桁

==========

<入力例>

ID： **basic_ninshou**

パスワード： Sakusei&Password999999

3.3.4. IP アドレス制限の追加

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイトアクセス制限] をクリックします。次に、[ディレクトリ選択] プルダウンから、IP アドレス制限をかけるディレクトリを選択します。

2） 「IP アドレス制限」欄の［IP アドレス追加］をクリックします。

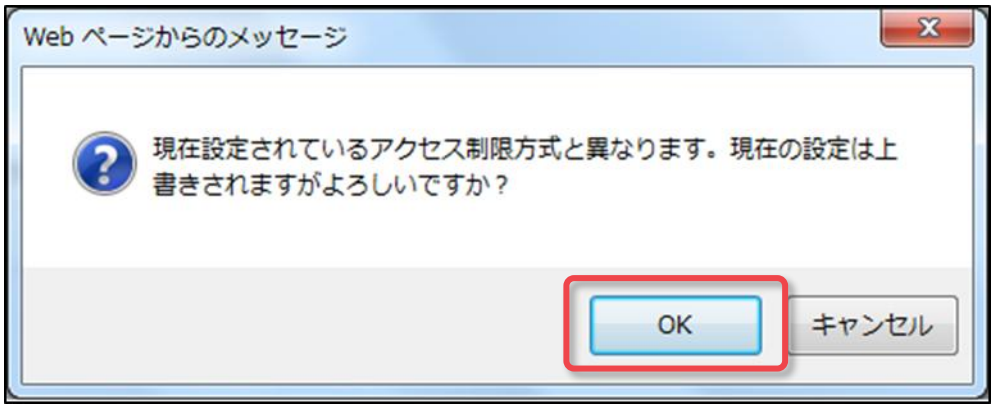
3） IP アドレス追加の画面が表示されたら、対象のディレクトリを確認して、各項目を入力した後、［保存］をクリックします。

項目	内容
ディレクトリ	IP アドレスを設定するディレクトリが表示されます。
IP アドレス／ サブネットマスク	許可/拒否したい IP アドレスを入力します。 ※ サブネットマスクの入力は必須ではありません。
アクセス制限方式	許可/拒否を選択します。

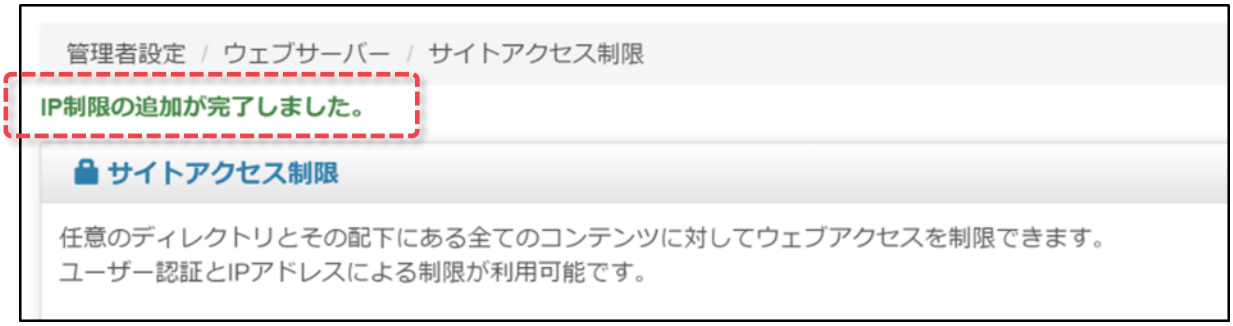
注意

- IP アドレスは静的(固定)　グローバル IP アドレスである必要があります。
- 本サービスの IP アドレスは設定しないでください。全サービスがご利用不可となる恐れがあります。
- 「127.0.0.1」を拒否する設定はしないでください。全サービスがご利用不可となる恐れがあります。
- IP アドレス、サブネット計算はサポート対象外となります。ウェブサイト等にてご確認ください。
- 許可/拒否、両方の設定は出来ませんのでご留意ください。
  (例) 許可設定を行っている場合、拒否を追加することによって許可設定は削除されます。

4） 確認メッセージが表示されたら、[OK] をクリックします。



5） 「IP 制限の追加が完了しました。」と表示されたら、完了です。



3.3.5. IP アドレス制限の削除・停止・再開

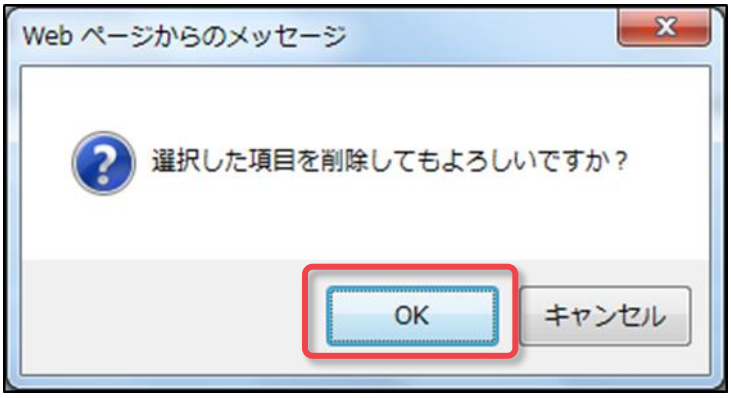
1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイトアクセス制限]をクリックします。次に、「ディレクトリ選択」プルダウンから、IP アドレス制限を処理（削除/停止/再開）するディレクトリを選択します。

2） 「IP アドレス制限」欄の「操作」から、処理を選択してください。

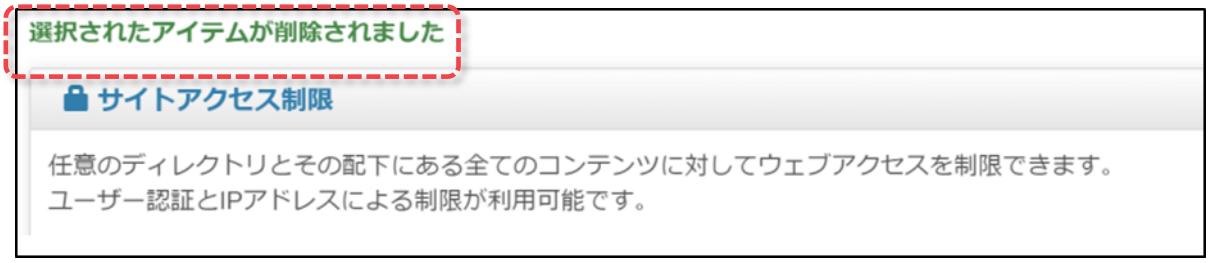
※ ここでは、「削除」を例としてご案内します。

項目	内容
削除	設定された IP アドレスを削除します。
停止	設定された IP アドレスの処理を停止します。
再開	設定された IP アドレスの処理を再開します。

3） 確認メッセージが表示されたら、［OK］をクリックします。



4） 削除完了のメッセージが表示され、一覧から該当の IP アドレスが削除されたら、完了です。



3.4. サイト編集権限

サイト編集権限を設定すると、外部公開可能なディレクトリが作成されます。お客さまのウェブサイトに、管理者以外の FTP とウェブの権限を有するユーザーが、ファイルをアップ ロードできるようになります。ユーザーは FTP などを使用して、指定されたディレクトリへファイルをアップロードすることが可能となります。

3.4.1. サイト編集権限の作成

新規サイト編集権限の作成手順をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイト編集権限] をクリックします。

2） 権限を付与したいユーザーを「権限付与ユーザー」のプルダウンから選択して、[新規作成] をクリックします。

注意

「サイト編集権限」を付与するユーザーには、あらかじめ「ファイル権限」を付与しておく必要があります。
※「ファイル権限」の付与は、ユーザー設定画面から設定できます。

3） 権限作成の画面が表示されたら、公開用のディレクトリ名を［URL］に入力して、［保存］をクリックします。 **※ 64 文字まで入力出来ます。**

4） 「ウェブサイト編集権限を追加しました。」と表示されたら、完了です。

3.4.2. サイト編集権限の確認

コントロールパネルの左メニュー「ウェブサーバー」から、［サイト編集権限］をクリックすると、登録されているサイト編集権限の一覧が表示され、確認することができます。

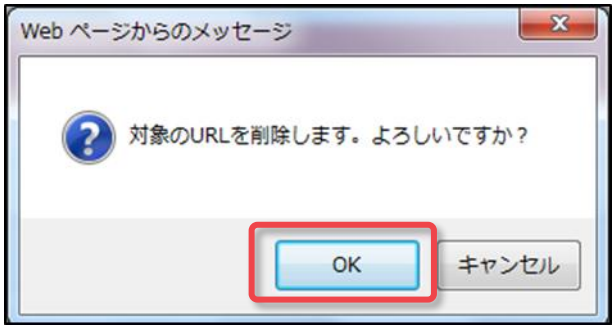
3.4.3. サイト編集権限の削除

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイト編集制権限]をクリックします。

2） 一覧が表示されたら、削除したい権限付与ユーザーの[削除]をクリックします。

※ 複数ユーザーにチェックを入れた際に上部に表示される[削除]をクリックすることで、**一括削除**も可能です。

3） 確認の画面が表示されたら、［OK］をクリックします。

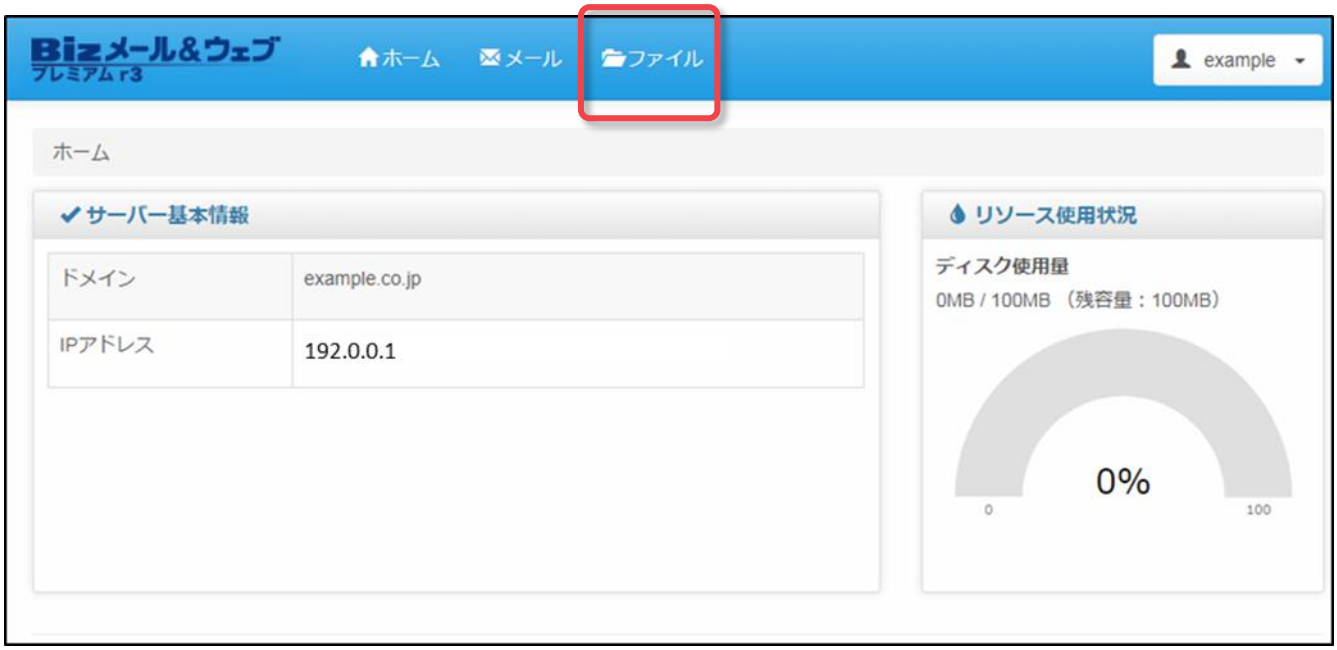


4） 削除完了のメッセージが表示され、一覧から該当の権限付与ユーザーが削除されたら、完了です。

3.4.4. サイト編集権限の利用方法

1） コントロールパネルに、サイト編集権限を付与した「ユーザーID」と「パスワード」でログインをします。

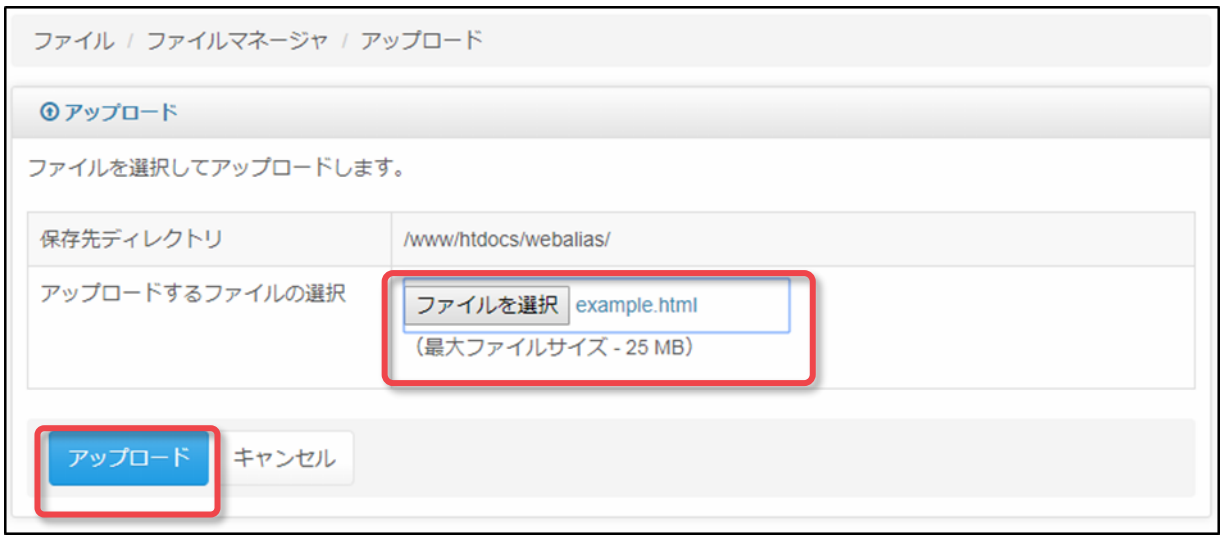
2） コントロールパネルの上部にある、［ファイル］をクリックします。



3） ファイルマネージャが表示されたら、「www」→「htdocs」→「サイト編集権限名」の順にクリックします。

4） ［アップロード］をクリックします。

5） アップロード画面が表示されたら、［ファイル選択］をクリックします。
アップロードしたいファイルを選択した後、［アップロード］をクリックしてください。



6） 「*＜ファイル名＞*が現在のディレクトリに保存されました。」と表示され、アップロードしたファイルが一覧に追加されたら、完了です。

アドバイス

アップロードしたファイルは、「http://*お客さまドメイン/サイト編集権限名*」で確認できます。

3.5. サイトバックアップ

3.5.1. バックアップの対象

「サイトバックアップ」は、管理者がウェブコンテンツや CGI スクリプトを手動でバックアップする機能です。

注意

バックアップの対象となるのは、**以下のディレクトリに限定**されます。
また、これらのディレクトリ配下に**実体が存在する**ものに限られます。

■独自ドメインの場合

/users/ドメイン管理者/www/独自ドメイン名/
/users/ドメイン管理者/www/cgi-bin/
/users/ドメイン管理者/www/htdocs/

■テンポラリドメインの場合

/www/cgi-bin/
/www/htdocs/

■■■ バックアップ対象にならない例 ■■■

- 利用者が、/users/<*ユーザーID*>/www/htdocs/<*サイト編集権限名*> にアップロードしたウェブコンテンツ
- 「/www/logs/」以下のファイル
- 「/www/」直下に格納された設定ファイル

アドバイス

「バックアップ」されたファイルは、ファイルの内容、ファイルのパーミッションが保存されます。

3.5.2. バックアップの作成

「サイトバックアップ」で、ウェブコンテンツをバックアップする手順をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイトバックアップ]をクリックします。

2） バックアップ対象のドメインを選択してから、[バックアップ作成]をクリックします。

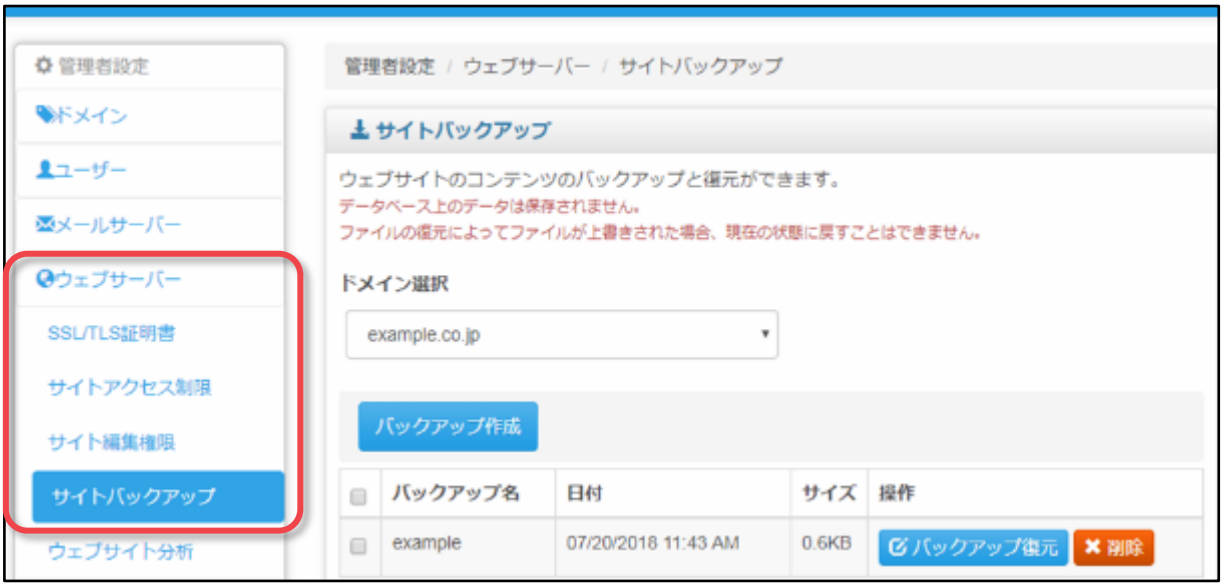
3） バックアップ作成の画面が表示されたら、[バックアップ名]を入力して、[作成]をクリックします。

4） 「新しいバックアップが作成されました。」と表示されたら、バックアップは完了です。

3.5.3. バックアップからの復元

「サイトバックアップ」でウェブコンテンツを復元する手順をご説明します。

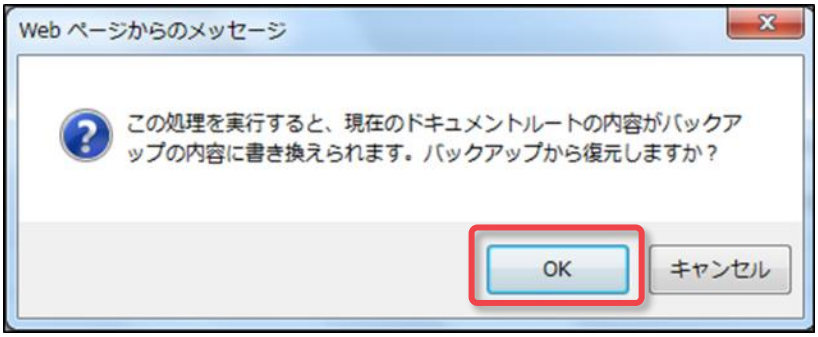
1） コントロールパネルの左メニュー「ウェブサーバー」から、「サイトバックアップ」をクリックします。



2） 復元するドメインを選択してから、［バックアップ復元］をクリックします。

z

3） 確認のダイアログが表示されたら［OK］をクリックします。



4）　「バックアップが復元されました。」と表示されたら、完了です。

注意

- 「バックアップからの復元」を実行すると、復元によって上書きされたファイルは、復元直前の状態に戻すことができなくなります。
- バックアップデータからの復元を行なう前に、「バックアップの作成」をしておくことをお勧めします。
- バックアップからの復元は、バックアップに含まれるファイルの追加のみ行なわれます。そのため、バックアップデータに対応するファイルがない場合、該当のファイルは削除されず、そのままの状態で残ります。

アドバイス

本サービスでは、次の 2 種類の方法でデータを復元することができます。

■ **バックアップ機能でバックアップされたデータの復元**

コントロールパネルの「ウェブサーバー」にある「サイトバックアップ」では、**/www/htdocs/**と**/www/cgi-bin/** 配下にあるディレクトリとファイルをバックアップしておくことができます。

このバックアップ機能については、本マニュアルの「3.5.2 バックアップの作成」と「3.5.3 バックアップからの復元(当項目)」を参照してください。

■ **コントロールパネルの「ファイルの復元」からの復元**

本サービスでは、外部記憶装置とは別に、約 1 日分のディスクバックアップを保存しています。

コントロールパネルの「ファイル」から［ファイルの復元］を実施することで、ディスクバックアップされたディレクトリもしくはファイルを復元できます。

※［ファイルの復元］については、**利用者マニュアルの「4.4 復元ファイル」**を参照してください。

3.5.4. バックアップデータの削除

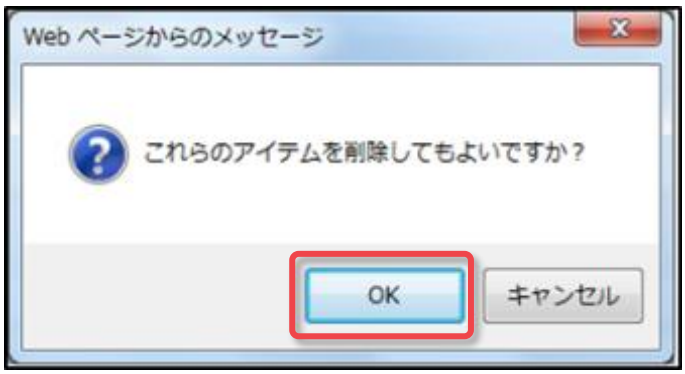
作成したバックアップデータを削除する手順をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[サイトバックアップ]をクリックします。

2） ドメインを選択してから、削除したいバックアップデータの［削除］ボタンをクリックします。

※ 複数のバックアップデータにチェックを入れた際に上部に表示される［削除］をクリックすることで、**一括削除**も可能です。

3） 確認メッセージが表示されたら、[OK] をクリックします。



4） 「バックアップが削除されました。」と表示され、一覧から該当のデータが削除されたら、完了です。

3.5.5. バックアップデータの格納ディレクトリ

バックアップデータは、次の位置に格納されています。

■ **index.txt**

バックアップデータのファイル名と表示名を関連付けるファイルです。
バックアップを作成すると、自動的に更新されます。

■ **バックアップデータの本体**

バックアップデータは **tar** と **gzip** でアーカイブ化されて格納されます。

> **注意**
>
> バックアップデータを削除する場合は、必ず「3.5.4 バックアップデータの削除」の手順で実施してください。
> **/backup/ ディレクトリから直接削除すると、正常に動作しなくなる可能性があります。**

3.6. WAF

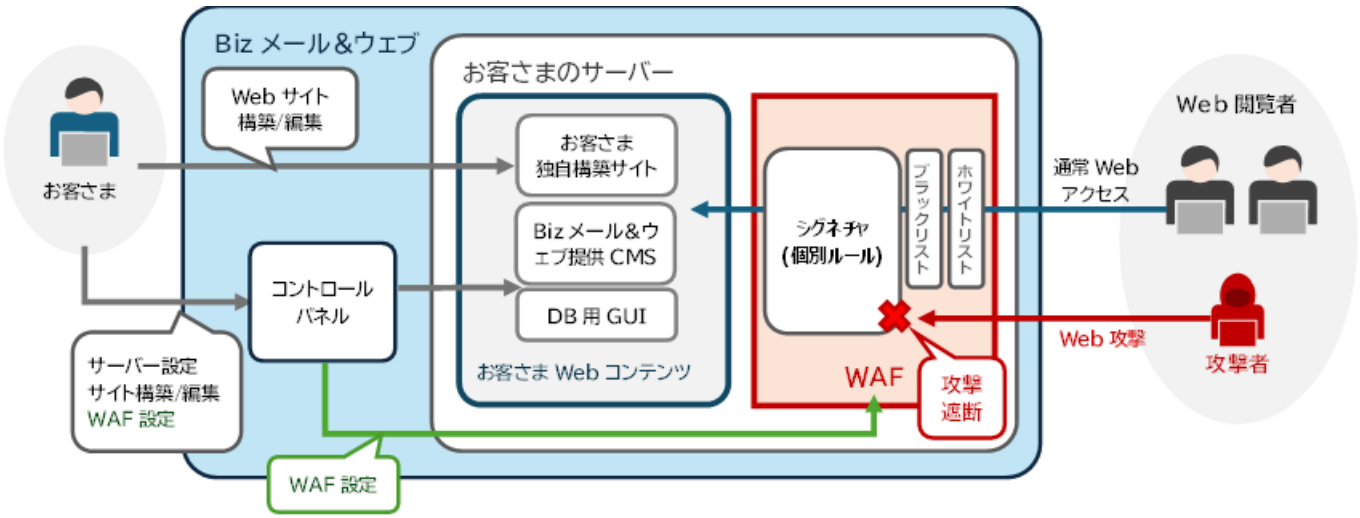
3.6.1. WAF の概要

WAF（Web Application Firewall）は、Web アプリケーションの脆弱性を悪用した攻撃や不正な通信から Web サイトを守るためのセキュリティ対策です。Web サイトにアクセスされる前に http/https（ポート 80/443）通信の中身をシグネチャ（攻撃パターン）をもとにチェックし、不正な通信を検知・ブロックするため、悪意のある攻撃からお客さまの WEB サイトを守り、情報漏洩や Web サイトの改ざんなどの被害を防ぎます。

※ WAF は Web アプリケーションに特化したセキュリティ対策のため、網羅的なセキュリティ対策としては、IDS/IPS、ファイアウォールといった他階層への攻撃を防御する対策と組み合わせて利用することが重要です。

Biz メール&ウェブの WAF の特徴

- 管理者は Biz メール&ウェブのコントロールパネルで、WAF の設定や検知結果の確認ができます。
- 「基本設定」では、用途に合わせて 3 つのモード（ブロック・検知・無効）を切り替えることが可能です。
- 「ホワイトリスト」「ブラックリスト」登録が可能なため、WAF 機能が有効な状態でも特定の送信元からのアクセスを制御できます。
- 「個別ルール設定」では、シグネチャで定義された各種攻撃パターンに対して、「ブロック」「検知」「無効」を切り替えることができます。



WEB サイトへ攻撃があった場合の WAF の挙動

WAF の「基本設定」で設定した動作モード（ブロック、検知、無効）と、各種設定（ホワイトリスト、ブラックリスト、個別ルール）の組み合わせによる WAF の挙動は、下表をご参照ください。

WL：ホワイトリスト　BL：ブラックリスト　WAF：検知結果
○：WEB サイトへのアクセス許可　×：WEB サイトへのアクセス拒否

基本設定	WAF の動作と用途	各設定時の挙動					
		WL 登録あり		WL 登録なし			
		BL 登録あり	BL 登録なし	BL 登録あり	BL 登録なし		
		WL または BL の登録が「あり」なので個別ルール(WAF のシグネチャ)は参照しません			個別ルール（ブロック）	個別ルール（検知）	個別ルール（無効）
ブロック	攻撃と判定されたアクセスをブロックするモード。 ※ WAF の初期設定完了後は本モードの利用を推奨します。 <主な用途> ・WEB サイトの実運用時	アクセス：○ ログ：WL	アクセス：○ ログ：WL	アクセス：× ログ：BL	アクセス：× ログ：WAF	__*1	アクセス：○ ログ：なし
検知	攻撃と判定されたアクセスを検知するモード。 ※ ブロックはしません。 ※ 検知ログを確認しながら WAF の設定を検証する場合等に利用します。 <主な用途> ・WAF の初期設定時 ・WAF の誤検知発生時	アクセス：○ ログ：WL	アクセス：○ ログ：WL	アクセス：○ ログ：BL	__*2	アクセス：○ ログ：WAF	アクセス：○ ログ：なし
無効	WAF(ホワイトリスト・ブラックリスト含む)を一時的に無効化するモード。 <主な用途> ・不具合の切り分け時	アクセス：○ ログ：なし	アクセス：○ ログ：なし	アクセス：○ ログ：なし	__*3	__*3	アクセス：○ ログ：なし

- 挙動の優先順位は、ホワイトリスト(WL) > ブラックリスト(BL) > 個別ルール の順です。
- ホワイトリストに登録があるアクセス元は「ログ：ホワイトリスト」に出力されます。
- ブラックリストに登録があるアクセス元は「ログ：ブラックリスト」に出力されます。
- ホワイトリスト/ブラックリストに登録がなく、攻撃と判定されたアクセス元は「ログ：検知結果」に出力されます。

※　「基本設定」または「個別設定」が［無効］の場合は、ログに出力されません。

*1 基本設定がブロックモードの場合は、個別ルールに［検知］ボタンは表示されません。

*2 基本設定が検知モードの場合は、個別ルールに［ブロック］ボタンは表示されません。

*3 基本設定が無効モードの場合は、個別ルールに［ブロック］および［検知］ボタンは表示されません。

提供機能

機能	詳細
WAF の 検知・ブロック	シグネチャにより通信内容をチェックし、攻撃と判定されたアクセスの検知・ブロックを行います。
検知結果 （一覧表示）	「WAF の検知結果[*1] ログ」「ブラックリストのログ」「ホワイトリストのログ」の 3 種類を切り替えて表示します。 ※　ログの容量上限は 1GB 程度（3 種類のログの合計）です。 最長保存期間は 1 年です。 ※　ブラックリスト・ホワイトリストに設定している IP アドレスからアクセスがあった場合は、WAF の検知前にブロックまたは許可の判断がされるため、ホワイトリスト・ブラックリストのログに出力されます。WAF の検知結果には表示されません。 [*1] WAF のシグネチャで攻撃と判定されたログ
検知結果 （詳細表示）	「WAF 検知結果一覧」に表示される各ログの詳細を個別に表示します。 検知内容の詳細を確認できる他、検知した攻撃に対する個別のルール設定やアクセス元 IP アドレスをブラックリスト・ホワイトリストに登録/削除することが可能です。
WAF 基本設定	WAF を利用するモードを設定できます。 モードは「ブロック」「検知」「無効」の 3 つから選択可能です。 WEB サイトの通常運用時は「ブロック」でのご利用を推奨します。 **<WAF の動作と主な用途>** ● ブロック：WAF で検知した攻撃をブロックするモード ※ WEB サイトの実運用時は基本的に本モードの利用を推奨します。 ● 検知　：WAF で攻撃を検知するモード(ブロックは行わない) ※ WAF の初期設定や動作検証の際に利用します。 ● 無効　：WAF の機能を無効とするモード ※ WAF の機能を一時的に無効化したい場合に利用します。
個別ルール設定	シグネチャで定義された攻撃パターンが一覧で表示されます。 各攻撃パターンに対して、「ブロック」、「検知」、「無効」の設定が可能です。 ※基本設定「ブロック」の場合の個別ルールの初期設定は、すべて「ブロック」となります。 ※基本設定「検知」の場合の個別ルールの初期設定は、すべて「検知」となります。
ホワイトリスト 設定	特定の IP アドレスからのアクセスはすべて安全なものとみなし、WAF の検知も不要としたい場合は、ホワイトリストに IP アドレスを追加することで実現が可能です。 ※　テキストファイルをインポートして一括登録することも可能です。 ※　登録数（推奨値）：3000 ※　ブラックリストよりホワイトリストが優先されるため、両方に同じ IP アドレスが登録されていた場合は、その IP アドレスからのアクセスはすべて許可されます。
ブラックリスト 設定	特定の IP アドレスからのアクセスはすべて安全でないものとみなし、WAF の検知もさせずにすべてのアクセスをブロックしたい場合は、ブラックリストに IP アドレスを追加することで実現が可能です。 ※　テキストファイルをインポートして一括登録することも可能です。 ※　登録数（推奨値）：3000 ※　ブラックリストよりホワイトリストが優先されるため、両方に同じ IP アドレスが登録されていた場合、その IP アドレスからのアクセスはすべて許可されます。

注意事項

- コントロールパネルに登録されているドメインに対して WAF のご利用が可能です。
- メールの送受信は WAF の検知対象外です。
- WAF の検知はシグネチャと照合して行うため、お客さまの Web サイトに対するすべての不正な通信や攻撃を検知/遮断するものではありません。
- 「基本設定」の初期設定は「検知」モードになっています。WAF で検知した攻撃をブロックするには、「基本設定」を「ブロック」モードに変更する必要があります。
- WAF のログを蓄積するため、ディスク容量を 1GB 程度空けたうえでご利用ください。
  ※ 1GB の空きがない場合、蓄積できるログが少なくなります。
  ※ 容量の空きが全くない場合は書き込みに失敗するため、ログの蓄積および表示はされません。
  ※ ログは合計「1GB」を上限として保持され、保存期間は 1 年です。容量を超えるまたは保存期間を超えたログは、新しいログで上書きされます。
- サービスの初期化をした場合は、WAF の設定や過去のログは全てリセットされます。

3.6.2. WAF の有効化

1） コントロールパネルに管理者でログインします。

2） 左メニュー「ウェブサーバー」から［WAF］をクリックして WAF 画面を開きます。

- 有効化前の WAF 画面では、WAF オプションのご契約の有無と MySQL の状態に合わせて以下のメッセージが表示されます。

メッセージ： MySQL が利用開始されていません

MySQL を一度も利用していない場合に表示されます。
この場合は、**手順3)**に進んでください。

メッセージ： MySQL が起動していません

MySQL が停止中の場合に表示されます。
この場合は、**手順8)**に進んでください。

メッセージ： WAF 機能が有効化されていません

MySQL が起動している場合に表示されます。
この場合は、**手順12)**に進んでください。

メッセージ： WAF オプションのご契約がないため、現在ご利用いただけません

WAF オプションが未契約の場合に表示されます。
お申込みいただく場合は、画面下部の［お申し込みはこちら］をクリックしてください。

> **注意**
>
> MySQL のバージョンについては 4.3.1 利用可能なデータベースをご参照ください。

手順３）～７）は MySQL を一度も利用していない場合の手順です。
MySQL を有効化済みの場合は手順１２）に進んでください。

３）　画面下部の［データベース設定］をクリックします。

４）　「データベース」画面が表示されます。MySQL の操作欄にある［利用開始］をクリックします。

５）　「利用開始設定」画面で、パスワードを入力して［利用を開始する］をクリックします。

※ ここで設定したパスワードを紛失しないようご注意ください。

６）　「MySQL を初期化しました。」と表示されたら、MySQL の有効化は完了です。

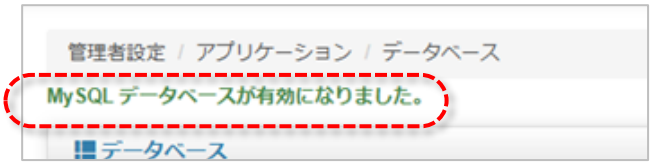
７）　左メニュー「ウェブサーバー」から［WAF］をクリックして WAF 画面に戻り、手順１２）に進んでください。

手順８）～１１）は MySQL が停止中の場合の手順です。
MySQL を起動済みの場合は手順１２）に進んでください。

８）　画面下部の［データベース設定］をクリックします。

９）　「データベース」画面が表示されます。MySQL の操作欄にある［起動］をクリックします。

１０）　「MySQL データベースが有効になりました。」と表示されたら、MySQL の起動は完了です。



１１）　左メニュー「ウェブサーバー」から［WAF］をクリックして WAF 画面に戻り、手順１２）に進んでください。

１２） WAF 画面下部にある［MySQL 管理パスワード］を入力して［WAF 機能を有効化する］をクリックします。

１３） データベース作成可否のポップアップ画面が表示されます。［OK］をクリックしてください。

１４） 「WAF 機能が利用可能になりました」というメッセージが表示されます。
WAF 機能の有効化（データベース作成）は以上で完了です。

3.6.3. WAF 設定

「WAF 設定」では、ドメインごとに基本設定/個別ルール/ホワイトリスト/ブラックリストの設定ができます。

- WAF 機能を有効化した直後は「WAF 設定」画面（基本設定）が表示されます。
- 「WAF 検知結果」画面を表示している場合は、[設定]をクリックすると「WAF 設定」画面に遷移できます。

  ※ 「WAF 設定」では「基本設定」がトップ画面として表示されます。

[1]「WAF 検知結果」画面に遷移します
参照）3.6.4 WAF 検知結果

[2] プルダウンから設定対象のドメインを選択できます
※ ここで選択した情報は他の画面に遷移しても保持されます。

[3]タブを選択すると各設定画面に切り替わります
参照）
- ■ 基本設定
- ■ 個別ルール設定
- ■ ホワイトリスト設定
- ■ ブラックリスト設定

■ 基本設定

「基本設定」では、WAF 機能の動作モード切り替えや、WordPress で利用するアクセスを WAF の検知対象から除外する設定が可能です。

- 初期設定では、WAF の動作モードを「検知」としています。
- 実運用の前に、数日間「検知」モードで検知状況をご確認いただき、適宜調整のうえ［ブロック］モードに切り替えることをお勧めします。

  ※ 検知状況は［検知結果］から確認できます。
  参照）3.6.4 WAF 検知結果

  ※ 必要なアクセスが攻撃として検知された場合は以下いずれかの方法をお試しください。
  ・該当ログの個別ルールを［検知］→［無効］に変更する
  （[無効]に設定した個別ルールは、動作モードをブロックに切替えても[無効]の状態が保持されます）
  ・該当ログのアクセス元 IP アドレスをホワイトリストに追加する

  参照）■ 個別ルール設定
  ■ ホワイトリスト設定

- 実運用時は、WAF のブロック機能が有効となる「ブロック」モードに設定してください。

［1］WAF 機能の動作モードを選択できます

■ **動作モード**

ブロック

攻撃と判定されたアクセスをブロックします。
※ 個別ルールは［ブロック］または［無効］に設定することができます。
※ 個別ルールを［無効］にした場合は、ブロックしません。
※ 個別ルールを［無効］にした場合は「WAF 検知結果のログ」は出力しません。

検知

攻撃と判定されたアクセスを検知します。
※ 個別ルールは［検知］または［無効］に設定することができます。
※ 個別ルールを［無効］にした場合は、検知しません。
※ 個別ルールを［無効］にした場合は「WAF 検知結果のログ」は出力しません。

無効

WAF(ホワイトリスト・ブラックリスト含む)を無効化します。
※ 個別ルールも［無効］となり、ログの出力はされません。

各動作モードと、各種設定（個別ルール、ホワイトリスト、ブラックリスト）の組み合わせによる挙動は「3.6.1 WAF の概要 ＞ WEB サイトへ攻撃があった場合の WAF の挙動」をご参照ください。

［2］WordPress で利用するアクセスを WAF の検知対象から除外するかを選択（ON/OFF）できます

※ 初期設定は［ON］です。

※ WordPress を利用している場合は［ON］、WordPress を利用していない場合は［OFF］に設定することを推奨します。

※ 本機能を［ON］にすることで、お客さまが行う WordPress 管理画面での基本的な操作はブロックされなくなりますが、不正なアクセスやブラックリストに登録されている IP アドレスからのアクセスはブロックします。

※ お客さまのご利用状況によっては、本機能を ON にしても WordPress で作成されたページや WordPress 管理画面での操作等に影響がでる可能性があります。その場合は、「個別ルール」の設定変更や「ホワイトリスト」への追加をお試しください。

参照）■ 個別ルール設定
■ ホワイトリスト設定

◆ 動作モードの切り替え

① 対象のドメインを選択する

② 切り替えたいモードをクリックする

③ ［保存］をクリックする

④ 確認のダイアログが表示されたら［OK］をクリックする

⑤ 「設定を保存しました」というメッセージが表示される

動作モードの切り替え手順は以上です。

■ 個別ルール設定

各種攻撃に対する個別ルールの動作を確認または変更する場合に利用します。
「基本設定」の動作モードがベースとなり、そのうえで個別ルールの設定が有効となります。

- 動作モード「ブロック」の場合、個別ルールは［ブロック］または［無効］に設定できます。
- 動作モード「検知」の場合、個別ルールは［検知］または［無効］に設定できます。
- 動作モード「無効」の場合、個別ルールも［無効］となり、設定は変更できません。

※ 動作モードが「ブロック」または「検知」の場合でも、［無効］にした個別ルールは検知結果ログには出力されません。
※ 動作モード「ブロック」の場合の個別ルールの初期設定は、すべて「ブロック」です。
※ 動作モード「検知」の場合の個別ルールの初期設定は、すべて「検知」です。
※ 手動で［無効］に変更した個別ルールは、動作モードに依らず［無効］を維持しますが、初期設定のままの個別ルールは、動作モードに合わせて設定が変更されます。

動作モード（基本設定）と、各種設定（個別ルール、ホワイトリスト、ブラックリスト）の組み合わせによる挙動は「3.6.1 WAF の概要 > WEB サイトへ攻撃があった場合の WAF の挙動」をご参照ください。

［1］リクエスト/レスポンスごとにカテゴリーから攻撃パターンを選択できます

［2］ 攻撃パターンごとのルール（ID/メッセージ）一覧です
※［1］カテゴリーで攻撃パターンをクリックすると該当のテーブルに移動します。

［3］各ルールに対する設定をボタン（ブロック/検知/無効）が表示されます。
動作モードにより、表示されるボタンは以下のとおり異なります。

動作モード	個別ルールの設定ボタン
ブロック	ブロック、無効
検知	検知、無効
無効	無効

◆ ルールのカテゴリー概要

カテゴリー(リクエスト)	概要
IP 評価	IP アドレスの信頼性に基づいてスコアリングを行い、通信の許可/不許可を判断します。
メソッド強制	ポリシーによって許可されていないメソッドを制限します。
DOS 防衛	DOS 攻撃から保護します。
スキャナ検出	ポートスキャンや脆弱性スキャン等から保護します。
プロトコル強制	プロトコルとエンコーディングの問題から保護します。
プロトコル攻撃	ヘッダーインジェクション、要求スマグリング、応答分割等から保護します。
マルチパート攻撃	multipart/form-data に関する脆弱性用のルールです。
ローカルファイルインジェクション	ローカルファイルインクルージョン（LFI）攻撃から保護します
リモートファイルインジェクション	リモートファイルインクルージョン（RFI）攻撃から保護します
リモートコード攻撃	リモート コード実行攻撃から保護します
PHP	PHP インジェクション攻撃から保護します
NODEJS	Node JS 攻撃から保護します
クロスサイトスクリプティング	クロスサイト スクリプティング攻撃から保護します
SQL インジェクション	SQL インジェクション攻撃から保護します
セッション固定	セッション固定攻撃から保護します
JAVA	Java 攻撃から保護します
ブロッキング評価	受信側の異常スコアを評価して、閾値を超過した場合にブロックします。 ※基本設定の動作モード「ブロック」で機能するため個別ルールの設定は変更できません。

カテゴリー(レスポンス)	概要
データ漏洩	WEB ディレクトリに関するデータの漏洩を防ぎます。
SQL データ漏洩	SQL に関するデータの漏洩を防ぎます。
JAVA データ漏洩	JAVA に関するデータの漏洩を防ぎます。
PHP データ漏洩	PHP に関するデータの漏洩を防ぎます。
IIS データ漏洩	IIS に関するデータの漏洩を防ぎます。
ブロッキング評価	送信側の異常スコアを評価して、基準を超過した場合にブロックします。 ※基本設定の動作モード「ブロック」で機能するため個別ルールの設定は変更できません。

※ WAF で検知された攻撃やシグネチャ（ルール）の詳細についてはサポート対象外となります。

◆ ルールの設定変更

① 対象のドメインが選択されていることを確認する

② 設定を変更したいルールの設定ボタンをクリックする
（ここでは例として、2 つのルールを［ブロック］から［無効］に変更します）
※ 設定ボタンをクリックしたルールは赤字で表示されます

③ ［変更内容を保存］をクリックする
※ 保存ボタンの下に変更しようとしているルールの数が表示されます。

④ 確認のダイアログが表示されたら［OK］をクリックする

⑤ 「設定を保存しました」というメッセージが表示される

ルールの設定変更手順は以上です。

■ ホワイトリスト設定

- WAF の個別ルール設定にかかわらず特定の IP アドレスからのアクセスを許可したい場合に利用します。

※ ホワイトリストに登録された IP アドレスは、WAF のシグネチャによる監査を行わずにアクセスが可能となります。

- ホワイトリストに登録された IP アドレスからのアクセス履歴は、「検知結果」画面の対象ログで［ホワイトリスト］を選択することで表示されます。
  ※ WAF の「検知結果」ログには表示されません
- テキストファイルをインポートして一括登録することも可能です。
- 登録数（推奨値）：3000
  ※ サブネットマスクでの指定：可能

> 動作モード（基本設定）と、各種設定（個別ルール、ホワイトリスト、ブラックリスト）の組み合わせによる挙動は「3.6.1 WAF の概要 ＞ WEB サイトへ攻撃があった場合の WAF の挙動」をご参照ください。

［１］ クリックすると IP アドレスフィールドに入力欄が表示されます

［２］ チェックボックスを選択した IP アドレスをまとめて削除できます

［３］ IP アドレスの追加をテキストファイルでインポートできます

［４］ 登録されている IP アドレス一覧をテキストファイルでエクスポートできます

［５］ 追加した IP アドレスが一覧表示されます

◆ IP アドレスの追加/編集

追加

① 対象のドメインが選択されていることを確認する

② ［IP アドレスの追加］をクリックする

③ 入力欄に IP アドレスを入力して Enter キーを押して入力内容を確定させる

※ 入力内容が確定すると［変更内容を保存］ボタンが表示されます。

※ ここで保存せずに、再度［IP アドレスの追加］をクリックすると入力欄が追加されるので、複数まとめて保存することも可能です。

※ 保存ボタンの下に追加/変更しようとしている数が表示されます。

④ ［変更内容を保存］をクリックする

⑤ 確認のダイアログが表示されたら［OK］をクリックする

⑥ 「ホワイトリストを保存しました」というメッセージが表示される

ホワイトリストへ IP アドレスを追加する手順は以上です。

注意

- 同じ IP アドレスを登録しないようご留意ください。

※ 重複した登録を許容する仕様となるためエラーにはなりません。重複しても動作には影響はありませんが、設定を変更（解除）する際に重複した分の対応も必要となります。

アドバイス

- 未入力のまま画面上の他の箇所をクリックしたり他の画面に遷移すると、Enter キーを押したときと同様に入力欄が確定されるため、「未設定」と表示された状態になります。

  編集マーク をクリックすると入力可能な状態になります。
  削除マーク をクリックすると行を削除できます。

編集

① 編集したい IP アドレスの編集マーク をクリックする

② 入力値を編集し、Enter キーを押して編集内容を確定させる

※ 入力内容が確定すると［変更内容を保存］ボタンが表示されます。

※ ここで保存せずに、他の編集や新規追加を複数まとめて保存することも可能です。

※ 保存ボタンの下に追加/編集しようとしている数が表示されます。

③ ［変更内容を保存］をクリックする

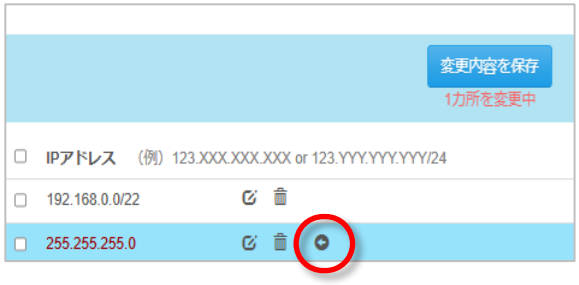
④ 確認のダイアログが表示されたら［OK］をクリックする

⑤ 「ホワイトリストを保存しました」というメッセージが表示される

ホワイトリストの IP アドレスを編集する手順は以上です。

アドバイス

- 編集内容を取り消したい場合は、保存する前に取消マーク をクリックすると、編集前の状態に戻ります。

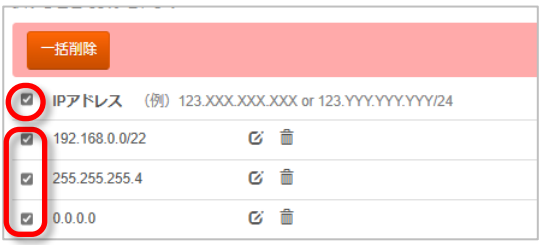


◆ IP アドレスの削除

① 削除したい IP アドレスの削除マーク　　または［一括削除］をクリックする

- 1つずつ削除する場合:
  削除したい IP アドレスの削除マーク をクリックします

- 複数まとめて削除する場合:
  削除したい IP アドレスのチェックボックスを選択して［一括削除］をクリックします



※ カラム行のチェックボックスを選択すると、すべて選択されます。
※ チェックボックスを選択すると［一括削除］ボタンが表示されます。

② ［変更内容を保存］をクリックする

※ 削除マーク/一括削除 をクリックすると［変更内容を保存］ボタンが表示されます。
※ 保存ボタンの下に追加/編集しようとしている数が表示されます。

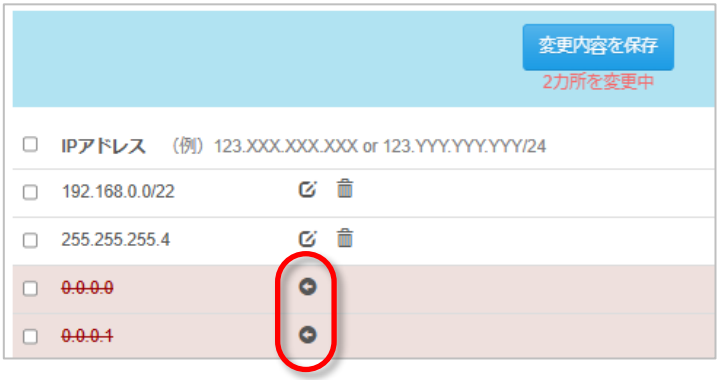
③ 確認のダイアログが表示されたら［OK］をクリックする

④ 「ホワイトリストを保存しました」というメッセージが表示される

ホワイトリストの IP アドレスを削除する手順は以上です。

アドバイス

- 削除を取り消したい場合は、保存する前に取消マーク をクリックすると、元の状態に戻ります。



◆ IP アドレスの一括登録(インポート)

インポートするテキストファイルの用意

- サンプルファイルは、［一括登録］をクリックして表示されたダイアログ左上の［フォーマットサンプル(.txt)のダウンロード］からダウンロードできます。

※　ダウンロードされるサンプルファイル名　：iplist_sample.txt

※　［フォーマットサンプル(.txt)のダウンロード］をクリックすると自動的にダウンロードを開始し、ご利用端末のダウンロードフォルダに保存されますが、お客さまのご利用環境によっては保存先を指定するダイアログが表示される場合もあります。その場合は任意の保存先を指定して保存してください。

注意

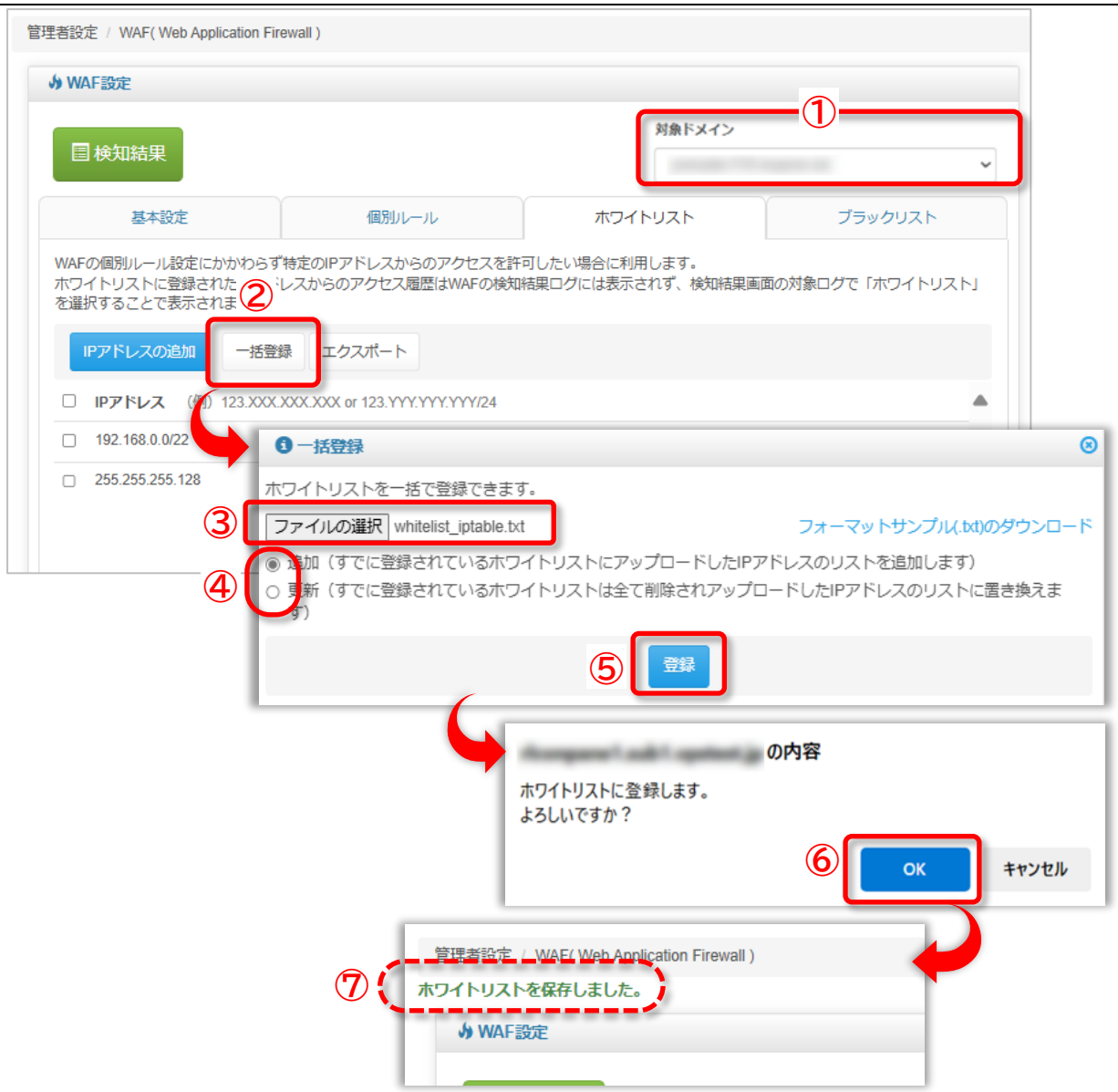
- インポートするファイルはテキスト（.txt）形式で作成してください。
  ※ ファイル名に使用する文字種に制限はありませんが、半角英小文字を推奨します。
- IP アドレスの書式が正しくない場合はエラーとなります。

===正しくない IP アドレスの例===

- □ IP アドレスの範囲（0.0.0.0～255.255.255.255）に含まれない　例）2200.100.10.0
- □ サブネットマスクのプレフィックス表記が正しくない　例）255.255.255.255/20
- □ 全角文字や数字以外の文字が含まれている　例）２５５.xxx.あああ.0
- □ .（ドット）や /（スラッシュ）が全角になっている　例）255.255.255. 0／24
- □ 前後や途中に不要なスペースが存在する　例）164.70.11 .1

※ IP アドレスやサブネットマスクの計算はサポート対象外となります。

一括登録（インポート）手順



① 対象のドメインが選択されていることを確認する

② ［一括登録］をクリックする

③ ［ファイルの選択］をクリックして用意したテキストファイルを指定する

④ ［追加］または［更新］を選択する

［追加］：インポートするファイルに登録済みの IP アドレスが含まれないようにご注意ください。
［更新］：登録済みのリストは削除されインポートしたリストに置き換えられます。
誤選択に注意してください。

⑤ ［登録］をクリックする

⑥ 確認のダイアログが表示されたら［OK］をクリックする

⑦ 「ホワイトリストを保存しました」というメッセージが表示される

ホワイトリストへ IP アドレスを一括登録する手順は以上です。

◆ IP アドレスのエクスポート

① 対象のドメインが選択されていることを確認する

② ［エクスポート］をクリックする

③ 確認のダイアログが表示されたら［OK］をクリックする

※ エクスポートされるファイル名： whitelist_iptable.txt

※ ［OK］をクリックすると自動的にダウンロードを開始し、ご利用端末のダウンロードフォルダに保存されますが、お客さまのご利用環境によっては保存先を指定するダイアログが表示される場合もあります。その場合は任意の保存先を指定して保存してください。

■ ブラックリスト設定

- WAF の個別ルール設定にかかわらず特定の IP アドレスからのアクセスを拒否したい場合に利用します。

※ ブラックリストに登録された IP アドレスは、WAF のシグネチャによる監査前にアクセスを拒否します。

- ブラックリストに登録された IP アドレスからのアクセス履歴は、「検知結果」画面の対象ログで［ブラックリスト］を選択することで表示されます。
  ※ WAF の「検知結果」ログには表示されません
- テキストファイルをインポートして一括登録することも可能です。
- 登録数（推奨値）：3000
  ※ サブネットマスクでの指定：可能

> 動作モード（基本設定）と、各種設定（個別ルール、ホワイトリスト、ブラックリスト）の組み合わせによる挙動は「3.6.1 WAF の概要 ＞ WEB サイトへ攻撃があった場合の WAF の挙動」をご参照ください。

［1］ クリックすると IP アドレスフィールドに入力欄が表示されます

［2］ チェックボックスを選択した IP アドレスをまとめて削除できます

［3］ IP アドレスの追加をテキストファイルでインポートできます

［4］ 登録されている IP アドレス一覧をテキストファイルでエクスポートできます

［5］ 追加した IP アドレスが一覧表示されます

◆ IP アドレスの追加/編集

追加

① 対象のドメインが選択されていることを確認する

② ［IP アドレスの追加］をクリックする

③ 入力欄に IP アドレスを入力して Enter キーを押して入力内容を確定させる

※ 入力内容が確定すると［変更内容を保存］ボタンが表示されます。

※ ここで保存せずに、再度［IP アドレスの追加］をクリックすると入力欄が追加されるので、複数まとめて保存することも可能です。

※ 保存ボタンの下に追加/変更しようとしている数が表示されます。

④ ［変更内容を保存］をクリックする

⑤ 確認のダイアログが表示されたら［OK］をクリックする

⑥ 「ブラックリストを保存しました」というメッセージが表示される

ブラックリストへ IP アドレスを追加する手順は以上です。

注意

- Localhost（127.0.0.1）や本サービスの IP アドレスは登録しないでください。
  予期せぬ問題が発生する可能性があります。
- 同じ IP アドレスを登録しないようご留意ください。

※ 重複した登録を許容する仕様となるためエラーにはなりません。重複しても動作には影響はありませんが、設定変更（解除）する際に重複した分の対応も必要となります。

アドバイス

- 未入力のまま画面上の他の箇所をクリックしたり他の画面に遷移すると、Enter キーを押したときと同様に入力欄が確定されるため、「未設定」と表示された状態になります。

  編集マーク をクリックすると入力可能な状態になります。
  削除マーク をクリックすると行を削除できます。

編集

① 編集したい IP アドレスの編集マーク をクリックする

② 入力値を編集し、Enter キーを押して編集内容を確定させる

※ 入力内容が確定すると［変更内容を保存］ボタンが表示されます。

※ ここで保存せずに、他も編集したり新規追加してから複数まとめて保存することも可能です。

※ 保存ボタンの下に追加/編集しようとしている数が表示されます。

③ ［変更内容を保存］をクリックする

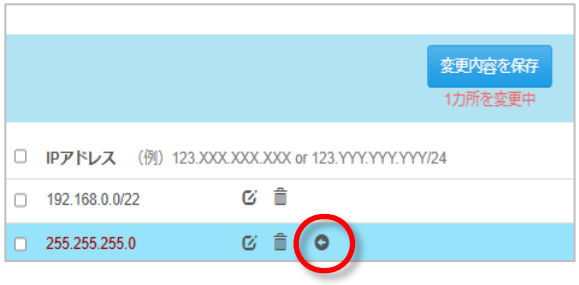
④ 確認のダイアログが表示されたら［OK］をクリックする

⑤ 「ブラックリストを保存しました」というメッセージが表示される

ブラックリストの IP アドレスを編集する手順は以上です。

アドバイス

- 編集内容を取り消したい場合は、保存する前に取消マーク をクリックすると、編集前の状態に戻ります。

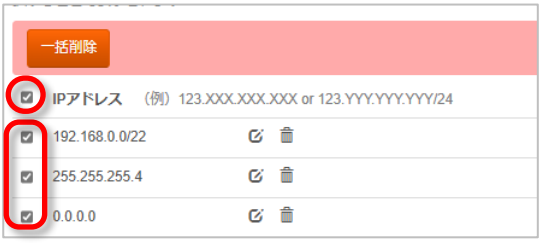


◆ IP アドレスの削除

① 削除したい IP アドレスの削除マーク　　または［一括削除］をクリックする

- 1つずつ削除する場合:
  削除したい IP アドレスの削除マーク をクリックします

- 複数まとめて削除する場合:
  削除したい IP アドレスのチェックボックスを選択して［一括削除］をクリックします



※ カラム行のチェックボックスを選択すると、すべて選択されます。
※ チェックボックスを選択すると［一括削除］ボタンが表示されます。

② ［変更内容を保存］をクリックする

※ 削除マーク/一括削除 をクリックすると［変更内容を保存］ボタンが表示されます。
※ 保存ボタンの下に追加/編集しようとしている数が表示されます。

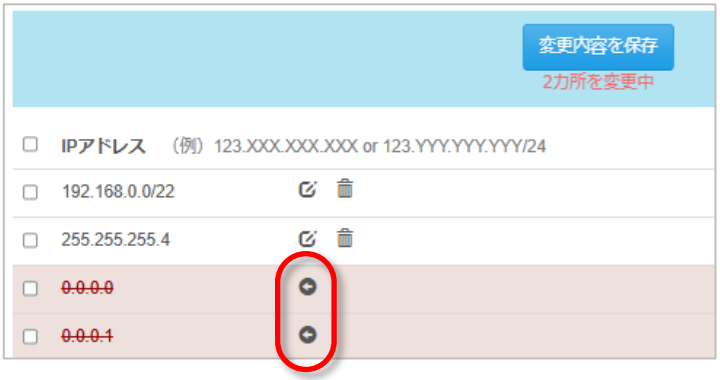
③ 確認のダイアログが表示されたら［OK］をクリックする

④ 「ブラックリストを保存しました」というメッセージが表示される

ブラックリストの IP アドレスを削除する手順は以上です。

アドバイス

- 削除を取り消したい場合は、保存する前に取消マーク をクリックすると、元の状態に戻ります。



◆ IP アドレスの一括登録(インポート)

インポートするテキストファイルの用意

- サンプルファイルは、［一括登録］をクリックして表示されたダイアログ左上の［フォーマットサンプル(.txt)のダウンロード］からダウンロードできます。

※　ダウンロードされるサンプルファイル名　：iplist_sample.txt

※　［フォーマットサンプル(.txt)のダウンロード］をクリックすると自動的にダウンロードを開始し、ご利用端末のダウンロードフォルダに保存されますが、お客さまのご利用環境によっては保存先を指定するダイアログが表示される場合もあります。その場合は任意の保存先を指定して保存してください。

注意

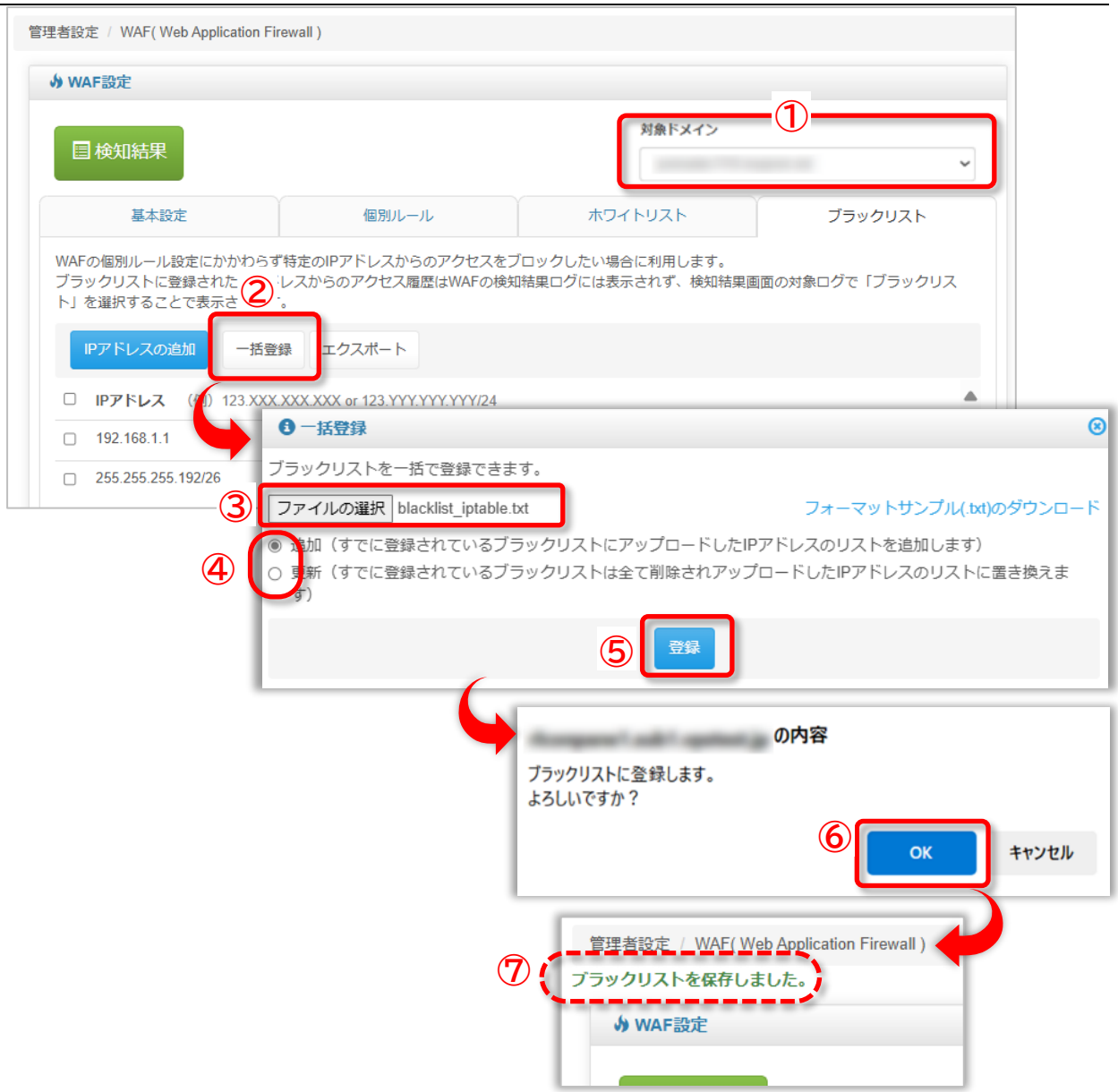
- インポートするファイルはテキスト（.txt）形式で作成してください。
  ※ ファイル名に使用する文字種に制限はありませんが、半角英小文字を推奨します。
- IP アドレスの書式が正しくない場合はエラーとなります。

□ IP アドレスの範囲（0.0.0.0～255.255.255.255）に含まれない　例）2200.100.10.0
□ サブネットマスクのプレフィックス表記が正しくない　例）255.255.255.255/20
□ 全角文字や数字以外の文字が含まれている　例）２５５.xxx.あああ.0
□ .（ドット）や /（スラッシュ）が全角になっている　例）255.255.255. 0／24
□ IP アドレスの前後や途中に不要なスペースが存在する　例）164.70.11 .1

※ IP アドレスやサブネットマスクの計算はサポート対象外となります。

- Localhost（127.0.0.1）や本サービスの IP アドレスは登録しないでください。
  予期せぬ問題が発生する可能性があります。

一括登録（インポート）手順



① 対象のドメインが選択されていることを確認する

② ［一括登録］をクリックする

③ ［ファイルの選択］をクリックして用意したテキストファイルを指定する

④ ［追加］または［更新］を選択する

［追加］：インポートするファイルに登録済みの IP アドレスが含まれないようにご注意ください。
［更新］：登録済みのリストは削除されインポートしたリストに置き換えられます。
誤選択に注意してください。

⑤ ［登録］をクリックする

⑥ 確認のダイアログが表示されたら［OK］をクリックする

⑦ 「ブラックリストを保存しました」というメッセージが表示される

ブラックリストへ IP アドレスを一括登録する手順は以上です。

◆ IP アドレスのエクスポート

① 対象のドメインが選択されていることを確認する

② ［エクスポート］をクリックする

③ 確認のダイアログが表示されたら［OK］をクリックする

※ エクスポートされるファイル名： blacklist_iptable.txt

※ ［OK］をクリックすると自動的にダウンロードを開始し、ご利用端末のダウンロードフォルダに保存されますが、お客さまのご利用環境によっては保存先を指定するダイアログが表示される場合もあります。その場合は任意の保存先を指定して保存してください。

3.6.4. WAF 検知結果

WAF 機能を有効化した後は、「WAF 検知結果」画面が WAF 機能のトップ画面として表示されます。

■ 一覧画面

- 「基本設定」の動作モードが［ブロック］または「検知」に設定されていて、攻撃と判定されたアクセスを検知/ブロックした場合にログが表示されます。
- ログは、合計「1GB」程度を上限として 1 年間保存されます。保持されているログの範囲内で表示/検索が可能です。
  ※ 容量を超えるまたは保存期間を超えたログは、新しいログで上書きされます。

> 動作モード（基本設定）と、各種設定（個別ルール、ホワイトリスト、ブラックリスト）の組み合わせによる挙動は「3.6.1 WAF の概要 > WEB サイトへ攻撃があった場合の WAF の挙動」をご参照ください。

［1］「WAF 設定」画面に遷移します
参照）3.6.3 WAF 設定

［2］［更新］をクリックして表示されるログのデータベースをリアルタイムで更新できます
※ 自動更新：1 時間ごと

［３］プルダウンから対象ログ（検知結果/ホワイトリスト/ブラックリスト）を選択できます
※ 対象ログ：検知結果　には、ホワイトリスト/ブラックリストに登録されているアクセス元 IP アドレスは含まれません。

［４］表示するログの期間（開始日時/終了日時）を指定できます

［５］［検索］をクリックすると、［３］対象ログと［４］表示期間で指定した条件でログが表示されます
※［２］の［更新］をクリックして「ログ DB 更新日時」が更新されたことを確認したうえで［検索］をクリックすると、最新のログが表示されます。

［６］ログが一覧表示されます
※ 表示できるログは 1000 件までです。1000 件を超える場合は表示期間を調整してください。
※ 長期間を指定して検索した際に、サーバー側でタイムアウトとなりエラーが表示される可能性があります。

［７］検索ワードを入力して、表示したログを絞り込み検索できます
※ ログがない場合、この機能は表示されません

［８］表示しているログを CSV でエクスポートできます
※ ログがない場合、この機能は表示されません

［９］各ログの詳細を確認できます
参照）■詳細画面

［１０］　プルダウンから表示対象のドメインを選択できます
※ ここで選択した情報は他の画面に遷移しても保持されます。

注意

WAF 検知結果画面にログが表示されない場合は、以下をご確認ください。

- **WAF のログを蓄積するには、ディスク容量を 1GB 程度空ける必要があります。**
  不要なメールデータやバックアップデータ等の削除をお試しください。
- **ログデータを削除している場合は、検知結果のログが表示されません。**以下のファイルまたは logs ディレクトリごと削除した場合は、サポート窓口までご連絡ください。

  ・ホームディレクトリ /www/logs に格納されているファイル（error_log、modsec_audit.log）
  ・ホームディレクトリ / users/[ドメイン管理者名]/www/logs に格納されているファイル（error_log）

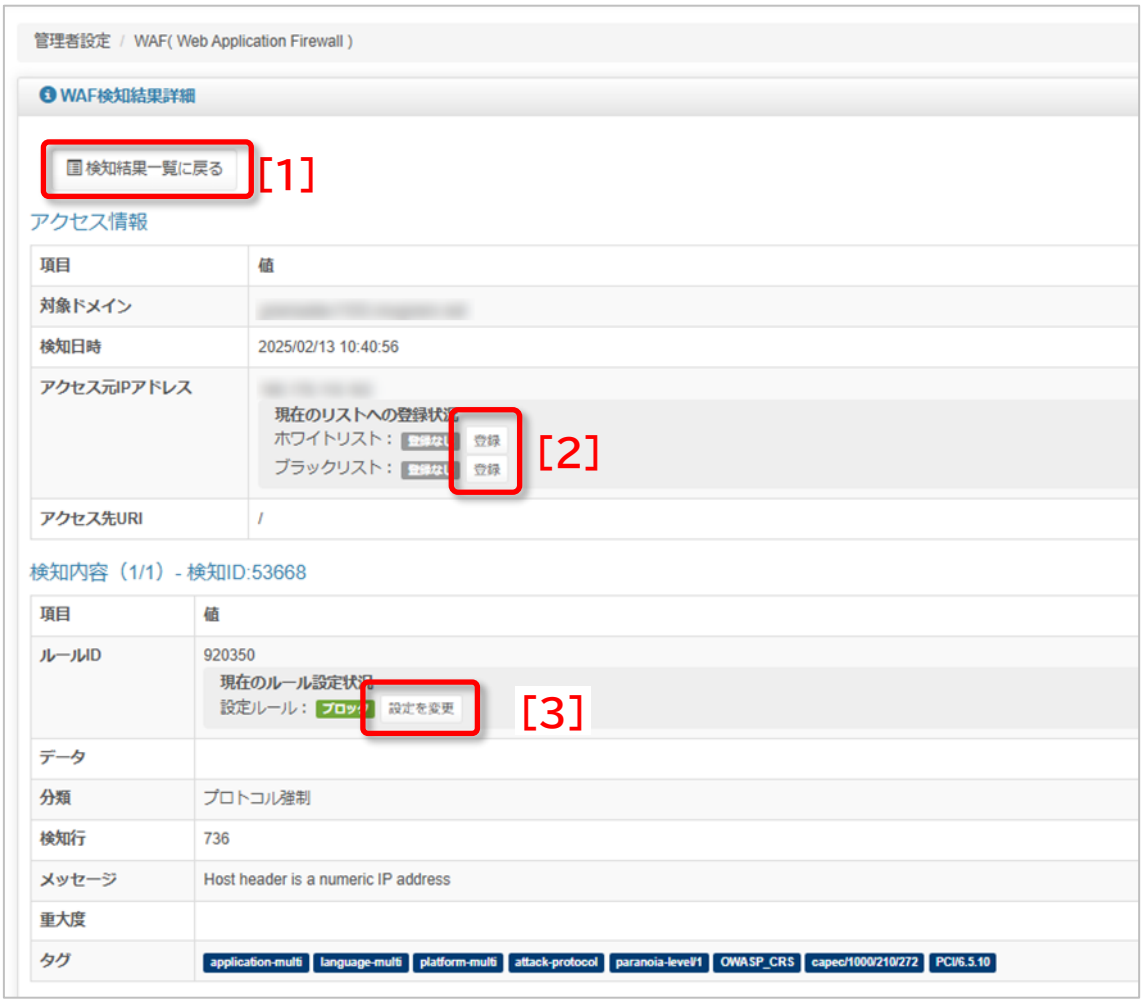
  お問い合わせ窓口｜Biz メール&ウェブ プレミアム
  https://support.ntt.com/mw-premiumr3/inquiry/detail/pid2200001fcc/
- **httpd.conf でドメインごとに記述されている「WAF の動作に必要なコンフィグファイルの参照先」を変更している場合はログが生成されません。**以下の正しい参照先に変更してください。

```
<IfModule mod_security2.c>
IncludeOptional "/etc/httpd/modsecurity.d/local_rules/{ドメイン名}/{ドメイン名}.conf"
</IfModule>
```

※ 上記の記述は、コントロールパネルに登録されているドメインごとに存在します。
※ {ドメイン名}部分は該当するドメインに置き換えてください。

■ 詳細画面

- 詳細画面では以下が可能です。
  ・検知された攻撃の詳細確認
  ・検知された攻撃の「個別ルール」の設定変更
  ・検知された攻撃のアクセス元 IP アドレスを「ホワイトリスト」登録/解除
  ・検知された攻撃のアクセス元 IP アドレスを「ブラックリスト」登録/解除
- 詳細画面で設定した内容は、各設定（個別ルール、ブラックリスト、ホワイトリスト）に反映されます。
- 1 つのアクセスが複数の攻撃種類として判定された場合は、検知されたすべての攻撃の種類が表示されます。



［1］「WAF 検知結果」一覧に遷移します
参照）■一覧画面

［2］アクセス元 IP アドレス「ホワイトリスト」「ブラックリスト」に登録できます
※ 登録済みの場合は［解除］ボタンが表示されます。

［3］ルール ID 単位で個別ルール設定の変更ができます

◆ ホワイトリスト/ブラックリストの登録と解除

登録

ここではホワイトリストを例にして登録手順をご案内します。

① 「アクセス情報」欄にあるホワイトリストの［登録］をクリックする

② 確認のダイアログが表示されたら［OK］をクリックする

③ 「設定の変更を保存しました」というメッセージと、ホワイトリストへの登録状況が「登録あり」と表示される

「WAF 検知結果詳細」画面でホワイトリストへ IP アドレスを登録する手順は以上です。

解除

ここではホワイトリストを例にして解除手順をご案内します。

① 「アクセス情報」欄にあるホワイトリストの［解除］をクリックする

② 確認のダイアログが表示されたら［OK］をクリックする

③ 「設定の変更を保存しました」というメッセージと、ホワイトリストへの登録状況が「登録なし」と表示される

「WAF 検知結果詳細」画面でホワイトリストから IP アドレスを解除する手順は以上です。

◆ 個別ルール設定変更

ここでは例として、「ブロック」から「無効」に変更する内容をご案内します。

① 「検知内容」欄で、変更したいルールの［設定を変更］をクリックする

② 設定変更のダイアログで［無効］を選択して［設定を保存］をクリックする

③ 「設定の変更を保存しました」というメッセージと、ルール設定状況が「無効」と表示される

「WAF 検知結果詳細」画面で個別ルールの設定を変更する手順は以上です。

3.7. ウェブサイト分析

3.7.1. ウェブサイト分析の概要

アクセス解析データやソーシャルデータを収集して、ウェブサイトの改善点や傾向を分析することが可能です。

項目	種類	説明
傾向分析	アクセス数の推移	Web サイトのアクセス数と訪問者数を表示します。 表示期間：直近 4 週間、過去 12 カ月、月指定
	アクセス元ページ	Web サイトへのアクセス元の割合を表示します。 （直接アクセス、検索エンジン、他サイト）
	検索数の推移	設定した分析ワードの検索数の推移を表示します。
	関連検索ワード	設定した分析ワードを検索した人がその他の検索で使用したワードを抽出・表示します。
	関連ニュース	設定した分析ワードが含まれるニュースを抽出・表示します。
ページ分析	ページ別アクセス数	Web サイト内のページ毎のアクセス数を表示します。
	上位 10 ページのアクセス数グラフ	Web サイトのアクセス数トップ 10 ページを表示します。
	遷移図	対象ページ閲覧前後の遷移状況（アクセス元、アクセス先）を表示します。
訪問者分析	利用デバイス	訪問者が利用している端末の割合を表示します。 （PC、タブレット、スマートフォン、その他）
	利用ブラウザー	訪問者が利用しているブラウザーの割合を表示します。
	アクセス元地域	アクセス数が多い都道府県 上位 10 件を表示します。
	アクセス元 IP アドレストップ 10	アクセス数が多い上位 10 件の IP アドレスを表示します。
AI 分析		ウェブサイトを改善する方法を提示します。

注意

- ウェブサイト分析をご利用いただく場合は、サーバー情報の A レコードに Biz メール&ウェブ プレミアムのサーバーの IP アドレスが設定されている必要があります。
  お客さまで DNS サーバーをご用意されている場合は、セットアップマニュアル「6.2 お客さま DNS サーバーの設定」をご参照の上、設定してください。
- ウェブ分析ツールをアンインストールすると、それまで蓄積した分析データも削除されます。
- 本機能は、お客様のウェブ利用方法によりデータの表示分析結果が異なります。
  また、参考値となりますので、データの精度を保証するものではありません。

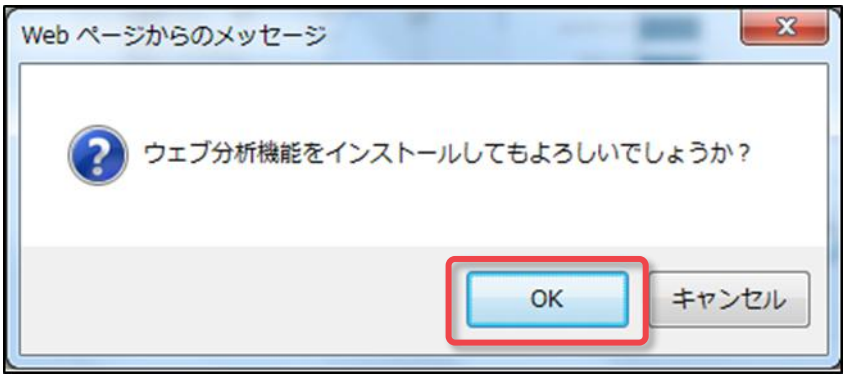
3.7.2. ウェブサイト分析のインストール

ウェブサイト分析のインストール方法をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[ウェブサイト分析] をクリックします。
ウェブサイト分析の画面が表示されたら、[ドメイン選択] をしてから、[MySQL 管理パスワード] を入力して、[インストール] をクリックします。

> **注意**
>
> MySQL のバージョンについては 4.3.1 利用可能なデータベースをご参照ください。

2） 確認メッセージが表示されたら、[OK] をクリックします。



3） 「ウェブ分析設定」の画面が表示されたら、完了です。

インストールが上手くいかない場合は、次ページの「ウェブサイト分析のインストールが上手くいかない場合」をご参照ください。

ウェブサイト分析のインストールが上手くいかない場合

ウェブサイト分析のインストールが上手くいかない場合は、以下の手順をお試しください。

1） MySQL の IP アクセス制限を［拒否］に設定する

① 左メニューの「システム」から［IP アクセス制限］をクリックします。
② MySQL の「デフォルトの挙動」を［拒否］にします。
③ ［設定を保存する］をクリックします。

プレミアム r2 から移行したお客さまの場合は、**手順３）**に進んでください。

２）　MySQL のパスワードを変更する

※ Mysql を利用しているアプリケーションにご留意ください。

① 左メニューの「アプリケーション」から［データベース］をクリックします。
② MySQL の［設定］をクリックします。

③ 「パスワード変更」欄に新しいパスワードを入力して、［保存］をクリックします。

画面はそのままで、手順３）に進んでください。

3） bind-access any を設定する

① 「設定ファイル（my.cnf)」欄に「bind-address = 0.0.0.0」を記載します。

※ 既に「bind-address = 127.0.0.1」という記載がある場合は、
「bind-address = 0.0.0.0」に変更してください。

② ［保存］をクリックします。

4） 再度「ウェブサイト分析」のインストールを実施する

インストール手順は、「3.7.2 ウェブサイト分析のインストール」をご参照ください。

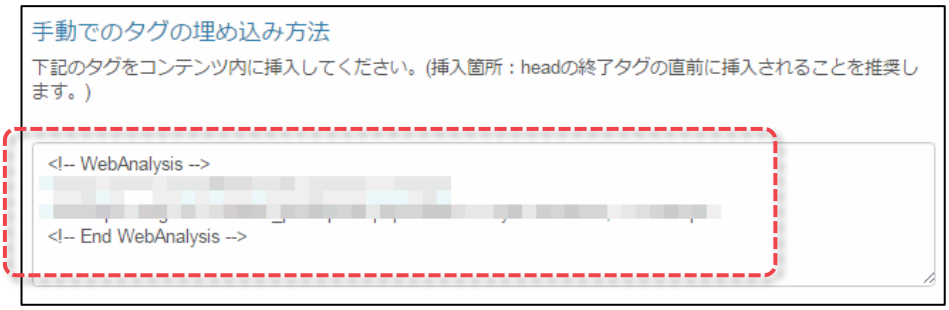
3.7.3. ウェブサイト分析の設定

ウェブサイト分析の設定方法をご説明します。

1） ウェブ分析設定画面ページで、「トラッキングタグ挿入ファイル」を選択します。

アドバイス

- トラッキングタグを手動で挿入する場合は、［タグの手動埋め込み方法］をクリックして、**<!-- WebAnalysis -->** から **<!-- End WebAnalysis -->** までをコピーし、ウェブサイトの解析を行う全てのページに貼り付けてください。

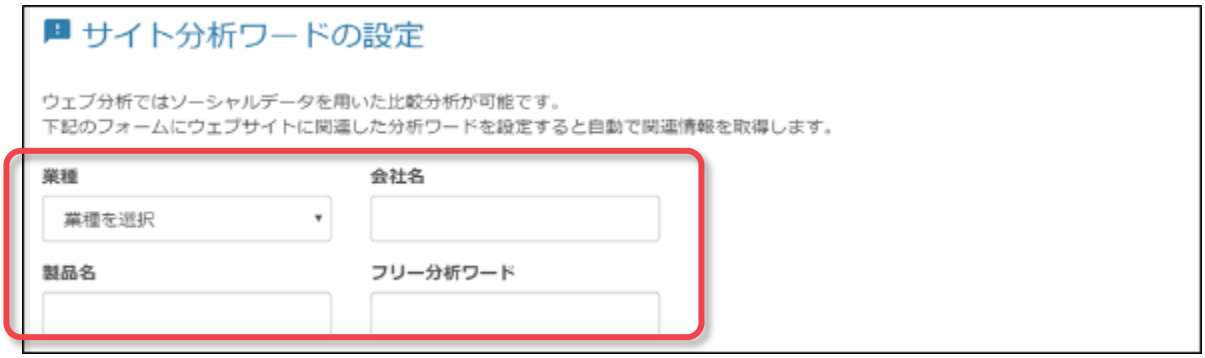


- ［タグの自動修復］を「ON」にすると、定期的/1 日毎にトラッキングタグの有無をチェックして、自動でトラッキングタグを修復します。

注意

- htdocs ディレクトリ配下の HTML ファイル(拡張子:html・htm・HTML・HTM)が、自動挿入ファイル対象です。
- トラッキングコードの埋め込み場所は、</head> の終了タグの直前に挿入することを推奨します。
- 動的コンテンツへの埋め込みについてはサポートしていません。

2） サイト分析ワードの設定を入力します。



アドバイス

分析ワードを入力することにより、検索傾向やニュースなどのソーシャルデータを取得して、アクセスパターンの分析や、ウェブサイトの改善点の分析を行うことができます。

3） 「レポートメールの設定」の［通知先メールアドレス］を入力して、［分析設定の保存］をクリックします。

レポートメール通知内容

レポートメール通知を ON にすると、毎週月曜日に通知先メールアドレスへ、ウェブ分析結果が配信されます。

＜例） 通知メール内容サンプル＞

From:管理者 ID@お客様ドメイン
subject: Biz メール＆ウェブ ウェブ分析 サマリーレポート YYYY/MM/DD

Biz メール＆ウェブ ウェブ分析サマリーレポートです。

先週(YYYY-MM-DD から YYYY-MM-DD まで)は、
XXXX ユニークユーザーから XXXX のアクセス(ページビュー)ありました。

分析結果の詳細はコントロールパネルからウェブ分析をご参照ください。
https://XXXXXX.bizmw.com/ControlPanel/

本メールはウェブ分析機能より自動配信されています。
設定の変更/解除はコントロールパネルのウェブ分析設定からご設定ください

4）　「ウェブ分析機能は設定が完了しました。」と表示されたら、完了です。

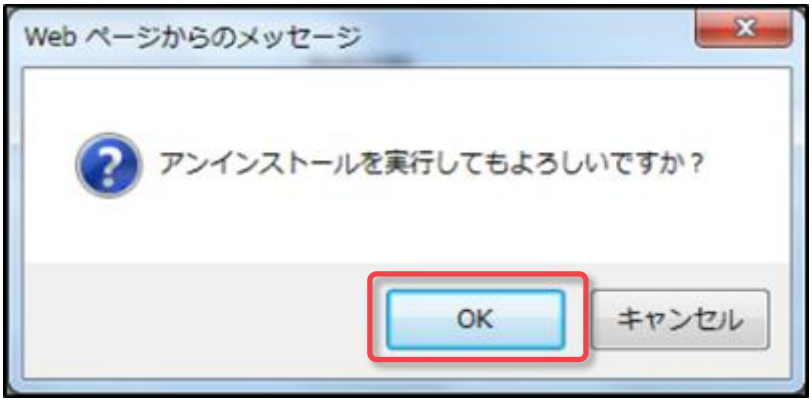
3.7.4. ウェブサイト分析のアンインストール

ウェブサイト分析のアンインストール方法をご説明します。

1） コントロールパネルの左メニュー「ウェブサーバー」から、[ウェブサイト分析] をクリックします。
次に、[ドメイン選択] してから、画面右端の [設定] をクリックしてください。

2） 「ウェブ分析機能のアンインストール」画面で、[アンインストールボタンを表示] をクリックします。
次に、[MySQL 管理パスワード] を入力して [アンインストールを実行] をクリックしてください。

3） 確認メッセージが表示されたら、[OK] をクリックします。



4） アンインストールが完了した旨のメッセージが表示され、初期インストール画面が表示されたら、完了です。

4　アプリケーション

4.1. 基本アプリ

4.1.1. 基本アプリの概要

本サーバー*で利用可能なスクリプト言語が確認できます。
ご利用可能なソフトウェアやアプリケーションなどのバージョンについては、以下の弊社サイトをご参照ください。

* OS は Rocky Linux8 です。

ソフトウェアのバージョン | Biz メール&ウェブ プレミアム
https://www.ntt.com/business/services/cloud/rental-server/vps/service23.html

4.1.2. PHP のバージョン

Biz メール&ウェブ では、以下のバージョンの PHP をご利用いただけます。

	バージョン
PHP	8.3 系

※ 提供元のセキュリティサポート終了に伴い PHP8.1 系の提供は終了しました。

PHP のバージョンおよび CGI/Module モードの切り替え方法は、後段の手順をご参照ください。

● PHP バージョンおよび CGI/Module モードの切り替え手順

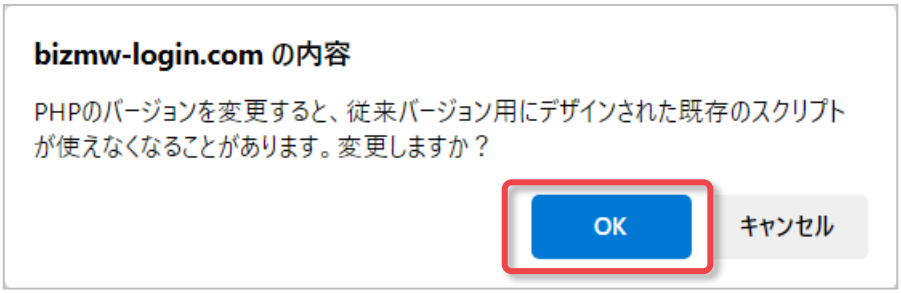
1） コントロールパネルの左メニュー「アプリケーション」から、[基本アプリ] をクリックします。

2） 「基本アプリ」画面で、スクリプト言語欄の「PHP」の [設定] をクリックします。

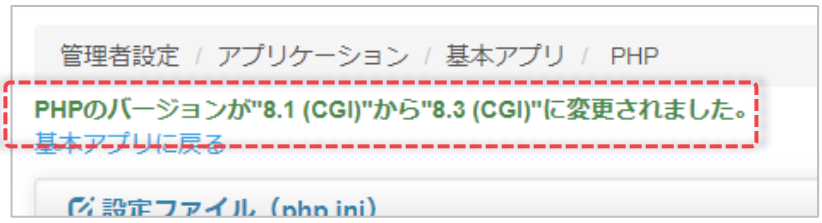
3） 「バージョンの選択」プルダウンから変更するバージョン/モードを選択して、[変更]をクリックします。

※ ここでは例として PHP8.1 系から 8.3 系へ変更する画面でご案内しています。

4） 確認メッセージが表示されたら、[OK]をクリックします。



5） 「PHP のバージョン/モードが変更された」旨のメッセージが表示されたら、完了です。



アドバイス

PHP の設定ファイルである **php.ini** は、各 PHP のバージョン毎に設置されています。
PHP のバージョンを変更すると 変更後のバージョンの php.ini を読み込みます。
PHP バージョン変更前の php.ini の情報は引き継がれないため、php.ini をカスタマイズしている場合は、PHP バージョン変更後に改めて php.ini を編集してください。

4.2. 追加アプリ

4.2.1. 追加アプリの概要

追加アプリとは、1 クリックでインストールが可能なアプリケーションです。
ブログ（WordPress）やアクセス解析（Matomo）等をインストールしてご利用いただけます。

◆ 利用可能なアプリは以下の通りです。

ブログ

アクセス解析


wiki クローン
（Pukiwiki）

※ パッケージ版「サイボウズ Office 10」の販売・サポート終了に伴い、Biz メール＆ウェブでのサイボウズ Office10 の提供（コントロールパネルからのインストール）は終了しました。

※ EC-CUBE と OpenPNE は PHP8.x ではご利用いただけません。

◆ 適合する言語／データベースのバージョンは、以下の通りです。

追加アプリ＼言語・データベース	PHP	MySQL		phpMyAdmin	pgAdmin
	8.3 系	8.0 系[*1]	8.4 系	5.2 系	
WordPress	○	○	○	○	PHP8.x では phpPgAdmin はご利用いただけません。**pgAdmin** をご利用ください。
Matomo	○	○	○	○	
Pukiwiki	○	−	−	−	

※ 提供元のセキュリティサポート終了に伴い PHP8.1 系の提供は終了しました。

＊1 提供元のセキュリティサポート終了に伴い、本サービスでは 2026 年 3 月 31 日までの提供となります。2026 年 2 月下旬より順次、弊社側で MySQL8.4 系への切り替え工事を実施する予定です。この場合、バックアップの取得や動作確認および MySQL8.0 系への切り戻しはできませんので、 MySQL8.0 系をご利用の場合は、お客さま側で 2026 年 2 月中旬までに MySQL8.4 系に切替えてください。
MySQL8.0 提供終了のお知らせ
https://support.ntt.com/mw-premiumr3/information/detail/pid2500002af5/

注意

- 本サービスの「追加アプリ」については、**インストールまでのご案内**となります。
  インストール後のご利用方法については、お客さまにて各アプリの公式サイト等で、お調べいただくようお願いいたします。
- 「追加アプリ」を利用する際には、**データベース(MySQL・PostgreSQL)** が必要となる場合がありますので、**事前に有効化**してください。

アドバイス

ご利用可能なソフトウェアやアプリケーションなどのバージョンについては、以下の弊社サイトをご参照ください。

ソフトウェアのバージョン｜Biz メール&ウェブ プレミアム
https://www.ntt.com/business/services/cloud/rental-server/vps/service23.html

4.2.2. 追加アプリのインストール

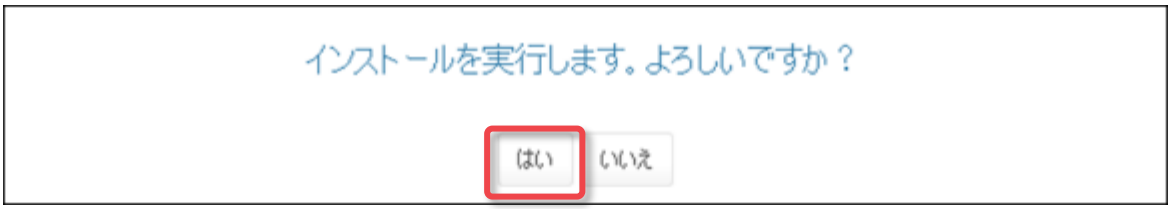
注意

- WordPress や Matomo を使用するには、**事前に MySQL の起動が必要**です。
  MySQL の詳細については、「4.3 データベース」をご確認ください。
- MySQL や PHP 等のバージョンについては以下をご確認ください。
  4.2.1 追加アプリの概要
  4.3.1 利用可能なデータベース

1） コントロールパネルの左メニュー「アプリケーション」から、[追加アプリ] をクリックします。

2） 対象のドメインを選択して、インストールしたいアプリの［インストール］をクリックします。

3） 確認メッセージが表示されたら、[はい] をクリックします。



4） インストールが完了すると、下図のように詳細情報が表示されます。
(この情報は、後からでも確認できます。)

※ 上図は、WordPress をインストールした際の詳細情報です。

また、ステータスが「インストール済」と表示されます。

注意

- WordPress の**自動更新は「無効化」**してご利用ください。

※ 本サービスでは、コントロールパネルからクイックインストールされるバージョンが動作検証済みのバージョンとなります。

※ 初期設定では WordPress の自動更新が「有効化」されていますが、自動で更新されるタイミングによってはご利用のプラグインや PHP/MySQL 等のバージョンと互換性がない状態になる恐れがあるため、自動更新を「無効化」してからご利用ください。

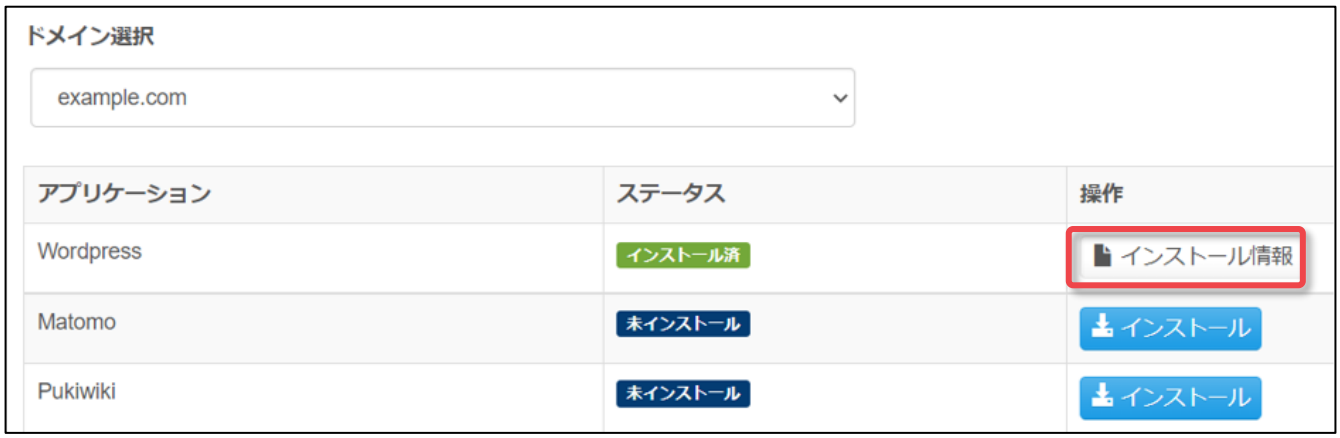
※ 手動で WordPress をバージョンアップする際は、事前にご利用のプラグインや PHP/MySQL 等のバージョンとの互換性をご確認ください。

※ 自動更新の切り替え方法についてはサポート対象外となります。各サイトや市販本などをご参照ください。

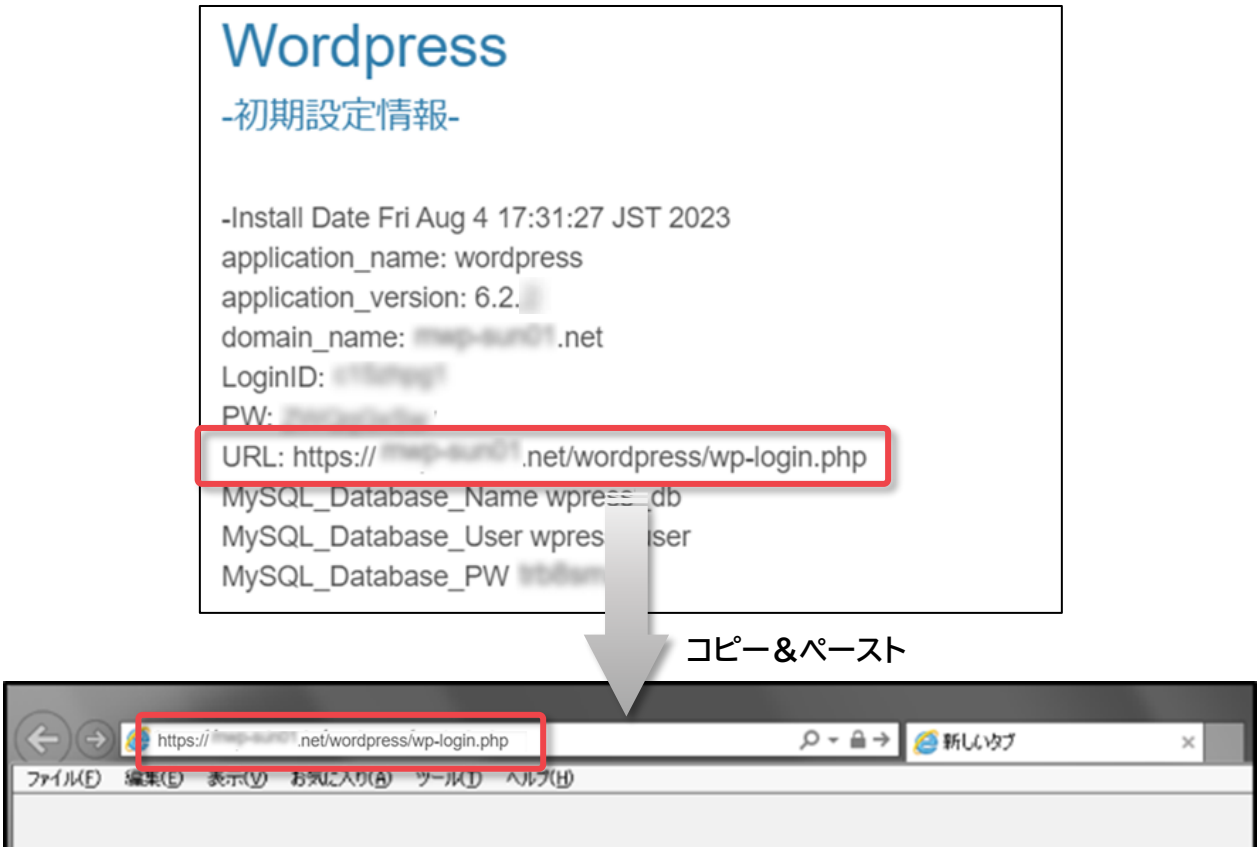
4.2.3. 追加アプリの管理画面

インストールした「追加アプリ」の管理画面へアクセスする方法について、
ここでは **WordPress を例**にして、ご説明します。

1） コントロールパネルの「追加アプリ」から、[インストール情報] をクリックします。



2） インストール情報（初期設定情報）に表示されている 管理画面の「URL」を、ウェブブラウザで開いてください。



3） ログイン画面が表示されたら、インストール情報に表示されていた［ユーザー名 (LoginID)］と［パスワード (PW)］を入力して、［ログイン］をクリックします。

4） ログインすると、下図のような管理画面が表示されます。該当アプリの管理や各種設定を行ってください。

※ 管理画面は「各追加アプリ」ごとに異なります。

注意

- **アクセス解析（Matomo）**については、別途、追加設定が必要になります。「4.2.4 Matomo（トラッキングコード）の設定」を、ご参照ください。
- それ以外の追加アプリについては、インストール完了後すぐに、ご利用可能です。

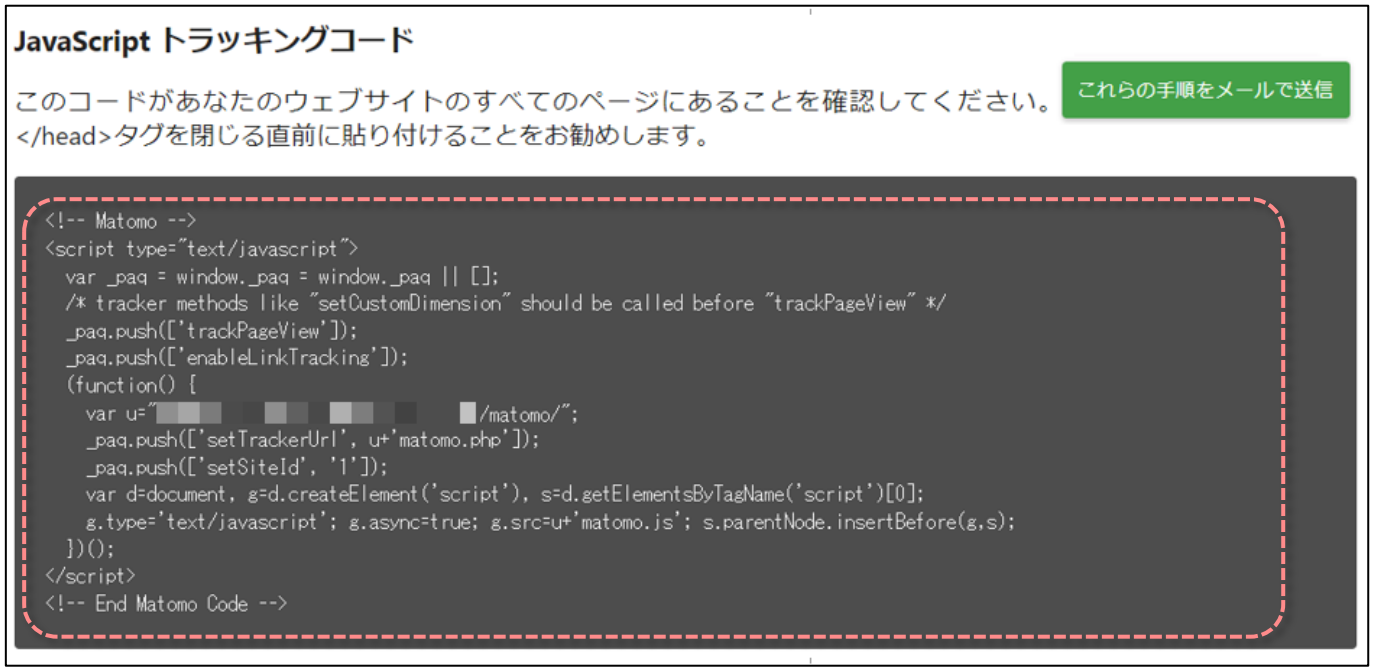
4.2.4. Matomo（トラッキングコード）の設定

アクセス解析ソフトウェアの Matomo を利用するには、**解析用のトラッキングタグをウェブサイトに埋め込む**必要があります。

1） Matomo のインストール情報（初期設定情報）に表示されている 管理画面の「URL」を、ウェブブラウザで開いてください。

2） Matomo サインイン画面が表示されたら、インストール情報に表示されていた［ユーザー名 (LoginID)］と［パスワード (PW)］を入力して、［サインイン］をクリックします。

3） 表示された画面の下部に「JavaScript トラッキングコード」が表示されます。
<!-- Matomo --> から <!-- End Matomo Code --> までをコピーして、ウェブサイトの解析を行う全てのページに貼り付けます。



注意

- トラッキングコードの埋め込み場所は、**</head>タグを閉じる直前** をお勧めします。
- 動的コンテンツへの埋め込みについてはサポートしていません。

4.2.5. 追加アプリの削除/再インストールについて

追加アプリを削除する場合は、各追加したアプリの「ファイル」と「ディレクトリ」を削除する必要があります。その後、再度インストールを行うことにより再インストールも可能です。

注意

- 本章の手順を実行する前に、バックアップしておく事をお勧めします。
- 現時点のインストール先が、デフォルトドメイン（c*******.mwprem.net）か 独自ドメインかによって、削除するディレクトリが異なりますので、十分にご注意ください。

現在のインストール先が デフォルトドメイン（c*****.meprem.net）の場合**

削除が必要なファイル/ディレクトリは、以下の通りです。

追加アプリ名	削除ファイル・ディレクトリ
WordPress	/www/htdocs/wordpress /users/サーバー管理者 ID/.wordpress_ドメイン名
Matomo	/www/htdocs/matomo /users/サーバー管理者 ID/.matomo_ドメイン名
Pukiwiki	/www/htdocs/pukiwiki /users/サーバー管理者 ID/.pukiwiki_ドメイン名
Cybozu	/users/サーバー管理者 ID/cbag(数字) /www/cgi-bin/cbag(数字) /www/htdocs/cb1060 /users/サーバー管理者 ID/.cybozu_ドメイン名
Eccube	/www/htdocs/shop /users/サーバー管理者 ID/eccube_data /users/サーバー管理者 ID/.eccube_ドメイン名
OpenPNE	① /www/htdocs/openpne ② /users/サーバー管理者 ID/openpne ③ /users/サーバー管理者 ID/.openpne_ドメイン名

※ パッケージ版「サイボウズ Office 10」の販売・サポート終了に伴い、Biz メール&ウェブでのサイボウズ Office10 の提供（コントロールパネルからのインストール）は終了しました。
※ EC-CUBE と OpenPNE は PHP8.x ではご利用いただけません。

警告

- **OpenPNE ファイル/ディレクトリは、必ず①②③の順に削除してください。**

※ 削除手順を誤ってしまった場合は、サポート窓口へご相談ください。

現在のインストール先が 独自ドメインの場合

削除が必要なファイル/ディレクトリは、以下の通りです。

追加アプリ名	削除ファイル・ディレクトリ
WordPress	/users/ドメイン管理者 ID/www/ドメイン名/wordpress /users/サーバー管理者 ID/.wordpress_ドメイン名
Matomo	/users/ドメイン管理者 ID/www/ドメイン名/matomo /users/サーバー管理者 ID/.matomo_ドメイン名
Pukiwiki	/users/ドメイン管理者 ID/www/ドメイン名/pukiwiki /users/サーバー管理者 ID/.pukiwiki_ドメイン名
Cybozu	/users/ドメイン管理者 ID/cbag(数字) /users/ドメイン管理者 ID/www/cgi-bin/cbag(数字) /users/ドメイン管理者 ID/www/ドメイン名/cb1060 /users/サーバー管理者 ID/.cybozu_ドメイン名
Eccube	/users/ドメイン管理者 ID/www/ドメイン名/shop /users/ドメイン管理者 ID/eccube_data /users/サーバー管理者 ID/.eccube_ドメイン名
OpenPNE	① /users/ドメイン管理者 ID/www/ドメイン名/openpne ② /users/ドメイン管理者 ID/openpne ③ /users/サーバー管理者 ID/.openpne_ドメイン名

※ パッケージ版「サイボウズ Office 10」の販売・サポート終了に伴い、Biz メール＆ウェブでのサイボウズ Office10 の提供（コントロールパネルからのインストール）は終了しました。
※ EC-CUBE と OpenPNE は PHP8.x ではご利用いただけません。

警告

- **OpenPNE ファイル/ディレクトリは、必ず①②③の順に削除してください。**

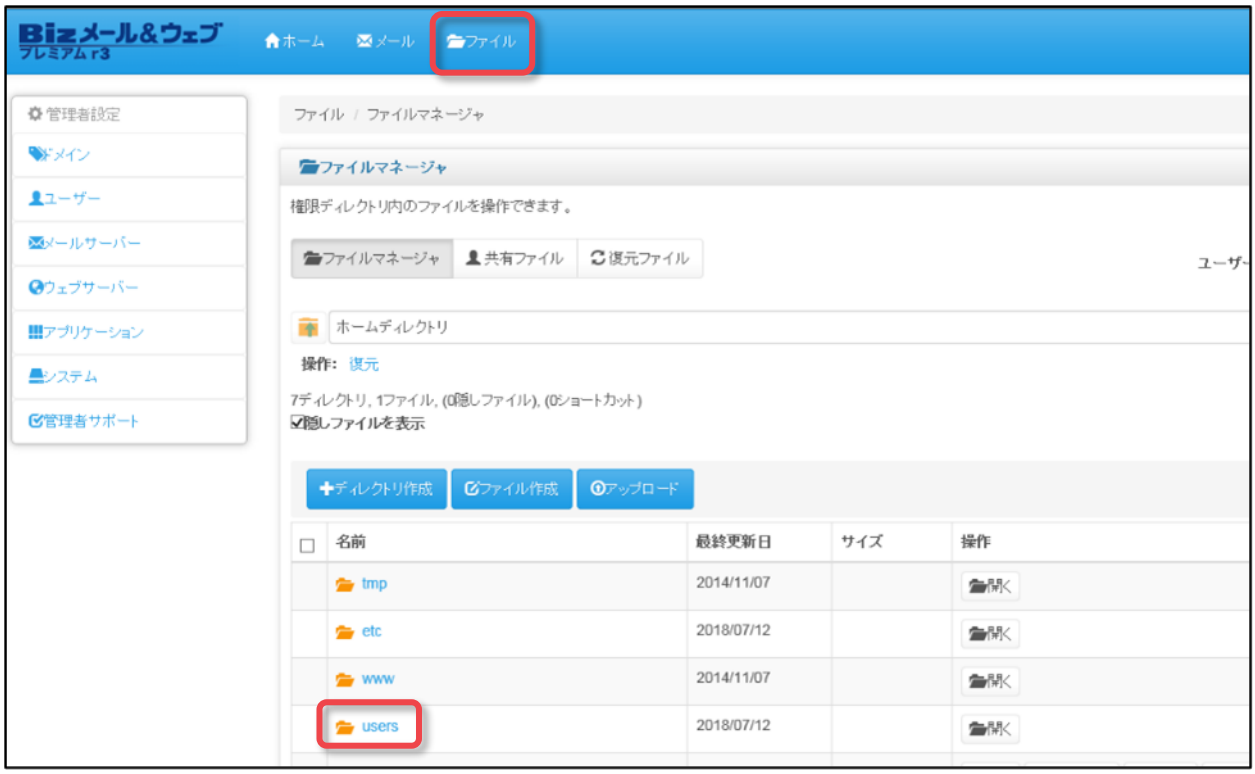
※ 削除手順を誤ってしまった場合は、サポート窓口へご相談ください。

再インストールの手順

ここでは、追加アプリを再インストールする手順を、**Wordpress を例**にしてご説明します。

始めに「.wordpress_ドメイン名」のファイルを削除します。

1） コントロールパネルの上部から［ファイル］をクリックして、ファイルマネージャを表示させたら、ディレクトリー覧の［users］をクリックします。



2） 「users」ディレクトリ内が表示されたら、[*サーバー管理者 ID*]のディレクトリをクリックします。

3） 「*サーバー管理者 ID*」のフォルダ内が表示されたら、「.wordpress_*ドメイン名*」のチェックボックスを選択して、［削除］をクリックします。

4） 削除の確認画面が表示されたら、ファイルに間違いがないことを確認して［削除］をクリックします。

5） 「".wordpress_*ドメイン名*" は削除されました。」と表示されたら、削除は完了です。

次に、追加アプリ（ここでは Wordpress）のディレクトリを削除します。

6）　［ホームディレクトリ］をクリックして、ファイルマネージャのトップ画面から［users］をクリックします。

7）　「ドメイン管理者のディレクトリ」をクリックします。

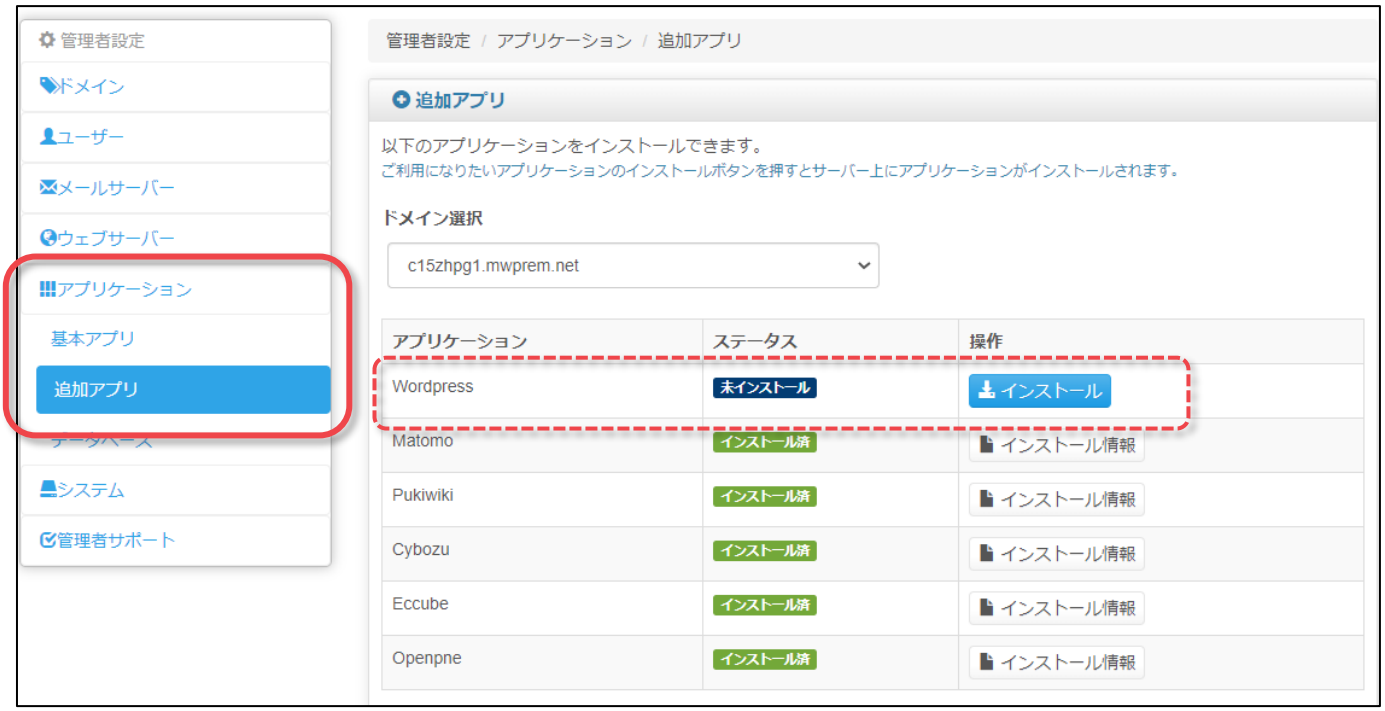
8） 「ドメイン管理者のディレクトリ」内にある［www］をクリックして、続いて「ドメイン名のディレクトリ」をクリックします。

9） 「ドメイン名のディレクトリ」内にある［wordpress］のチェックボックスを選択して、［削除］をクリックします。

１０） 削除の確認画面が表示されたら、ディレクトリに間違いがないことを確認して［削除］をクリックします。

１１） 「Wordpress は削除されました。」と表示されたら、アプリのディレクトリ削除は完了です。

１２） 左メニューの「アプリケーション」から「追加アプリ」画面を開くと、該当の追加アプリ（ここでは Wordpress）が「未インストール」の状態になります。
再インストールを行う場合は、この画面で「インストール」をクリックします。



4.3. データベース

4.3.1. 利用可能なデータベース

Biz メール&ウェブ プレミアムでは、MySQL と PostgreSQL が利用可能です。

データベース	バージョン
MySQL	8.0 系[*1] / 8.4 系 *1 提供元のセキュリティサポート終了に伴い、本サービスでは 2026 年 3 月 31 日までの提供となります。2026 年 2 月下旬より順次、弊社側で MySQL8.4 系への切り替え工事を実施する予定です。この場合、バックアップの取得や動作確認および MySQL8.0 系への切り戻しはできませんので、MySQL8.0 系をご利用の場合は、お客さま側で 2026 年 2 月中旬までに MySQL8.4 系に切替えてください。 **MySQL8.0 提供終了のお知らせ** https://support.ntt.com/mw-premiumr3/information/detail/pid2500002af5/
PostgreSQL	12 系
phpMyAdmin	4.4 系[*2] / 5.0 系[*2] / 5.2 系 *2 PHP5.4 系と 7.4 系の提供が終了しているため、今後コントロールパネルには表示されなくなる予定です。
phpPgAdmin	5.6 系 ※ PHP8.x では phpPgAdmin をご利用いただけません。 pgAdmin をご利用ください。
pgAdmin	9 系

アドバイス

ご利用可能なソフトウェアやアプリケーションなどのバージョンについては、以下の弊社サイトをご参照ください。

ソフトウェアのバージョン｜Biz メール&ウェブ プレミアム
https://www.ntt.com/business/services/cloud/rental-server/vps/service23.html

4.3.2. MySQL の利用開始（初期化）

「データベース」画面から、MySQL の設定変更・起動と停止・パスワード変更が可能です。
なお、コントロールパネルから MySQL を最初に起動した場合に限り、MySQL を初期化する必要があります。

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、MySQL の操作欄にある［利用開始］をクリックします。

2） 初めて使用する場合は、下図の「利用開始設定」画面が表示されます。
パスワードを入力して、［利用を開始する］をクリックしてください。

注意

パスワードで利用可能な文字種や記号は以下の通りです。

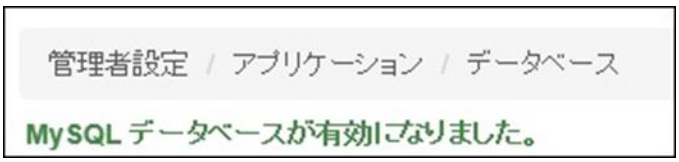
- パスワードは 8～32 文字の長さが必要です。
- 英大文字、英小文字、数字、記号をそれぞれ 1 文字以上含む必要があります。
- パスワードに利用可能な記号は、次のとおりです。
  @ # $ % ^ * ( ) _ + = - &

3） 「MySQL を初期化しました。」と表示されたら、完了です。

4.3.3. MySQL の利用開始

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、MySQL の操作欄にある［起動］をクリックします。

2） 「MySQL データベースが有効になりました。」と表示されたら、MySQL の起動は完了です。



4.3.4. MySQL の停止

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、MySQL の操作欄にある［停止］をクリックします。

2） 「MySQL データベースが無効になりました。」と表示されたら、完了です。

注意

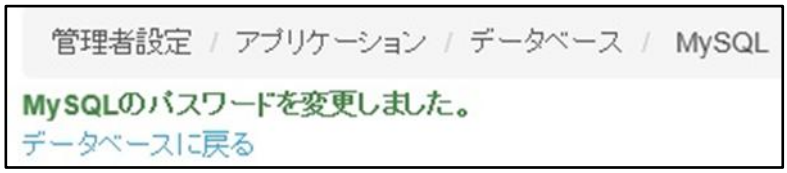
MySQL を利用しているアプリケーションがある場合は、MySQL を無効にすると正常にご利用できなくなりますので、ご注意ください。

4.3.5. MySQL のパスワード変更

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、MySQL の操作欄にある［設定］をクリックします。

2） パスワード変更画面で新しい［パスワード］を入力して、［保存］をクリックします。

3） 「MySQL のパスワードを変更しました。」と表示されたら、完了です。



注意

MySQL を利用しているアプリケーションがある場合は、MySQL のパスワードを変更すると正常にご利用できなくなります。該当のアプリケーション側に設定している MySQL のパスワードも、変更後の新しいパスワードに修正してください。

4.3.6. MySQL のバージョン変更

MySQL 提供元のサポート終了（EOL）のタイミングにより、Biz メール＆ウェブで提供する MySQL のバージョンが複数存在する場合は、以下の手順でバージョンを変更できます。

注意

- MySQL を上位バージョンへ切り替える場合は、データベースは自動で移行します。
  下位バージョンへ切り替える場合は、データベースは移行されません。

  例）MySQL8.0 系→8.4 系へ切替える場合：データベースは自動で移行される
  MySQL8.4 系→8.0 系へ切替える場合：データベースは移行されない

- 設定ファイル（my.cnf）は、バージョン毎に設置されているため、変更前バージョンの設定ファイル（my.cnf）は引き継がれません。
  設定ファイル（my.cnf）をカスタマイズしている場合は、変更後バージョンの設定ファイル（my.cnf）を編集する必要があります。

※ 設定ファイル（my.cnf）の［保存］をクリックすると MySQL が再起動します。

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、MySQL の操作欄にある［設定］をクリックします

以降の画面表示は、バージョン 8.0 系から 8.4 系に変更する場合を例にしています。

2） 画面下部の［バージョン］欄で以下を操作します。

①［パスワード］に MySQL のパスワードを入力する
②［MySQLx.x にバージョン変更］をクリックする

注意

- パスワードが不明な場合は「4.3.5　MySQL のパスワード変更」の手順で変更できますが、MySQL を利用しているアプリケーション側に設定している MySQL のパスワードも、変更後の新しいパスワードに修正する必要があります。
- ［MySQLx.x にバージョン変更］をクリックすると、MySQL が再起動します。

3） バージョン変更を確認するダイアログが表示されたら［OK］をクリックします。

4） バージョンが変更された旨のメッセージが表示されたら完了です。

4.3.7. MySQL の利用について

■ MySQL への接続について

PHP からの MySQL 接続や ODBC 等を利用する場合に、下記の設定が必要です。

情報	内容
ポート番号	3306
接続ホスト名	お客さまドメイン名、または Web サーバーの IP アドレス、または localhost
データベース名	使用するデータベース名
ID	データベースへアクセスできる権限を持つ MySQL ユーザー名
パスワード	MySQL アカウント作成時に設定したパスワード

※ ストレージエンジンは InnoDB です。

注意

<Biz メール&ウェブ プレミアム サーバー以外 からの ODBC 接続について>

- MySQL ユーザーの特権変更および my.cnf での設定が必要です。

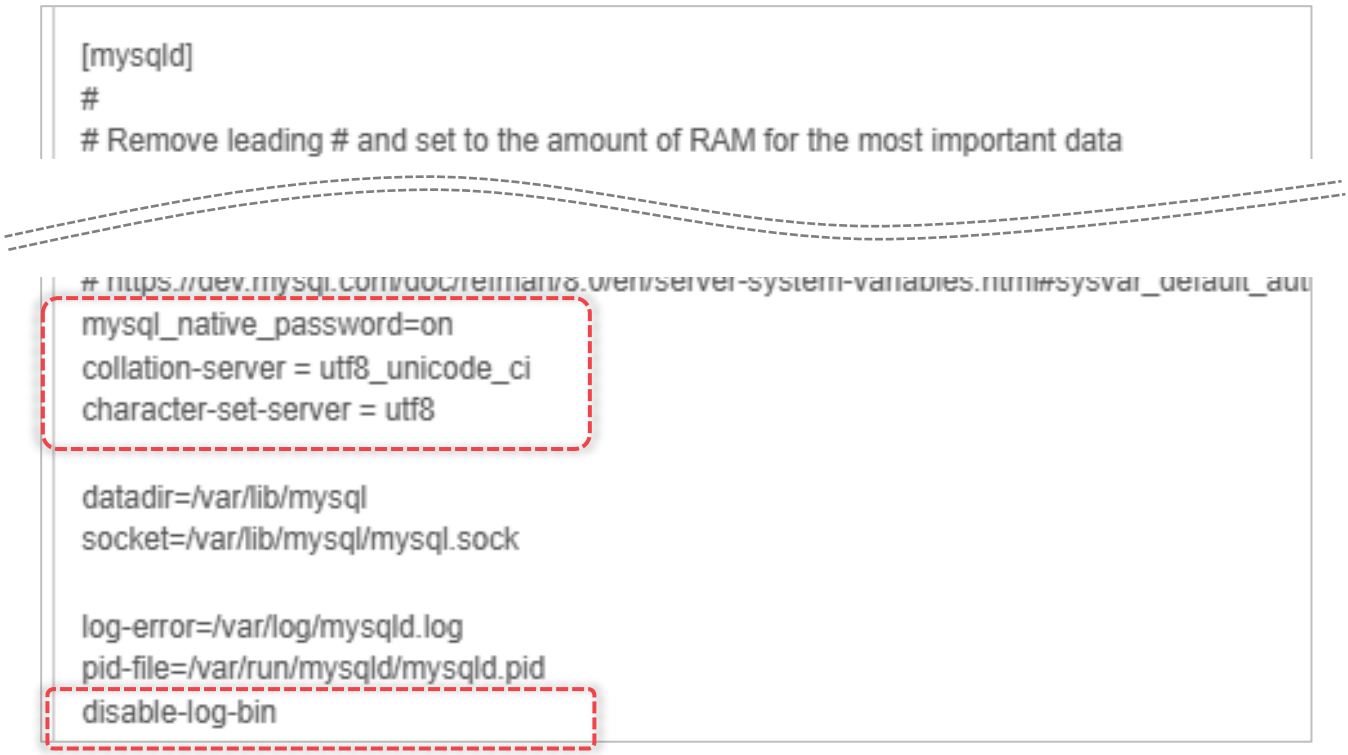
※ my.cnf は、コントロールパネルの［データベース］- MySQL の［設定］から編集可能です。

- 3306 ポートが利用可能な状態か、コントロールパネルの［システム］-［IP アクセス制限］でご確認ください。

■ MySQL8.4 系の設定ファイル（my.cnf）について

Biz メール＆ウェブで提供している設定ファイル（my.cnf）は、［mysqld］に以下の記述を追加しています。

- mysql_native_password=on
  認証方式「mysql_native_password」を有効化しています
- collation-server = utf8_unicode_ci
  MySQL でデータをソートする際等のルールの初期値を"utf8_unicode_ci"に設定しています
- character-set-server = utf8
  MySQL で利用する文字コードの初期値を"utf8"に設定しています
- disable-log-bin
  バイナリログ出力を無効化しています



注意

上述の記述はお客さまのご利用方法に合わせて編集することが可能ですが、
バイナリログに関しては、海外からの不正アクセスや攻撃等によりログが大量に出力されることでディスク容量を圧迫し、サーバーの安定稼働に支障をきたす恐れがあるため無効にしています。
バイナリログの出力を有効にする必要がある場合は、以下の FAQ の「注意事項」および「管理」についてご確認のうえ記述を変更してください。

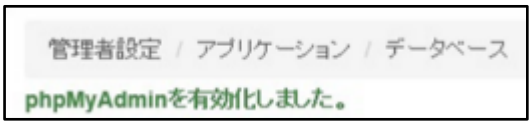
MySQL のバイナリログ（binlog）は出力されますか｜よくあるご質問
https://support.ntt.com/mw-premiumr3/faq/detail/pid2300002a3l/

4.3.8. phpMyAdmin の起動

MySQL をホームページ上から管理するためのソフト「phpMyAdmin」を有効化する方法を、ご説明します。

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、phpMyAdmin の操作欄にある［有効化］をクリックします。

2） 「phpMyAdmin を有効化しました。」と表示されたら、完了です。

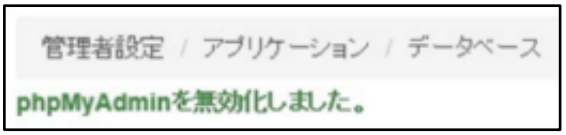


> ⚠ 注意
>
> MySQL サービスを起動していないと、phpMyAdmin をご利用いただけません。
> MySQL が停止している場合は、「4.3.3 MySQL の利用開始」を参照して MySQL を起動してください。

4.3.9. phpMyAdmin の停止

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、phpMyAdmin の操作欄にある［無効化］をクリックします。

2） 「phpMyAdmin を無効化しました。」と表示されたら、完了です。



4.3.10. phpMyAdmin のログイン

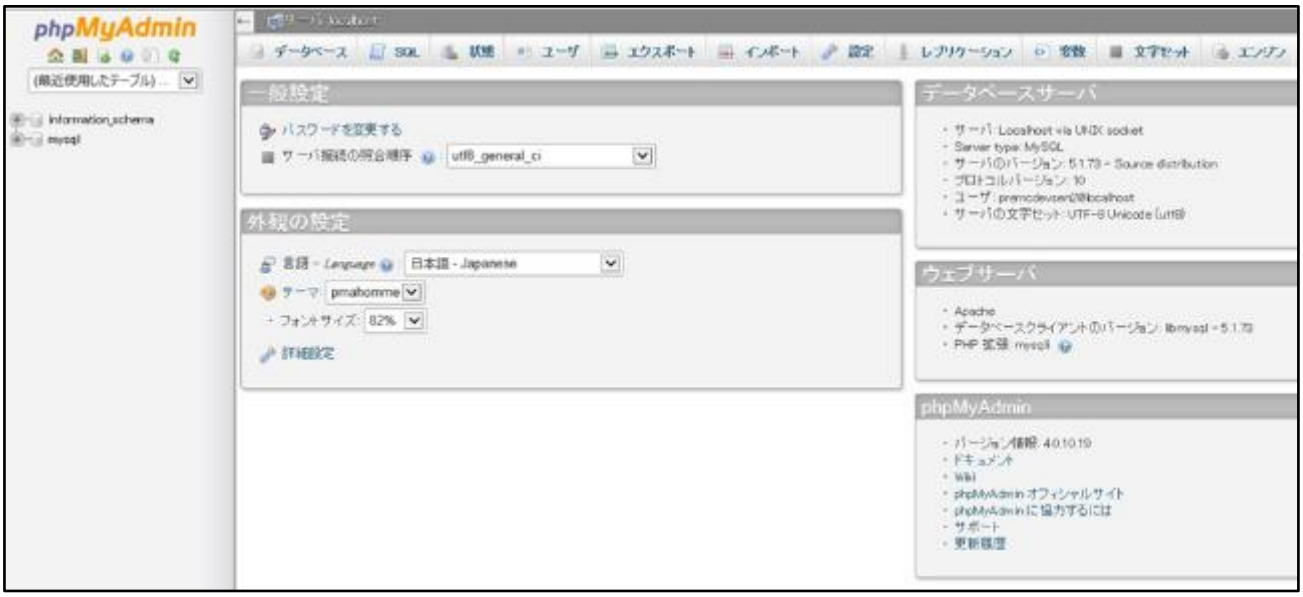
1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、［phpMyAdmin を開く］のアイコン をクリックします。

2） phpMyAdmin のログイン画面が表示されたら、［ユーザー名］と［パスワード］を入力して、［実行］ボタンをクリックします。

アドバイス

ログインには、サーバー管理者 ID と「4.3.5 MySQL のパスワード変更」で設定したパスワードを使用します。

3） ログインが完了すると、下図の管理画面が表示されます。



注意

MySQL や phpMyAdmin の利用方法などは、サポート対象外となります。

4.3.11. phpMyAdmin のバージョン変更

PHP のバージョンによって、phpMyAdmin を対応バージョンに変更する必要があります。

- PHP8.x を使用 → phpMyAdmin5.2 系 + MySQL8.x

※ PHP や MySQL の提供バージョンについては以下をご確認ください。

4.1.2 PHP のバージョン
4.3.1 利用可能なデータベース

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、phpMyAdmin の操作欄にある［設定］をクリックします。

2） バージョン変更画面が開いたら、必ず注意事項と現在のバージョンを確認した上で、問題がなければ［phpMyAdmin*x.x.x* にバージョン変更］をクリックします。

3） 「phpMyAdmin のバージョンを変更しました。」と表示されたら、変更完了です。

4.3.12. PostgreSQL の利用開始（初期化）

「データベース」の画面から、PostgreSQL の設定変更・起動と停止・パスワード変更が可能です。なお、コントロールパネルから PostgreSQL を最初に起動した場合に限り、PostgreSQL を初期化する必要があります。

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、PostgreSQL の操作欄にある［利用開始］をクリックします。

2） 初めて使用する場合は、下図の「利用開始設定」画面が表示されます。
パスワードを入力して、［利用を開始する］をクリックしてください。

注意

パスワードで利用可能な文字種や記号は以下の通りです。

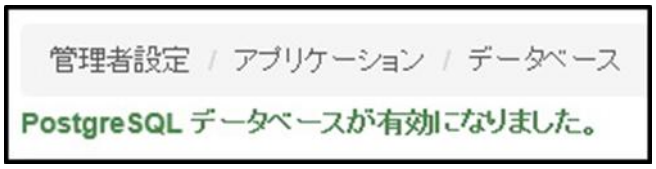
- パスワードは 8～32 文字の長さが必要です。
- 英大文字、英小文字、数字、記号をそれぞれ 1 文字以上含む必要があります。
- パスワードに利用可能な記号は、次のとおりです。
  @ # $ % ^ * ( ) _ + = - &

3） 「PostgreSQL を初期化しました。」と表示されたら、完了です。

4.3.13. PostgreSQL の利用開始

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、PostgreSQL の操作欄にある［起動］をクリックします。

2） 「PostgreSQL データベースが有効になりました。」と表示されたら、PostgreSQL の起動は完了です。



4.3.14. PostgreSQL の停止

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、PostgreSQL の操作欄にある［停止］をクリックします。

2） 「PostgreSQL データベースが無効になりました。」と表示されたら、PostgreSQL の停止は完了です。

注意

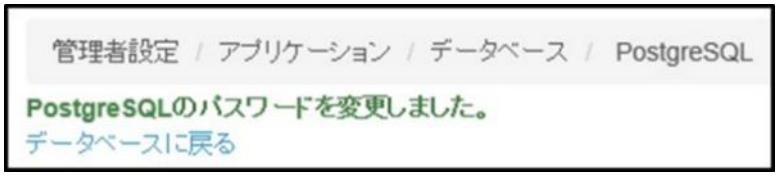
PostgreSQL を利用しているアプリケーションがある場合は、PostgreSQL を無効にすると正常にご利用できなくなりますので、ご注意ください。

4.3.15. PostgreSQL のパスワード変更

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、PostgreSQL の操作欄にある［設定］をクリックします。

2） パスワード変更画面で新しい［パスワード］を入力して、［保存］をクリックします。

3） 「PostgreSQL のパスワードを変更しました。」と表示されたら、完了です。



注意

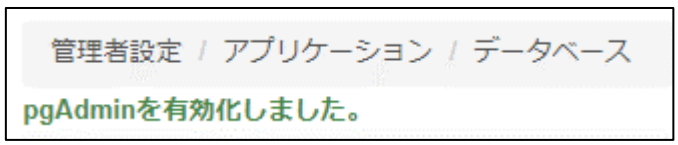
PostgreSQL を利用しているアプリケーションがある場合は、PostgreSQL のパスワードを変更すると正常にご利用できなくなります。該当のアプリケーション側に設定している PostgreSQL のパスワードも、変更後の新しいパスワードに修正してください。

4.3.16. pgAdmin の起動

PostgreSQL を管理するためのソフト「pgAdmin」を有効化する方法を、ご説明します。

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、pgAdmin の操作欄にある［有効化］をクリックします。

2） 「pgAdmin を有効化しました。」と表示されたら、完了です。



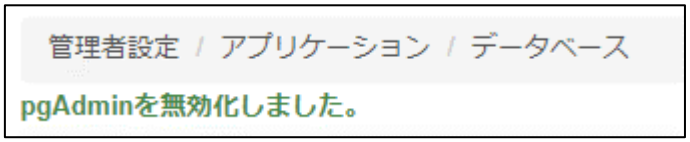
注意

PostgreSQL サービスを起動していないと、pgAdmin をご利用いただけません。
PostgreSQL が停止している場合は、「4.3.13 PostgreSQL の利用開始」を参照して PostgreSQL を起動してください。

4.3.17. pgAdmin の停止

1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、pgAdmin の操作欄にある［無効化］をクリックします。

2） 「pgAdmin を無効化しました。」と表示されたら、完了です。



4.3.18. pgAdmin のログイン

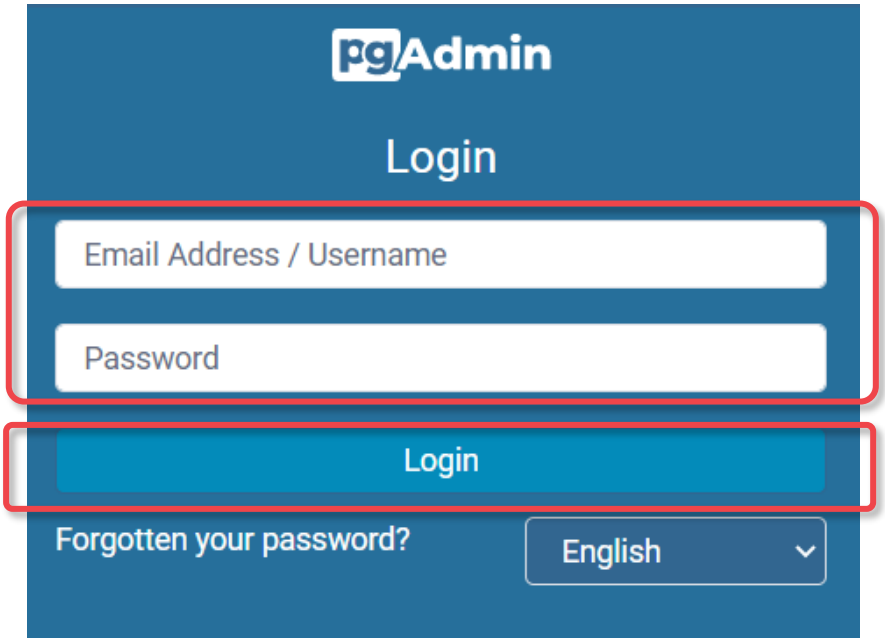
1） コントロールパネルの左メニュー「アプリケーション」から［データベース］をクリックして、pgAdmin の右隣りにある［ログイン情報］をクリックします。

2） pgAdmin ログイン情報画面が表示されたら、［Email Address］と［Password］をメモして、［閉じる］もしくは［pgAdmin を開く］をクリックします。

※［pgAdmin を開く］をクリックした場合は、手順 4）に進んでください。

3） コントロールパネルの画面で、[pgAdmin を開く] のアイコン をクリックします。

4） pgAdmin のログイン画面が表示されたら、手順２）でメモした［Email Address］と［Password］を入力して、［Login］ボタンをクリックします。



5） ログインが完了すると、下図の管理画面が表示されます。

注意

PostgreSQL や pgAdmin の利用/操作方法などは、サポート対象外となります。

4.4. WebDAV

4.4.1. WebDAV の概要

WebDAV(ウェブダブ)機能を使うと、サーバーに、ID・パスワード付きのファイル共有用フォルダを作成して、ファイル共有サーバーとして利用できます。

4.4.2. 共有フォルダとユーザーの追加設定

1） コントロールパネルの左メニュー「アプリケーション」から、[基本アプリ] をクリックします。

2） 「基本アプリ」の画面が表示されたら、[WebDAV] をクリックします。

3） ［新規作成］をクリックします。

4） ［フォルダ名］と［説明］を入力して、［保存］をクリックします。

5） 「*<共有フォルダ名>*を追加しました。」と表示されたら、フォルダの追加は完了です。

続いて、WebDAV のユーザーを追加します。

6）　［ユーザー］をクリックします。

7）　［ユーザー名］と［パスワード］を入力して、［保存］をクリックします。

8）　「*<ユーザーID>*を追加しました。」と表示されたら、ユーザーの追加は完了です。

注意

- メール&ウェブ プレミアムで追加したユーザーと WebDAV のユーザーは、別管理となります。

4.4.3. CarotDAV のインストールと設定

1） CarotDAV をインストールする前に、pgAdmin を［無効化］します。

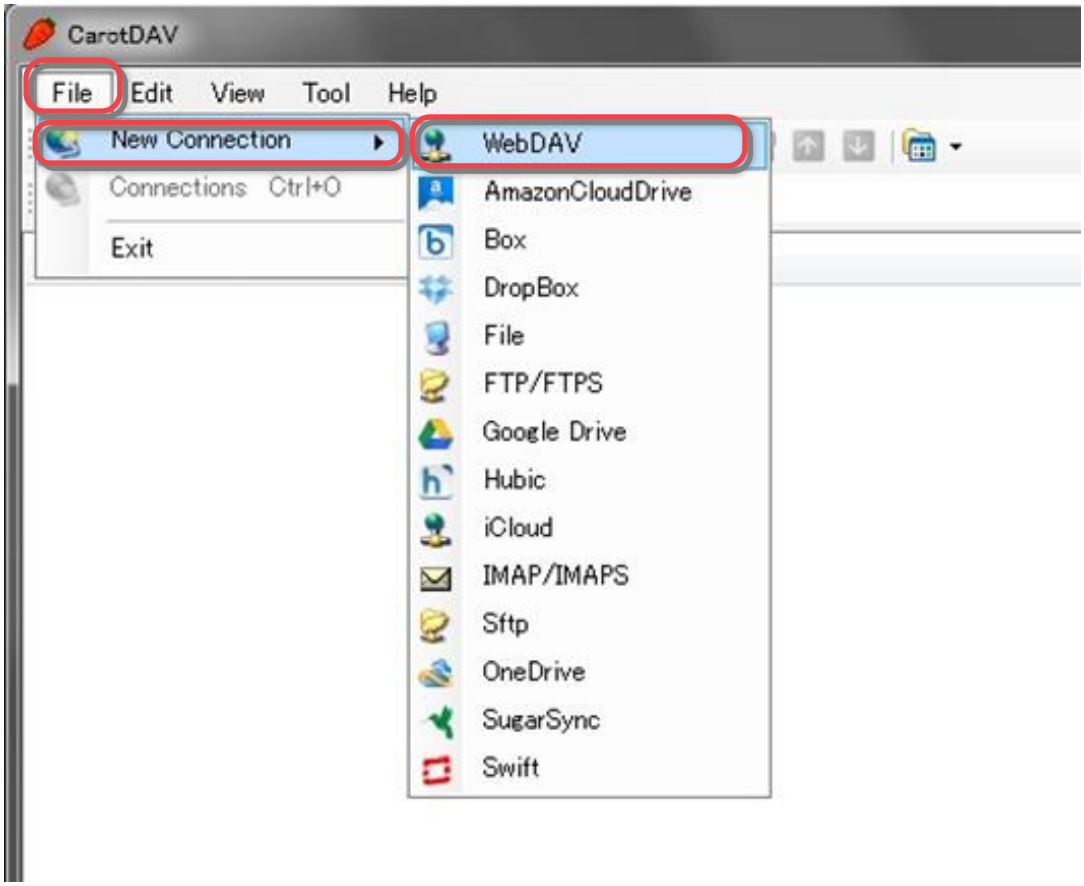
※ pgAdmin を無効化する方法は、「4.3.17 pgAdmin の停止」を参照してください。

> **注意**
>
> - ファイル共有を行う全ての端末にインストールする必要があります。
> - 当ソフトウェアは、一部を除き英語版となります。

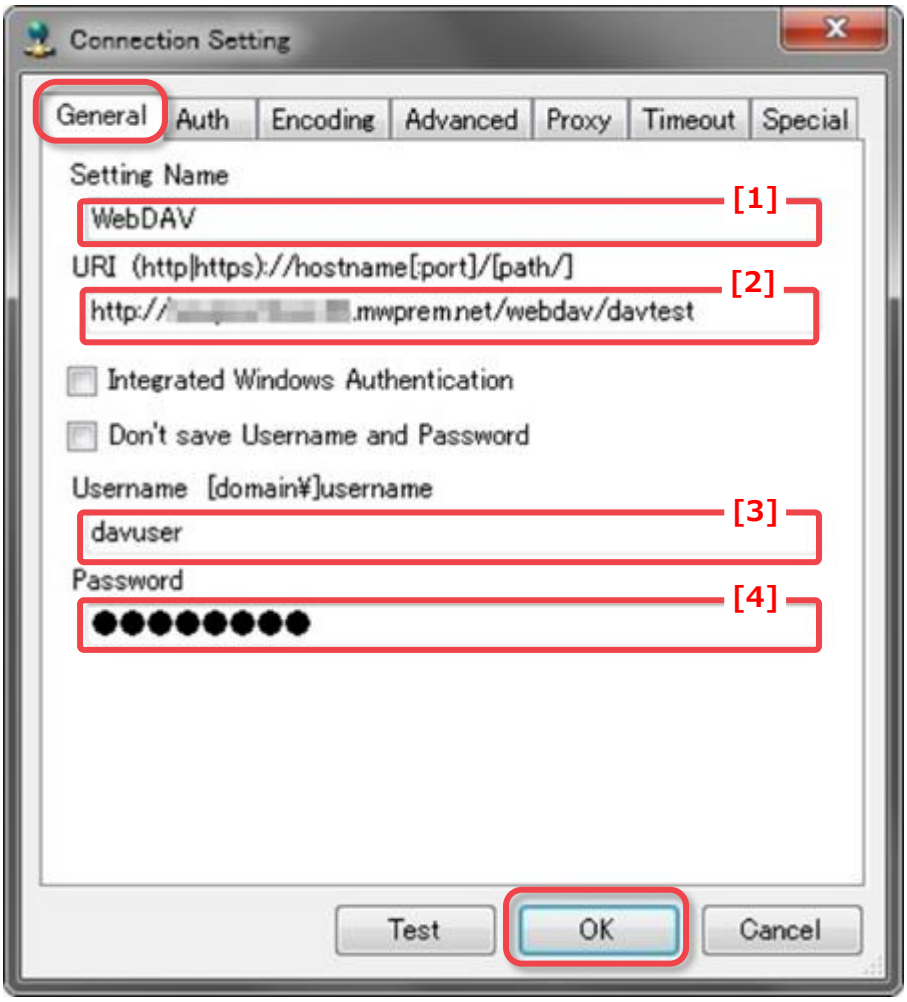
2） 窓の杜（https://forest.watch.impress.co.jp/library/software/carotdav/）等のオンラインソフトウェアを紹介するサイトから、CarotDAV をダウンロードします。

3） ダウンロードしたファイルを実行して、イントールを完了させてください。

4） CarotDAV を起動して［File］をクリックし、「New Connection」から［WebDAV］をクリックします。



5） 「General」タブの必要な項目を入力して、[OK]をクリックします。



	項目	説明
[1]	Setting Name	任意の名前を入力します。
[2]	URI	https://*c******.mwprem.net/webdav/*WebDAV 名(共有フォルダ名)*を入力します。
[3]	Username	「4.4.2 共有フォルダとユーザーの追加設定」で設定した、［ユーザ名］と［パスワード］を入力します。
[4]	Password	

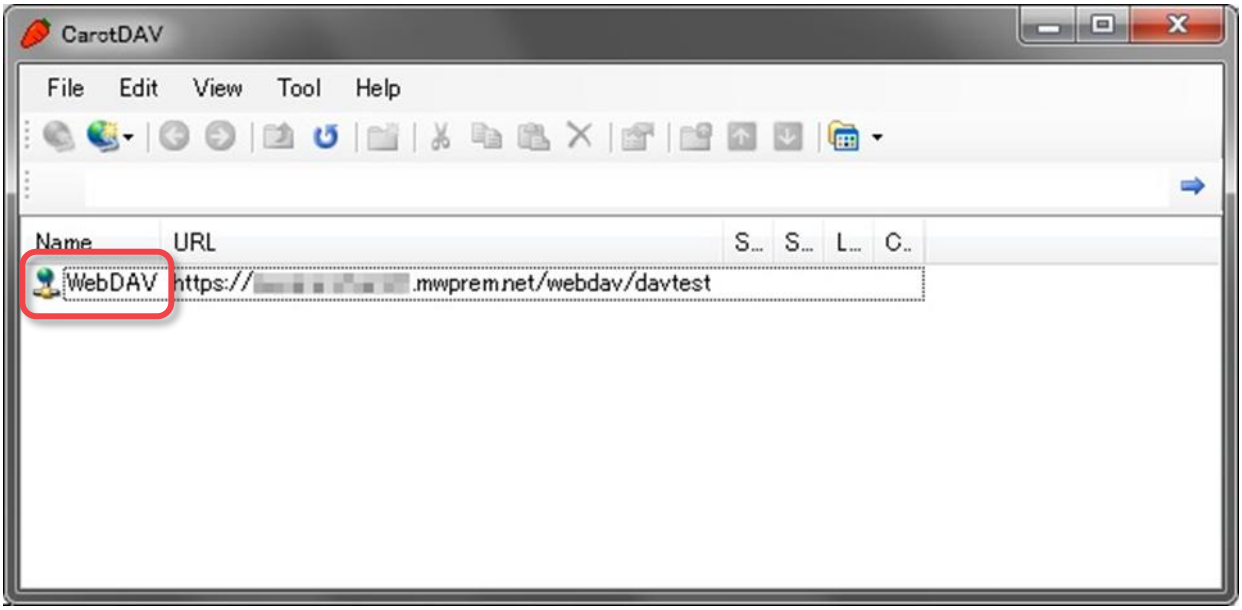
以上で CarotDAV の設定は完了です。

注意

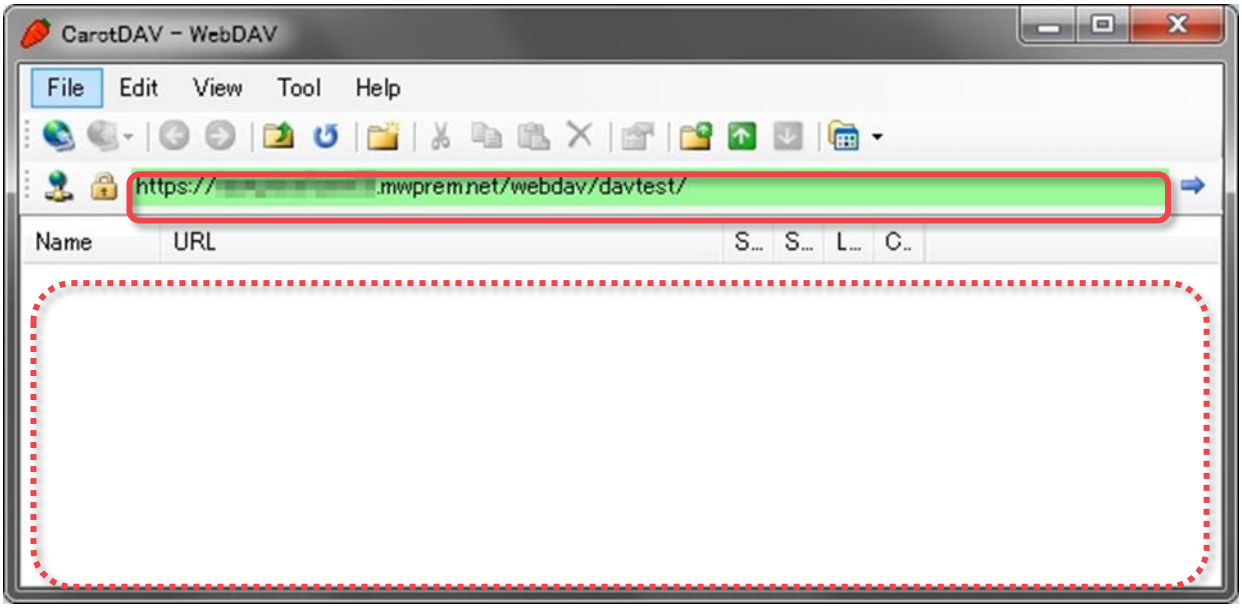
- **［Test］や［OK］がグレーアウト**している場合は、**[2] URI** の入力内容に誤りがあります。コントロールパネルの URL を参考に、再度、入力内容を確認してください。

4.4.4. ファイルのアップロード・ダウンロード

1） 「4.4.3 CarotDAV のインストールと設定」で設定した内容は、下図のように表示されます。サーバーに接続するには、「Name」の項目をダブルクリックします。

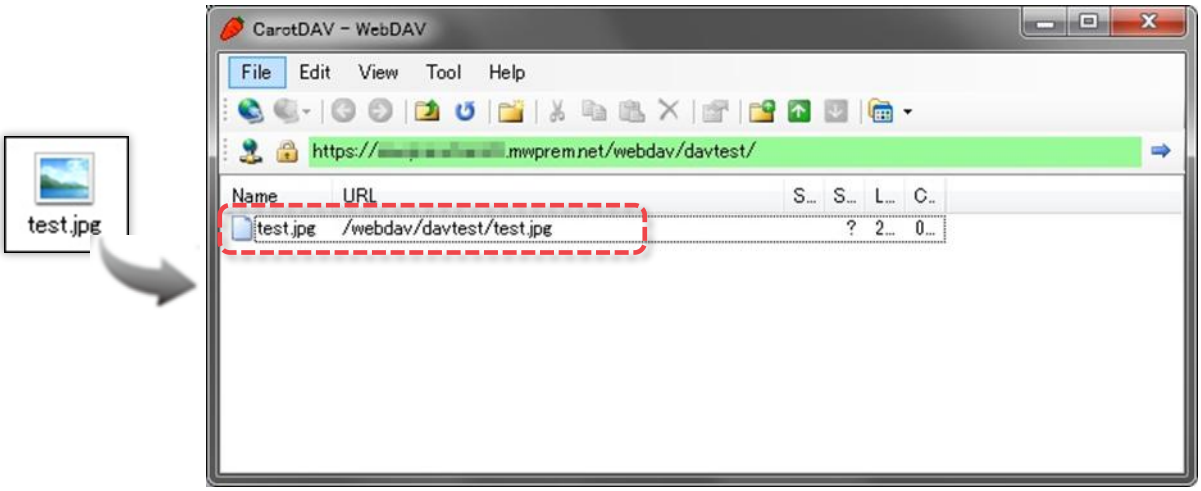


2） アドレス欄が緑色になれば接続できています。

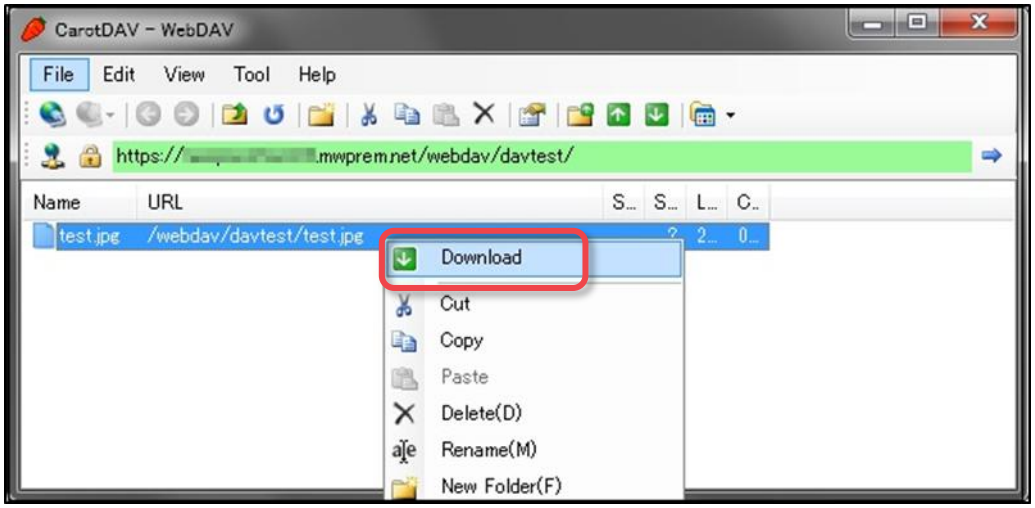


※ 上図の点線内に表示されるのは、サーバー側のファイルです（FTP ソフト等と違い、ローカル側のファイルは表示されません）。

3） アップロードする場合は、ローカルから CarotDAV の画面へ、ファイルをドラッグ＆ドロップします。



4） ダウンロードする場合は、CarotDAV 画面でファイルを右クリックして、[Download]から保存先を選択して、ダウンロードします。



注意

- **ご契約のディスク容量が上限となります。**ユーザーごとの容量制限には依存しません。
  ディスク容量の圧迫を避ける為、不要なファイルは定期的に削除してください。
- **WAF（オプションサービス）を利用している場合、転送（アップロード/ダウンロード）するファイルサイズの上限は 1.5GB まで**となります。
  WAF をご利用でない場合は転送するファイルサイズに上限はありませんが、大容量の添付ファイルを一度に転送すると、**サーバーのレスポンスが低下する可能性があります。**
- CarotDAV のその他の利用方法については、サポート対象外となります。インターネット情報等にてご確認ください。

5　システム

5.1.　定期実行タスク

5.1.1.　　定期実行タスクの概要

定期実行タスクとは、サーバー上で実行可能なコマンドやスクリプトを、自動的に起動するツールのことです。
コントロールパネルの左メニュー「システム」から［定期実行タスク］をクリックして、設定画面にアクセスできます。

注意

- タスク管理を使用する際は、タイムゾーンを確認することを強くお勧めします。スケジュールを設定してからタイムゾーンを変更すると、システムが正常に動作しなくなる可能性があります。
- タイムゾーン変更の手順については、**利用者マニュアルの「2.5 コントロールパネルの設定（日付と時刻）」**を参照してください。

アドバイス

- タスク管理を使用するためには、シェルスクリプトやプログラムを作成し、サーバー上に保存しておくことが必要です。また、該当のスクリプトやプログラムには実行権限が必要です。
- スクリプトやプログラムに関する作成や実装、問題発生時の対処などは、お客さまの自己責任で実施していただきますようお願いいたします。

5.1.2. 定期実行タスクの作成

タスク管理にタスクを作成すると、指定した時間に、自動的にスクリプトが実行されます。

ここでは、『 **test.sh というスクリプトを、毎朝 6 時に自動起動する**』という例をご説明します。（ドメイン管理者のホームに、test.sh があるものとします。）

はじめに、「test.sh」 に実行権限をつけます。

1） コントロールパネル上部の「ファイル」をクリックします。

2） /users/ドメイン管理者 ディレクトリを開き、「test.sh」の［詳細］をクリックします。

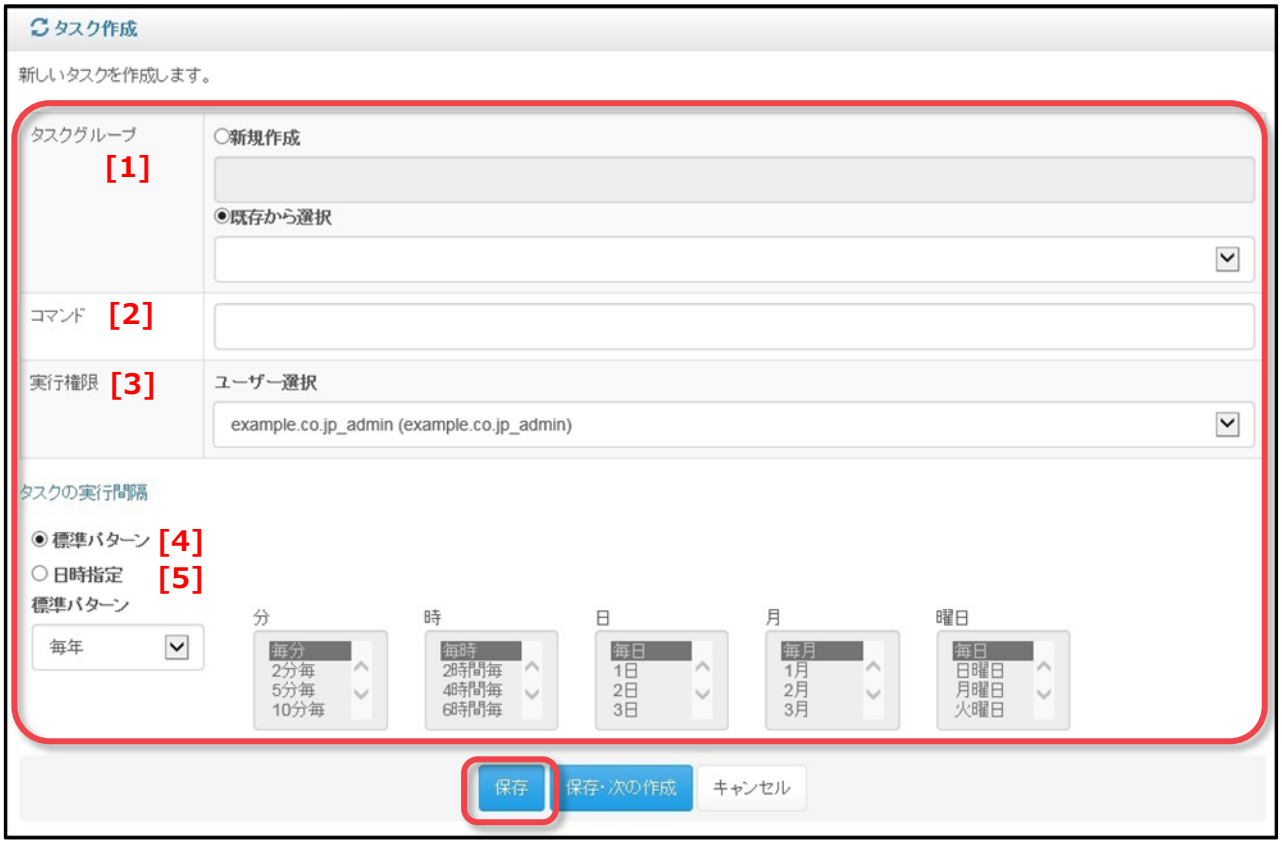
3） 「操作」欄の［属性変更］をクリックします。

4） 所有者の［実行］にチェックを入れて、［保存］をクリックします。

次に、タスク管理にタスクを作成します。

5） コントロールパネル左メニューの「システム」から「定期実行タスク」の画面を開き、［新規作成］をクリックします。

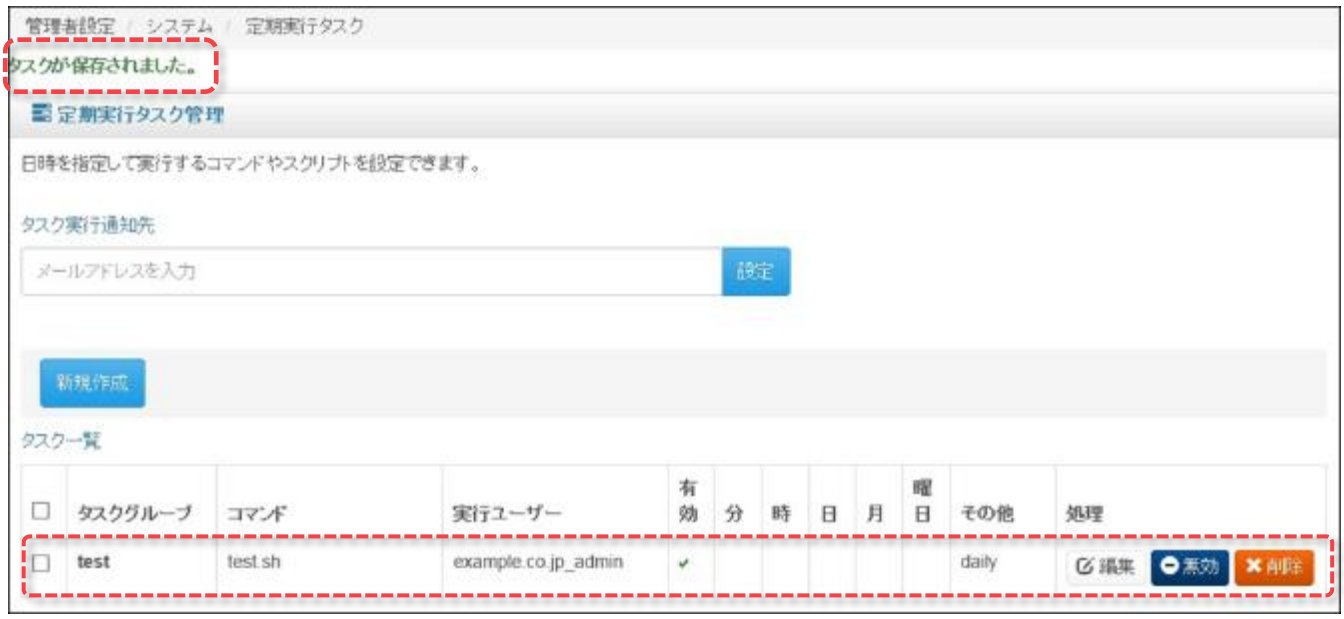
6） 設定項目を選択/入力して［保存］をクリックしてください。



各設定項目について

	設定項目	内容
[1]	タスクグループ	● タスクがたくさんある場合に、グループを作成すると便利です。 **例：**「daily」「weekly」「system」…など ● 作成済みのグループは、［既存から選択］のプルダウンから選択できます。
[2]	コマンド	● スクリプトのパスを入力します。 /usr/home/*サーバー管理者*/users/*ドメイン管理者*/***.sh と入力します。
[3]	実行権限	● タスクの実行を行うユーザーを設定します。
[4]	標準パターン	● ［標準パターン］を選択した場合、プルダウンから、「毎年」「毎月」「毎週」「毎日」「毎時」「リブート時」を選択できます。
[5]	日時指定	● ［日時指定］を選択した場合、詳細なスケジュール時間を設定できます。 **分：** 「毎分」「2 分毎」「5 分毎」「10 分毎」「15 分毎」「0 … 59 分」 から選択 **時：** 「毎時」「2 時間毎」「4 時間毎」「6 時間毎」「0 … 23 時」 から選択 **日：** 「毎日」「1 … 31 日」 から選択 **月：** 「毎月」「1 … 12 月」 から選択 **曜日：**「毎日」「日, 月, 火, 水, 木, 金, 土 曜日」 から選択 各項目の組み合わせにより、次のような日時指定ができます。 **例：**「毎週水曜日の 6:40 に実行」「毎月 1 日の 4 時に実行」…など

7） 「タスクが保存されました。」と表示され、「タスク一覧」に、設定したタスクが反映されたら完了です。



5.1.3. 定期実行タスクの処理

作成済みのタスクを**編集**して別の時間に実行するようにしたり、タスクの**削除**、タスクの**無効化**が可能です。

「タスク一覧」の処理欄から、実行したい処理をクリックしてください。

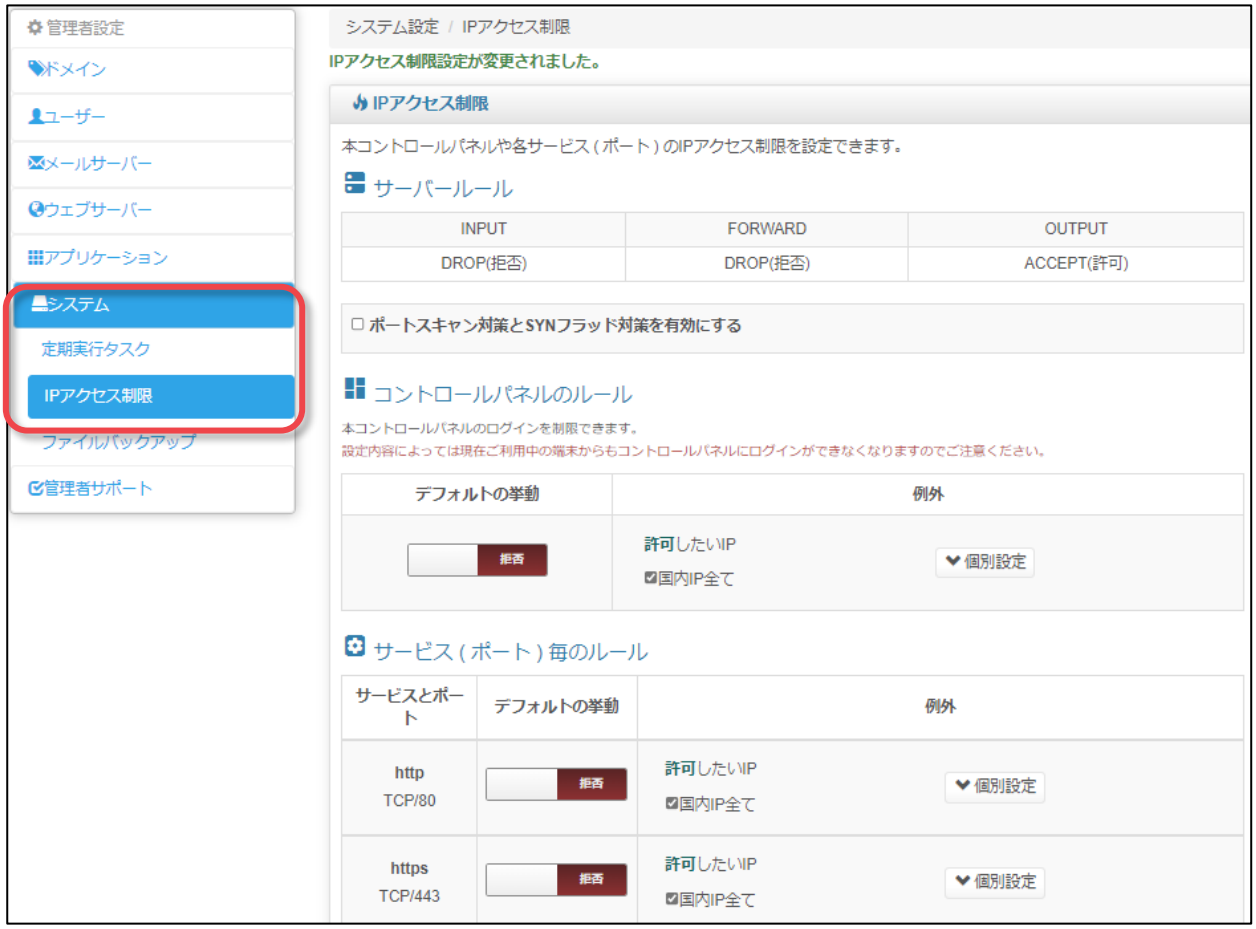
項目	内容
編集	［編集］をクリックすると、タスクの実行時間や、コマンドを別のスクリプトに変更することができます。 ※ タスクの作成時と同じように設定できます。
無効	［無効］をクリックすると、タスクの実行を中止することができます。 ※ 無効なタスクを有効にする場合は、［有効］をクリックします。
削除	［削除］をクリックすると、不要なタスクを削除することができます。

5.2. IP アクセス制限

5.2.1. IP アクセス制限の概要

IP アクセス制限とは、特定の IP アドレスからのアクセスを制限する機能で、外部からの攻撃や不正アクセス防止として利用できます。

コントロールパネルの左メニュー「システム」から［IP アクセス制限］をクリックして、設定画面にアクセスできます。
初期状態では、海外からのアクセスを拒否し、日本国内のみアクセスが許可されています。



アドバイス

海外からの IP アクセス拒否状態を解除する方法については、**セットアップマニュアル「3.2 IP アクセス制限」**を参照してください。

注意

IP アクセス制限を設定する際には、制限対象の IP アドレスを確認いただくことを強くお勧めします。
誤って設定した場合、サーバーへアクセス出来なくなる可能性があります。

5.2.2. 個別設定

ここでは例として、『POP 通信を特定の IP アドレスからアクセスのみを許可し、それ以外は拒否する』場合の設定手順をご説明します。

1） コントロールパネルの左メニュー「システム」から［IP アクセス制限］をクリックします。

2） ［国内 IP 全て］のチェックを外し、［個別設定］をクリックします。

3） 許可する IP アドレスを入力します。

アドバイス

- **追加** をクリックすると、入力項目を増やすことが出来ます。
- **例外の一括解除** をクリックすると、入力した IP アドレスをクリアできます。

4） IP アドレスの入力が完了したら、画面下の［設定を保存する］をクリックします。

5） 確認画面が表示されたら、［OK］をクリックします。

6） 「IP アクセス制限設定が変更されました。」と表示されたら、個別設定は完了です。

アドバイス

個別設定がされている場合は、「○○件設定済」と表示され、［個別設定］をクリックすると内容を確認できます。

コントロールパネルのルール：入力エラーついて

「コントロールパネルのルール」を［拒否］に設定する際、［国内 IP 全て］を選択せず［IP アドレス］も空欄のまま［設定を保存する］をクリックした場合は、【入力エラー】のアラートが表示されて保存できません。

［国内 IP 全て］を選択するか、個別設定の［IP アドレス］を入力してから［設定を保存する］をクリックしてください。

サービス（ポート）のルール： 各項目説明

「IP アクセス制限」を設定する際は、下表を参考に、お客さまのご利用環境に応じてご設定ください。

注意

- 初期設定としての推奨内容となります。
- 制限したサービス・ポートに対して海外の IP アドレスからアクセスする場合は、「個別設定」で該当の IP アドレスを許可する必要があります。
- 下表以外のサービス・ポートには設定出来ません。
- 不正アクセス、または攻撃を完全に防止する機能ではございません。

推奨○： 制限を推奨、推奨 －： 制限を非推奨

サービス	ポート番号	制限対象のサービス	推奨	推奨・非推奨の理由
ポートスキャンと SYN フラッド対策	全ポート	-	○	アクセスが集中した場合、防御機能が働き、サイトの閲覧が出来なくなる可能性があります。
HTTP	80	ホームページを閲覧する（暗号化なし） 例：http://example.jp/	-	ホームページアクセスに支障が出る可能性があります。
HTTP over SSL	443	ホームページを閲覧する（暗号化あり） 例：https://example.jp/ ウェブメール（Active!Mail）の利用	-	https でアクセスする画面（例：資料請求や問合せなどのフォームメール、Active!Mail）の利用に支障が出る可能性があります。
SMTP	25	利用者・外部からのメール送信	-	メール送信に支障が出る可能性があります。
Message submission	587	利用者のメール送信	-	メール送信に支障が出る可能性があります。
POP	110	利用者・外部環境からメールソフトを用いたメール受信（暗号化なし）	○	不正アクセス防止。
POP over SSL	995	利用者・外部環境からメールソフトを用いたメール受信（暗号化あり）	○	不正アクセス防止。
IMAP	143	利用者・外部環境からメールソフトを用いたメールデータの同期 （暗号化なし）	○	不正アクセス防止。
IMAP over SSL	993	利用者・外部環境からメールソフトを用いたメールデータの同期 （暗号化あり）	○	不正アクセス防止。
MySQL	3306	データベースへのアクセス	○	不正アクセス防止。
PostgreSQL	5432	データベースへのアクセス	○	不正アクセス防止。
FTP	21	FTP ソフトでホームページを設置する	○	ホームページ改竄防止

5.3. ファイルバックアップ

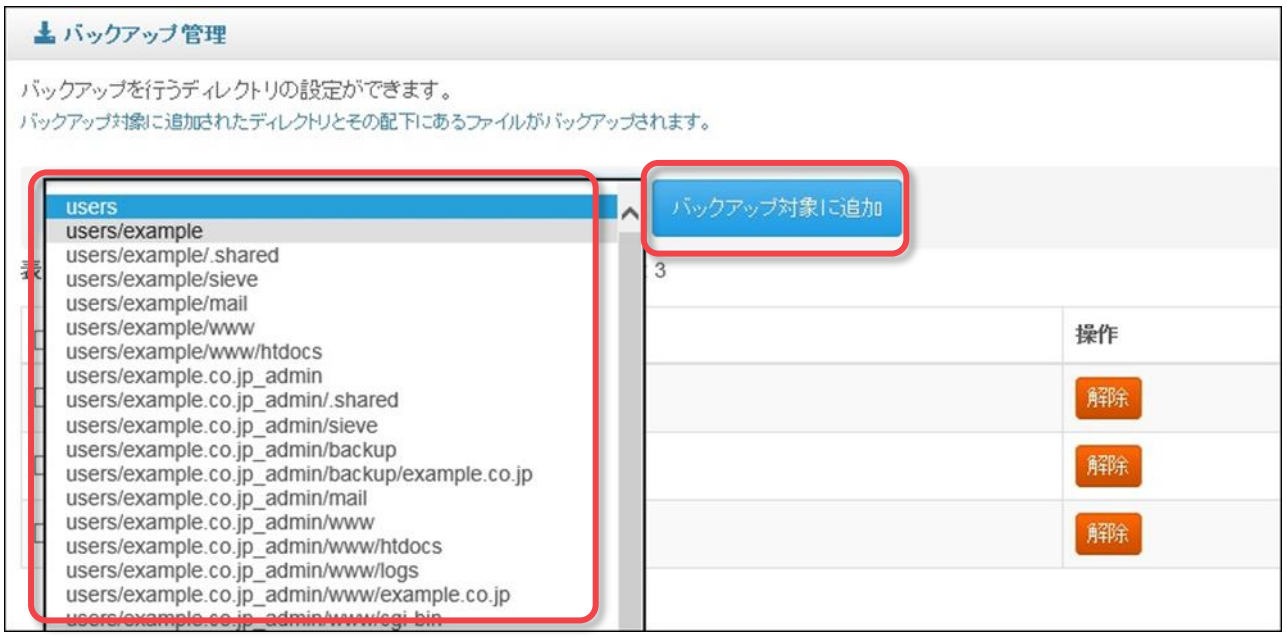
5.3.1. ファイルバックアップの概要

「ファイルバックアップ」を設定すると、ファイルマネージャの「復元ファイル」機能を利用して、ファイルを復元できます。
初期状態では、サーバー上の重要なファイル・ディレクトリはバックアップ対象として設定されています。必要に応じて、個別に追加設定を行ってください。

5.3.2. バックアップ対象の追加

1） コントロールパネルの左メニュー「システム」から［ファイルバックアップ］をクリックします。

2） バックアップしたいディレクトリをプルダウンから選択して、［バックアップ対象に追加］をクリックします。



3） 確認画面が表示されたら、[追加]をクリックします。

4） バックアップを行うディレクトリの一覧に追加されていれば、完了です。

アドバイス

バックアップ対象に追加されたディレクトリは、翌日以降に、ファイルマネージャから復元することが出来るようになります。

5.4. 管理者パスワード再設定

サーバー管理者 ID のパスワードを紛失・忘れてしまった場合は、再設定をすることが可能です。

1） ログインに失敗した場合は、下図のようなメッセージが表示されます。
［パスワードを忘れた方はこちら］をクリックしてください。

2） 再設定の画面が開いたら、**セットアップマニュアル「3.1.2 パスワード再設定用 URL 通知メールアドレス登録方法」**で設定したメールアドレスを入力して、［パスワード再設定］をクリックします。

3） 入力した「パスワード再設定用 URL 通知メールアドレス」に、パスワード再設定用の URL がメールで送信されます。

パスワード再設定通知メールアドレスへ、再設定の案内メールを送信しました。メールをご確認ください。

4） 以下のような内容のメールが送信されますので、リンクをクリックしてください。

件名： Biz メール&ウェブ コントロールパネル パスワード再設定
差出人： *サーバー管理者のアドレス*

本文： Biz メール&ウェブ コントロールパネルからのお知らせです。
お客様の操作により、Biz メール&ウェブ コントロールパネル 管理者アカウントの
ログインパスワード再設定(リセット)要求が行われました。

管理者 ID: [redacted]

管理者アカウントのパスワードを再設定する場合は、以下の URL よりご設定ください。
https://bizmw-login.com/*ユーザ ID(管理者)*/reset_password?token=＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＝

URL の有効期限: 2021/＊＊/＊＊ 12:00:00 まで

5） パスワード再設定画面が表示されたら、「新しいパスワード」を入力して、［保存］をクリックします。

6） 「パスワードが更新されました。」と表示されたら、パスワードの再設定は完了です。再設定したパスワードで、コントロールパネルへのログインをお試しください。

パスワードが更新されました。

5.5. リソース負荷状況の確認

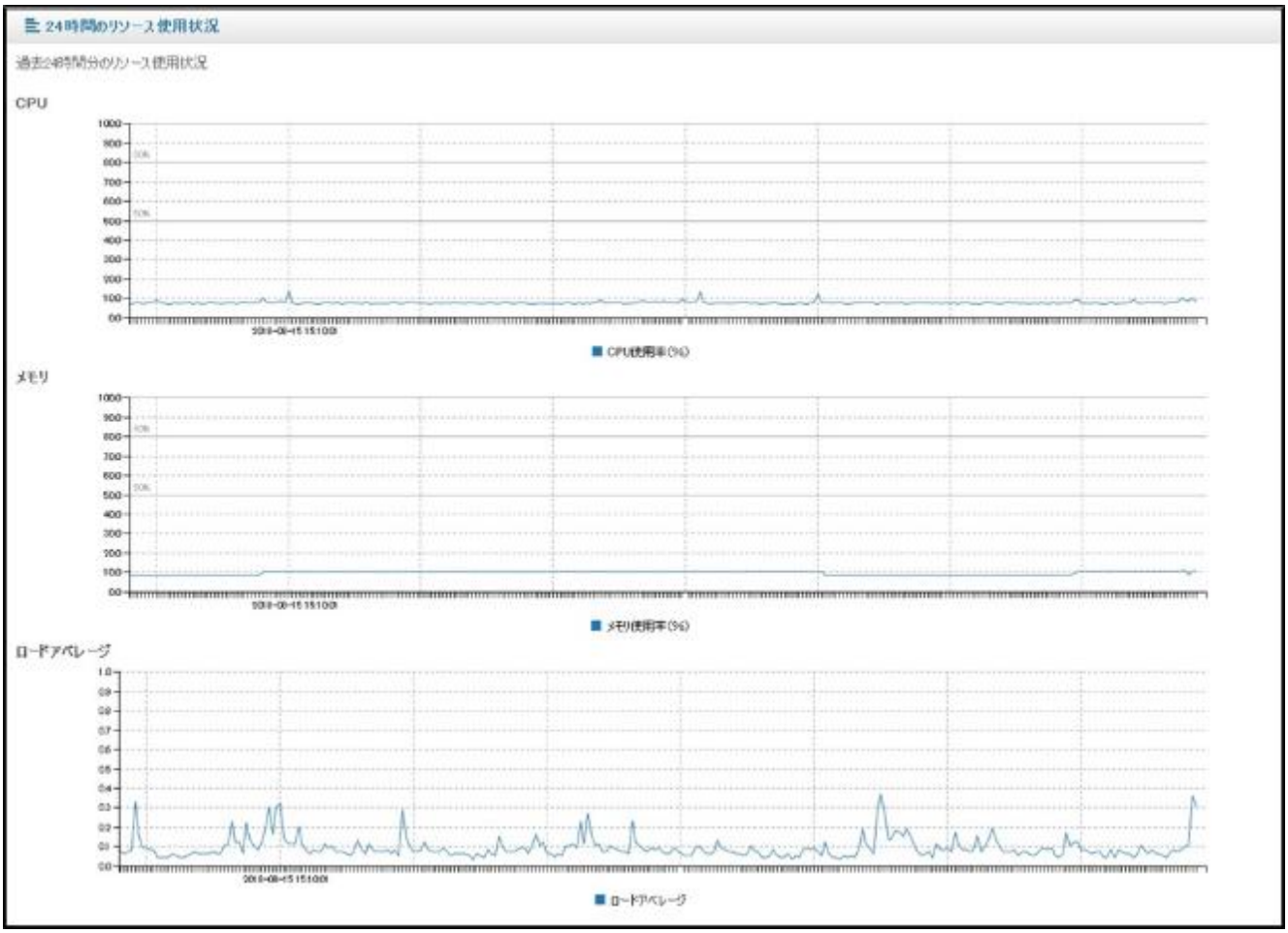
コントロールパネルの「リソース使用状況」から、サーバーの CPU やメモリ使用量、負荷状況を確認することが可能です。

1） コントロールパネルの「ホーム」画面から、[リソース負荷状況] をクリックします。

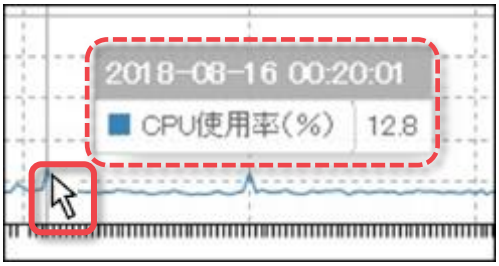
2） CPU・メモリ・ロードアベレージの項目ごとに、グラフ表記されています。

※ CPU とメモリは、使用率が表示されます。

※ 過去 24 時間と 1 週間の負荷状況が表示されます。



3） グラフにマウスカーソルを合わせると、カーソルを合わせた時点（日時）のリソース状況が、ポップアップで表示されます。



アドバイス

- ロードアベレージは、サーバー全体の負荷状況を示しています。
  一般的には、CPU のコア数を超える場合は「負荷が高い」と判断されます。
  高負荷状態が短時間・一時的なものであれば、特に問題はございません。

※ **高負荷状態が長時間継続する場合**は、アクセス集中やプログラム・データベースの暴走等が考えられます。

※ **長時間の高負荷が継続すると**、メール送受信の遅延・通信が出来ない・Web アクセスに時間がかかる等の事象が発生し、サーバー自体がダウンすることもあります。

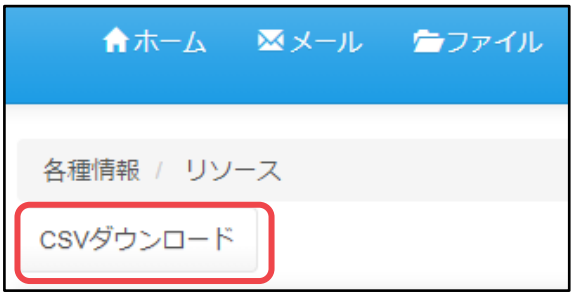
- 長時間の高負荷が発生した際には、サーバースペックの増強や、高負荷の起因となっているプログラムの修正などを実施していただくようお願いいたします。

4） 詳細なサーバーの負荷状況を確認したい場合は、CSV 形式のファイルをダウンロードすることで、5 分おきの負荷状況が確認できます。

CSV ファイルのダウンロード方法

画面上部の［CSV ダウンロード］をクリックして、保存先を選択し、［保存］します。

※ ブラウザの設定によっては、自動的に規定の保存先にダウンロードされる場合もあります。



- 保存される際のファイル名は「resmon.csv」です。
- CSV 形式のデータファイルは、メモ帳や Excel 等で開いて閲覧してください。
- CSV ファイルを Excel で開いた場合は、下図のように表示されます。

	A	B	C	D
1	DATE TIME	CPU(%)	MEMORY(%)	LDAVG-5
2	2018/8/10 12:05	7.33	10.05	0.11
3	2018/8/10 12:10	7.39	10.18	0.1
4	2018/8/10 12:15	7.26	10.08	0.18
5	2018/8/10 12:20	7.8	10.09	0.13
6	2018/8/10 12:25	7.65	10.17	0.13
7	2018/8/10 12:30	7.19	10.07	0.07

5.5.1. ディスク使用量の警告メールについて

コントロールパネルの「リソース使用状況」が 80%・90%を超えた場合は、「管理者」に以下のような『ディスク使用量警告メール』が送信されます。

※ 警告メールの From と To は、どちらも管理者のメールアドレスになります。

警告メール例：80%を超過した場合

From: c*******@c*******.mwprem.net
To: c*******@c*******.mwprem.net
Subject: [重要] Biz メール&ウェブ ディスク使用量に関するご案内

Biz メール&ウェブ管理者様

Biz メール&ウェブをご利用いただき、ありがとうございます。

ご利用中の Biz メール&ウェブの利用ディスク領域が 80%を超えています。
ディスクの追加を検討するかコントロールパネルより不要ファイルの削除、バックアップの管理よりバックアップ対象の変更などを行ってください。
なお利用ディスク領域が 90%を超えた場合はコントロールパネルより
最新のバックアップデータの復元ができなくなりますのでご注意ください。

※本メールは、配信専用です。このメールに返信いただいても対応できませんのであらかじめご了承ください。

警告メール例：90%を超過した場合

From: c*******@c*******.mwprem.net
To: c*******@c*******.mwprem.net
Subject: [重要] Biz メール&ウェブ ディスク使用量に関するご案内

Biz メール&ウェブ管理者様

Biz メール&ウェブをご利用いただき、ありがとうございます。

ご利用中の Biz メール&ウェブの利用ディスク領域が 90%を超えます。
ディスクの追加を検討するかコントロールパネルより不要ファイルの削除、
バックアップの管理よりバックアップ対象の変更などを行ってください。

現在コントロールパネルより最新データのファイルの復元ができない状態になっています。
コントロールパネルでファイルの復元を利用するには、
上記の対応を行っていただく必要がございます。

※本メールは、配信専用です。このメールに返信いただいても対応できませんのであらかじめご了承ください。

5.6. ディスク使用量の確認

機能別のディスク使用量（メール、ウェブ、システム、アプリケーション、空き容量）の確認と、ユーザーごとのメール蓄積量が確認できます。

1）コントロールパネルの「ホーム」画面から［ディスク使用量詳細］をクリックすると、ディスク使用量詳細画面が開きます。

※ ユーザーが多い場合は、データの読み込みが完了するまで数十秒～数分程を要します。
データの読み込み中は、ブラウザの［戻る］ボタンや［更新］ボタンのクリックおよび、画面のリロードはしないでください。

○ ディスク使用量詳細 画面

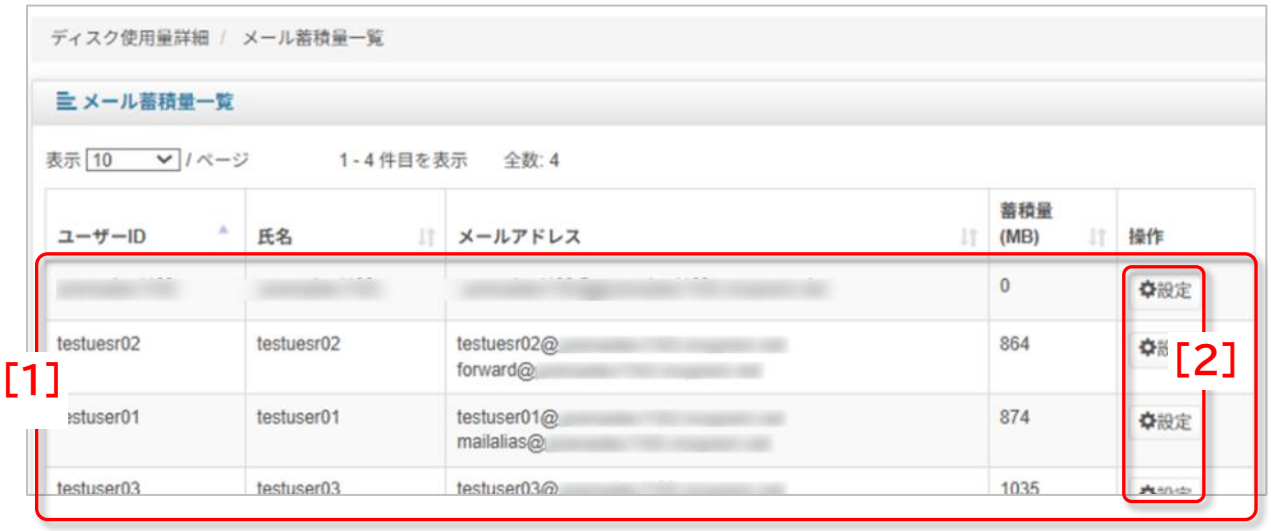
［1］ディスク使用量の割合をグラフで表示します
［2］ディスクの 使用量/全体容量（残容量）をテキストで表示します
［3］ディスク使用量割合を機能別に表示します
［4］クリックするとメール蓄積量一覧画面へ遷移します
※ データ読み込中でも［詳細］ボタンをクリックして遷移することが可能です

2）ディスク使用量詳細画面で、「メールデータ」の［詳細］をクリックすると、メール蓄積量一覧画面が開きます。

※　ユーザーが多い場合は、データの読み込みが完了するまで数十秒程を要します。
データの読み込み中は、ブラウザの［戻る］ボタンや［更新］ボタンのクリックおよび、画面のリロードはしないでください。

メール蓄積量一覧画面では、ユーザーごとのメールデータの蓄積量を確認できます。

○ メール蓄積量一覧 画面



［1］ユーザーごとに、メールの蓄積量が一覧で表示されます。

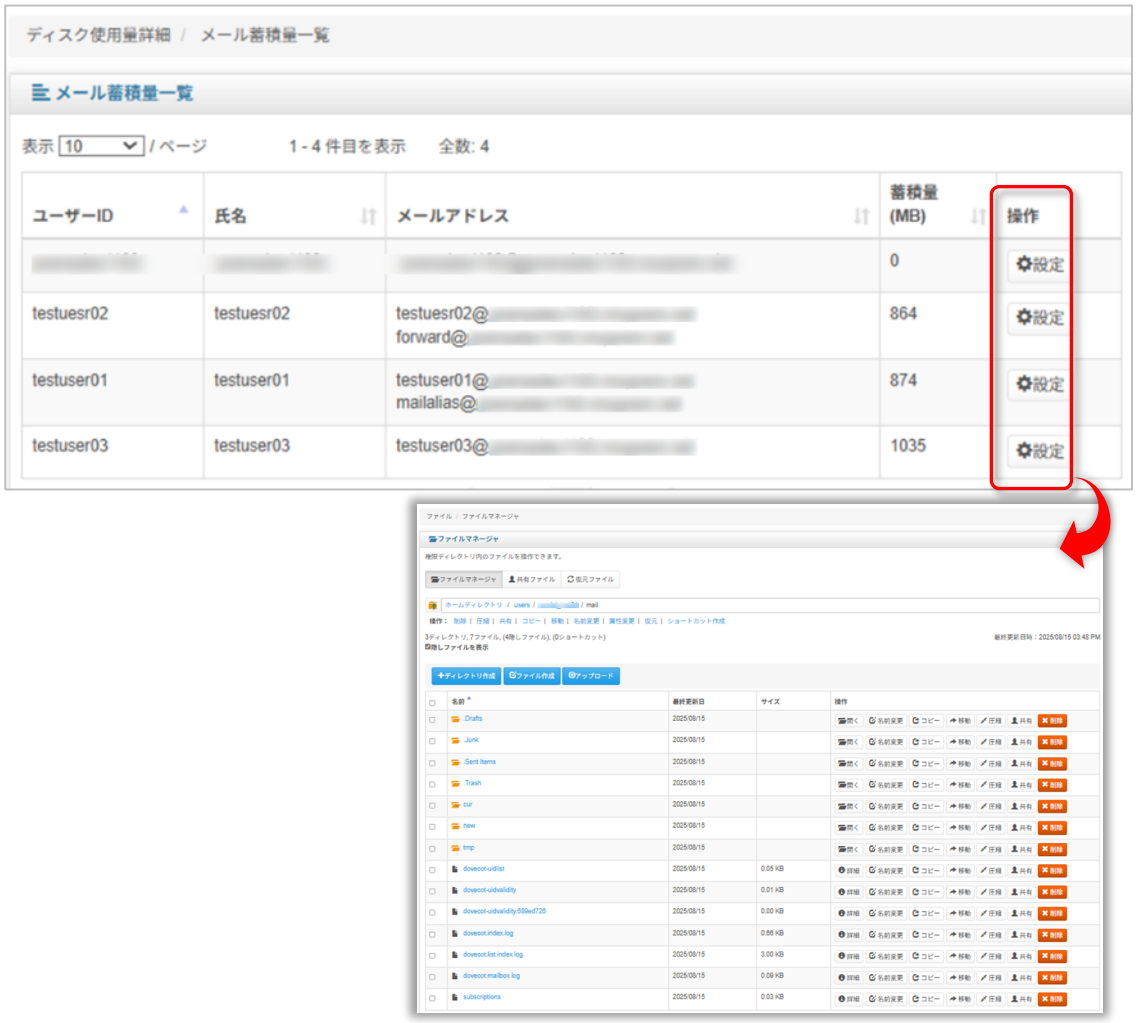
※　各カラムでソート（降順/昇順）が可能です。
※　メールアドレス機能で以下を設定しているユーザーのメールアドレス欄には、設定した分のメールアドレスも表示されます。
・「受信 - 受信ユーザー:」で既存のユーザーにメールエイリアスを付与
・「受信 - 詳細設定:」で既存のユーザーに転送
メールアドレス機能については、本書 2.2 メールアドレス をご参照ください。

［2］クリックすると、ファイルマネージャに遷移して該当ユーザーの mail ディレクトリが表示されます。

注意

「ディスク使用量詳細」画面に戻る場合は、上部メニューの［ホーム］からホーム画面に戻って［ディスク使用量詳細］をクリックしてください。
ブラウザの［戻る］ボタンをクリックするとセッションが切れ、再度ログインが必要になります。

3） 操作欄の［設定］をクリックすると、該当ユーザーの［mail］ディレクトリ（ファイルマネージャ）に遷移します。



メールデータを削除する必要がある場合は、
該当ユーザーに、メールクライアントで不要なメールを削除するようお伝えください。

注意

- **メールデータを削除する際は必ずメールクライアント（Active!mail, Outlook 等々）で削除してください。**FTP やコントロールパネルで削除すると、システムが正常に動作しなくなる恐れがあります。
- **「ディスク使用量詳細」画面や「メール蓄積量一覧」画面に戻る場合は、上段１） ２）の方法で開きなおしてください。**ブラウザの［戻る］ボタンをクリックするとセッションが切れ、再度ログインが必要になります。
- **サーバーのディスク容量は、常時 15% 以上の空きを確保することをお奨めします。**大量のメール送受信や大容量ファイルの転送などの際に容量不足が発生してご利用いただけない状態となった場合、必要なメール等が受け取れなくなります。

■ mail ディレクトリ配下のディレクトリとファイルについて

○ ディレクトリ：下表のディレクトリごと削除/ディレクトリ名の変更はしないでください。
システムが正常に動作しなくなる恐れがあります。

ディレクトリ	概要
.Drafts	下書きメールを保存するフォルダ
.Junk	迷惑メール(スパム)を保存するフォルダ
.Sent	送信済みメールを保存するフォルダ
.Trash	削除されたメールを一時的に保存するフォルダ(完全削除前の保管場所)
cur	既読メールが保存される
new	未読メールが保存される
tmp	プログラムの実行中に一時的に使用されるファイル(例:メールの添付ファイル、配送中のメール等)が保存される

○ ファイル： 下表のファイルを変更/削除しないでください。
システムが正常に動作しなくなる恐れがあります。

ファイル	概要
dovecot-uidlist	各メールボックスのメール UID を管理するファイル
dovecot-uidvalidity	メールボックスの一意性を識別する数値(UIDV)を格納するファイル
dovecot-uidvalidity.*[UIDV]*	メールボックスに UIDV を割り当てる処理に必要なファイル
dovecot.index	メールのメタデータ(既読/未読、フラグなど)を管理するファイル
dovecot.index.cache	メールメッセージのメタデータをキャッシュするためのファイル
dovecot.index.log	メールのインデックス変更履歴を記録するファイル
dovecot.list.index	フォルダー一覧のインデックスファイル
dovecot.list.index.log	フォルダー一覧に関連する変更履歴を記録するファイル
dovecot.mailbox.log	メールボックスを操作した際に記録されるファイル
subscriptions	IMAP クライアントがどのフォルダを表示・同期するかを記録するファイル
maildirfolder	IMAP クライアントやメールサーバーが、このファイルが格納されているディレクトリを「メールフォルダ」として認識するための目印

6　CGI の仕様

6.1. CGI スクリプトの設置場所へのリンク

本サービスでは、CGI スクリプトの実装が可能です。本サーバーに実装したウェブコンテンツから、CGI スクリプトを呼び出す場合、次の記述でリンクを設定できます。

- **CGI スクリプトの設置場所へのリンク**

  /cgi-bin/*<CGI ファイルへのパス>*/*<CGI ファイル名>* に設置した場合

  http://<*お客さまドメイン名*>/cgi-bin/<*CGI ファイルへのパス*>/<*CGI ファイル名*>

  例: http://www.examle.jp/cgi-bin/test.pl

アドバイス

利用者が作成したウェブコンテンツからも、該当ドメイン内の CGI スクリプトの設置場所へのリンクを設定できます。リンクの設定方法は、管理者と同じ
/www/cgi-bin/<*CGI ファイルへのパス*>/<*CGI ファイル名*> となります。

注意

- cgi-bin ディレクトリにファイルをアップロードした場合、ファイルのアクセスパーミッションには、本サービス環境標準のもの（644, -rw-r--r-- ）が割り当てられます。

- 設置したファイルに対して直接の起動を掛けたい場合は、ファイルの転送後、実行権限を与える(755, -rwxr-xr-x ）等のアクセスパーミッション変更が必要になります。

- ファイル単位でのアクセスパーミッションの変更は、FTP ソフトやコントロールパネルから行うことができます。
  コントロールパネルからファイルを変更する場合は・・・
  ①「ファイルマネージャ」機能でファイルが設置されたディレクトリを表示します。
  ② 該当ファイルの［詳細］をクリックします。
  ③「ファイル詳細」画面から［属性変更］をクリックします 。

6.2. 使用できる言語とスクリプトの実装

6.2.1. 言語とシェル

本サーバーで CGI を作成する場合、次に示すプログラミング言語とシェルスクリプトが、使用可能です。
本サービスの CGI 環境で使用可能な言語の種類と、該当するフルパスを次に示します。

言語/シェル		フルパス
Perl		/usr/bin/perl
PHP	php8.3	/usr/local/global-bin/php-8.3.cgi
python		/usr/bin/python3
ruby		/usr/local/bin/ruby
sh		/bin/sh

※ PHP のフルパスは、利用している PHP に合わせてバージョンまで指定してください。
※ 提供中の PHP バージョンは「4.1.2 PHP のバージョン」をご参照ください。

6.2.2. 使用可能なコマンドの例

本サービスでは、一般的な UNIX コマンドの他にも、次に示すコマンドが使用可能です。

/usr/local/bin/nkf (日本語文字のコード変換)
/usr/bin/uuencode (バイナリーファイルのエンコード)
/usr/sbin/sendmail (メールの送信、sendmail 互換プログラム)

アドバイス

各コマンドの機能や使用方法については、サポート対象外です。各種サイトや市販本などを参照してください。

6.2.3. スクリプト言語の宣言文

各種スクリプト言語を使用する際には、必ず宣言文を用いる必要があります。

言語	宣言文
Perl	#!/usr/bin/perl
python	#!/usr/bin/env python3
ruby	#!/usr/local/bin/ruby
sh	#!/bin/sh

6.2.4. CGI スクリプト実装上の注意事項

本サーバーにスクリプトを実装する場合、次の要件を満たすことが必要です

- 改行コードは、１バイト(LF) にする
- 日本語の文字は UTF-8 形式でエンコーディングする
- ファイルパーミッションの変更（実行権限付与）が必要（**755, -rwxr-xr-x** など）
- サーバーのフルパスでは、 /usr/home/*<ユーザーID>*/ となります

cron やプログラムで PHP を呼び出す場合は、以下が一致していることをご確認ください。

- 使用している PHP のバージョン
- パスで指定している PHP のバージョン

※ バージョンが一致しない場合は、cron およびプログラムが動作しなくなります。

参照）6.2.1　言語とシェル

１バイト(LF) の改行コードでファイルを作成するには、次の方法があります。

- コントロールパネルの「ファイルマネージャ」を使用して、ファイルを作成する
- Windows 環境でファイルを作成した場合は、ファイル転送時に FTP の ASCII モードで転送を掛ける

CGI スクリプトで使用可能なコマンドや 各言語のバージョン、インストール済みのライブラリなどについては、以下の弊社ホームページをご参照ください。

◆Biz メール＆ウェブ プレミアム　独自 CGI
https://www.ntt.com/business/services/cloud/rental-server/vps/service09.html

◆Biz メール＆ウェブ プレミアム　ソフトウェアのバージョン
https://www.ntt.com/business/services/cloud/rental-server/vps/service23.html

◆Biz メール＆ウェブ プレミアム　Perl モジュール一覧
https://www.ntt.com/business/services/cloud/rental-server/vps/perlmodule.html

◆Biz メール＆ウェブ プレミアム　PHP モジュール一覧
https://www.ntt.com/business/services/cloud/rental-server/vps/phpmodule.html

アドバイス

各コマンドの機能や使用方法については、サポート対象外です。
各種サイトや市販本などを参照してください。

6.3. ファイルマネージャによる CGI ファイルの作成

6.3.1. スクリプトファイルの要件

CGI スクリプトが格納されたファイルを、コントロールパネルの「ファイルマネージャ」機能で作成することができます。

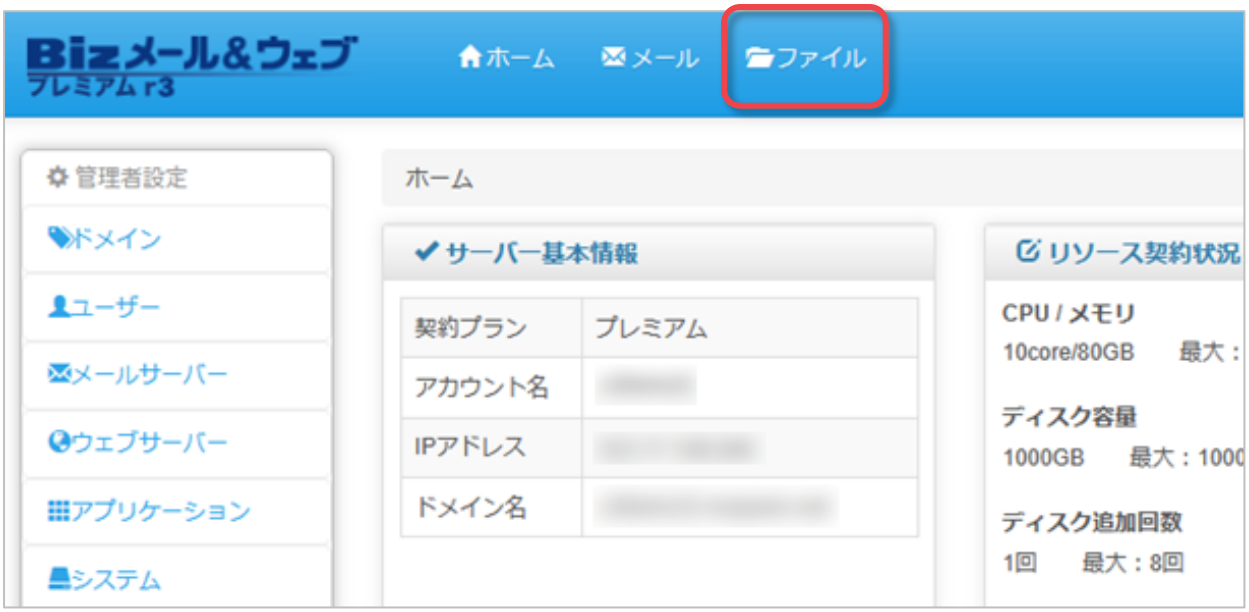
内容に日本語の文字を含む CGI スクリプトを本サーバーに設置する場合、各ファイルは、次の要件を満たす必要があります。

- 改行コードが 1 バイト("LF") である
- 日本語が UTF-8 の形式でエンコードされている
- ファイルのアクセスパーミッションには、実行権限が付与されている
- 作成したスクリプトが 次の要件を満たしていることも、合わせて必要です。
  - スクリプトが、日本語の文字は UTF-8 の形式で処理するように設定されている
  - スクリプトには、文法エラーや設定値の誤りなどの問題が含まれていない

6.3.2. ファイルの作成

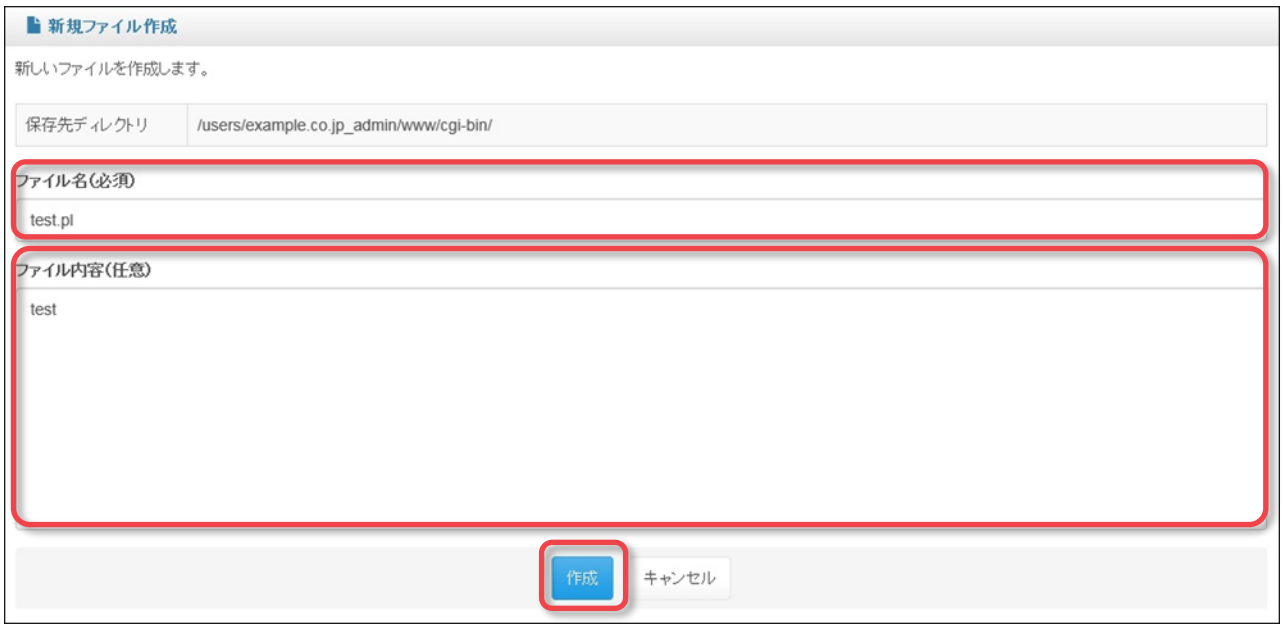
ここでは、コントロールパネル内の「ファイルマネージャ」機能を使用して、
『test.pl という名前のファイルを、サーバー上の **/users/*ドメイン管理者 ID*/www/cgi-bin/** に作成する』場合の手順を説明します。

1） コントロールパネルの画面上部にある、［ファイル］をクリックします。



2） ディレクトリ一覧で、「users」→「*ドメイン管理者 ID*」→［www］→［cgi-bin］の順にクリックします。
アイコンの欄に、「ホームディレクトリ/users/*ドメイン管理者 ID*/www/cgi-bin」が表示されていることを確認して、［ファイル作成］をクリックします。

3）　［ファイル名］に「*test.pl*」と入力します。
［ファイルの内容］にスクリプトの内容を入力したら、［作成］をクリックします。



4）　「*test.pl*を作成しました」と表示されたら完了です。
ディレクトリの一覧に、該当のファイルが保存されていることを確認してください。

6.4. スクリプトファイルへの実行権限の付与

本サーバー内に設置したスクリプトファイルを実行するためには、実行権限を付与する必要があります。ここでは、コントロールパネルの「ファイルマネージャ」で実行権限を付与する手順を説明します。

以降の例では、「/users/ドメイン管理者 ID/www/cgi-bin/」に格納された「*test.pl*」ファイルに、実行権限を付与しています。

1） コントロールパネルの画面上部にある、［ファイル］をクリックします。

2） ディレクトリ一覧で、「users」→「*ドメイン管理者 ID*」→［www］→［cgi-bin］の順にクリックします。
アイコンの欄に、「ホームディレクトリ/users/*ドメイン管理者 ID*/www/cgi-bin」が表示されていることを確認して、「*test.pl*」の［詳細］をクリックします。

3） 「操作」欄の［属性変更］をクリックします。

4） 「属性変更」画面で、「所有者」「グループ」「その他」それぞれに対応する［実行］を選択して、［保存］をクリックします。

5） 「属性を変更しました」と表示されたら、完了です。

アドバイス

Perl で書かれたスクリプトのほかに、Python や Ruby で書かれたスクリプトも、同様の手順(ファイル名のみが異なる) で、サーバー内に設置できます。

注意

実行権限を付与していない場合、記述が正しくても正常に動作しません。
各コマンドの機能や使用方法については、サポート外となります。各サイトや市販本などを参照してください。

7　システム管理者さまへのお願い

7.1. ユーザー管理についての注意事項

本サーバーでは、メールや FTP などを利用するユーザーを管理者が任意に作成できます。そのため、ユーザー管理に関して、下記の内容をご配慮くださいますよう、お願いいたします。

◆ 利用者が増えた場合は、その都度、新たにユーザー登録をしてください。１つの登録ユーザーを複数の利用者で共用すると、同じメール BOX 等へのアクセス集中によるサーバーの高負荷を招く恐れがあります。

◆ ユーザー登録の際に、簡単なログイン名・パスワードの組み合わせで作成すると、悪意のあるユーザーに乗っ取られ、他のサーバーへの攻撃の踏み台にされるなどの危険性が高くなります。ユーザー登録およびパスワードの管理には、十分に注意してください。
なお、パスワードは、以下のような条件を満たす『第三者から類推されにくい文字列』を使用することを推奨します。

- **辞書に載っている単語や固有名詞などは使用しない。辞書に載っている単語を含める場合には、あえてスペルを誤る。**
- **メモを残さなくてよいように、自分では思い出しやすいものにする。**
- **同じフレーズを繰り返すなど、長さを より長くする。**

◆ ユーザー登録の際の「メール」「ファイル」の権限付与につきましても、使用しない権限は付与せずに、必要最小限での付与をお勧めします。

◆ 利用者が一時的に利用を停止する場合は、その期間、権限を無効化することをお勧めします。また、転属や退職などで不要になったユーザーID が生じた場合は、業務に支障が無いことを確認したうえで削除する等、利用していないユーザーID を放置しないようお願いいたします。

◆ 定期的に登録状況やご利用状況の精査を行い、悪意のあるユーザーのアクセスへの脅威や無用な問題の発生に備える必要があります。

- 不要な登録ユーザーや権限の洗い出し
- 管理者および各利用者のパスワードの定期的な変更
- サーバー容量
- 「access log」や「error log」のサイズの推移（コントロールパネル内「ファイル管理」から確認可能）

以上の内容をご考慮いただいたうえでの運用を、お願いいたします。

アドバイス

本サービスを快適にご使用いただくためには、サーバーのご利用状況を把握していただき、効率的に運用していく必要があります。ここでは、本サービスの円滑なご利用にあたり、システム管理者の方にご留意いただきたい事項をまとめています。

7.2. サポートに関する注意事項

問題が発生してサポート窓口に相談される場合は、以下の点をご確認くださいますようお願いいたします。

■ **サポート方法について**
電話、およびメールによるサポートのみとなります。
訪問による設定サポートなどは実施しておりません。

■ **サポート範囲について**
サポート範囲は、各種マニュアル/メールアドレスの設定/提供機能の設定までとなります。ホームページの作成方法や内容などに関しては、サポート対象外となります。

■ **ホームページ CGI について**
お客さま側で作成されたホームページ CGI の内容に関しては、サポート対象外となります。

■ **データベース(MySQL)　や各スプリクト(PHP など)　の記述について**
本サービスでは、MySQL/PHP などの動作環境のみを提供しています。
データベースの操作方法や各スクリプトの記述等に関しては、サポート対象外となります。

■ **ログの提供について**
共用サーバーでの提供の特性上、アクセスログはお客さまが参照可能な位置に格納されていますが、メールや FTP などのその他のログは、お客さまが参照できない位置に格納されており、提供しておりませんのでご了承ください。

本サービスのサーバーに問題がある場合は、サポート窓口で問題解決の支援が可能ですが、ご利用のパソコンやインターネット回線などの接続環境に原因がある場合などは、その限りではございません。
そのため、原因をお調べいただき、該当の窓口にご相談していただくことが、問題の早期解決のために必要となります。

管理者は、利用者と情報を共有することにより、問題の早期解決に向けた作業の効率化を計ることが可能です。

● **効率的な情報の伝達**
利用者マニュアルなどの基本情報や、工事やサービス停止の連絡など、弊社からの案内を組織内で全員に共有していただくことにより、管理業務の効率化が図れます。

- **問題発生時の状況確認とその後の対応について**
  問題が発生した場合、その内容・状況をお客さまでご確認頂き、解決に必要な情報をとりまとめていただきますと、事象の回復への工程が効率化します。
  また、併せて弊社からご連絡する事柄を、皆さまで共有していただくことにより、再発防止の効果も生まれます。

- **サポート窓口での調査や依頼に必要な情報について**
  問題を解決するためには、「問題の該当箇所」をご確認頂く事が必要です。
  そのため、サポート窓口へご連絡頂く前に、以下の情報をご確認くださいますようお願いいたします。

  - H から始まるお客さま番号
  - 問題の発生時刻、発生の頻度、再現が可能であれば再現手順
  - 問題が発生した際のエラーメッセージなどの記録
  - OS の種類やソフト、インターネット接続環境などのお客さまのご利用環境
  - メールでの問題発生の場合、差出人や宛先のメールアドレス

8　サービスのご利用にあたって

8.1. 本サービス提供形態に関する注意

本サービスは１台のサーバーを複数のユーザーで共有していただく仮想専用サーバーの形態で提供しています。

仮想専用サーバーとは、１台のサーバーに対して複数の仮想サーバーを実現するソフトウェアをインストールする事で、専用サーバーと同等の環境を実現させているサーバーを指します。このメカニズムによって、サーバーの物理的なリソースを効率的に分割することができます。

本サービスで提供しているソフトウェアは、原則、開発元から出荷された機能で実装していますが、本サービスのサーバーハードウェアは共用のサービスであり、各ユーザーではサーバーそのものの管理者権限を持たないため、ソフトウェアの一部機能で使用上の制約が発生することがあります。
同様に、各ソフトウェアから出力されるログも、アクセスログについてはお客さまが参照可能な位置に格納されていますが、メールや FTP など他のソフトウェアのログは、お客さまに提供している権限では参照できない位置に格納されています。

また、サーバーの障害等に関与しない受信記録の詳細な説明や、具体的な送信元 IP アドレス等の情報を開示することは電気通信事業法に定められております「通信の秘密を侵すこと」に該当するおそれがあるため、ご契約者ご本人様からのご依頼の場合であっても控えさえて頂いております。

快適に本サービスをご利用いただくには、プランごとに推奨値を定めています。具体的な値については、以下のページを参照してください。

Biz メール&ウェブ プレミアム 推奨値：
https://www.ntt.com/business/services/cloud/rental-server/vps/service19.html

8.2. 本サービスの機能

本サービスでは、ご契約されたお客さまの１契約に対して１つの「仮想サーバー」を提供しています。
この仮想サーバーでは、ご利用開始時から次の機能を提供しています。

■ **固定 IP アドレス**
固定のグローバルアドレスを割り振っています。このアドレスは、原則として、変更されることなくご使用いただけます。

■ **バックアップ**
バックアップ(ディスク、外部記憶装置) を取得しております。ただし、バックアップの対象はハードディスク上に記録されたデータだけです。編集中の「状態」やメモリー上でのみ稼働しているデータベースなどは、バックアップの対象にはなりません。

■ **コントロールパネル**
本サービスでは、その機能をご利用頂く為の、専用の「コントロールパネル」を提供しています。サーバーの管理や各種ソフトウェアの使用も、原則として、コントロールパネルにログインした状態での作業が必要です。

コントロールパネルへのアクセスには、インターネットブラウザを使用します。
このため、本サービスの管理作業や各種機能をご利用いただくには、インターネット経由でウェブにアクセスできる環境が必要になります。

■ **テンポラリドメインとサーバー証明書**
本サーバーには、「c******.mwprem.net」に対応したサーバー証明書をインストール済みです。この証明書により、次に示すセキュアな通信を実現できます。

- FTPS の利用
- POP over SSL(Port 995) や STARTTLS (Port 587) を利用したメールサーバーへのアクセス

※ 「c******」は、『ご利用内容のご案内』に記載されている［ユーザ ID(管理者)］です。

8.3. 本サービス保全に関する注意事項

本サービスは共用サーバーとなるため、運用にあたってご留意いただきたいことがあります。

■ サーバー資源の使用状況によっては、弊社から使用内容の見直しや、使用状況の改善をお願いさせていただくことがあります。
また、電気通信設備の保守上又は工事上やむを得ない場合に、お客さまの収容サーバーを変更する場合があります。この場合、あらかじめそのことを契約者に通知します。
ただし、緊急時やむを得ない場合は、この限りではありません。
なお、お客さまのコンテンツ、設定情報等の変更はありません。

■ 本サービスでは工事を実施する場合があります。
以下のように、工事によりサーバーに影響が出る場合には、事前にお客さまサポートサイト（工事・故障情報）でご案内しますので、定期的なご確認をお勧めします。

- 工事によりサービスへ以下の影響がある場合
  (1) 動作が不安定になる可能性がある場合
  (2) サーバーが停止する可能性がある場合
  (3) サーバーを再起動する可能性がある場合

工事･故障情報一覧｜Biz メール＆ウェブ プレミアム r3｜お客さまサポート
https://support.ntt.com/mw-premiumr3/maintenance/search

ソフトウェアの品質や問題点への対応には、可能な限り早い対応を行いますが、最新のセキュリティパッチや改良版については、本サービス提供環境での稼働確認などの為、ある程度のお時間をいただく可能性があります。また、機能改良版については、一定以上のお時間が掛かる場合もありますことをご留意ください。

Biz メール＆ウェブ プレミアム r3

管理者マニュアル

発行 NTTドコモビジネス株式会社