

マイサーバーサービス 利用マニュアル
(root 権限者用 Web サーバー設定)
マイサーバーVPS compact

RIMNET <http://www.rim.or.jp/support/>

Members Guide Book **2010/07**

はじめに

本利用マニュアルでは、HDE Controller に root 権限者としてログインし専用サーバーのホストユーザーとして、「Web サーバー」を操作する方法を説明します。

目次

はじめに	1
目次	1
1. root 権限者用 Web サーバー設定	2
1-1. 概要	2
1-2. 基本設定	2
1-3. ディレクトリ管理	6
1-4. ディレクトリ追加	10
1-5. ディレクトリ認証設定	13
1-6. ディスク使用量一覧	14
1-7. Alias 設定	15
1-8. MIME 設定	18
1-9. ModSecurity 設定	20
1-10. ModSecurity フィルター管理	23
1-11. アクセス統計	27

1. root 権限者用 Web サーバー設定

1-1. 概要

HDE Controller にroot権限者としてログインし専用サーバーのホストユーザーとして、Webサーバーを設定する方法を説明します。

次項に従って設定及び確認を実施してください。

1-2. 基本設定



通常は変更する必要がありません。

基本設定については、デフォルトの状態でも特に問題は発生しませんが、ご利用される環境に応じて変更を行ってください。

The screenshot shows the '基本設定' (Basic Settings) configuration page. The '基本設定' tab is highlighted in red. The page contains the following fields and options:

- サーバー名: lc5 example.com
- ポート番号: 80
- 管理者メールアドレス: root@example.com
- ドキュメントルート: /var/www/html (with a 'ディレクトリ選択' button)
- 設定する (Set) button

A message at the top of the configuration area reads: 'Webサーバーの基本的な設定を行います。通常は特に変更する必要はありません。' (We perform basic settings for the web server. Usually, there is no need to change anything.)

●詳細設定

バーチャルドメインユーザーが Web を公開する際に利用される URL タイプを選択します。
運用ポリシーに合わせて選択をしてください。

基本設定 **詳細設定** エラーメッセージの設定 suEXEC設定

詳細設定

ここでは、サーバーの規模と個人のページのURLの指定方法を選択します。
サーバーの規模では、設定に応じて最適なWebサーバー(になるようにチューニングが行われます。

サーバーの規模 ① 150

ユーザー領域のURLのタイプ ② http://example.com/~username/

サーバーログ形式

エージェント ③ 記録する

参照元 ④ 記録する

画像 ⑤ 記録する

ログファイルの保存形式 ⑥ 通常の保存形式 (logrotatedの処理対象)

リモートホスト名の逆引き ⑦ しない

サーバーバージョン表示 ⑧ 表示しない

TRACEメソッドの使用 ⑨ 禁止する

設定する

●サーバーの規模

「最小(15)」「150」「200」「最大(250)」いずれか、
お使いのサーバーの使用環境に合わせて設定します。

●「ユーザー領域のURLのタイプ」を選択します。

下記のいずれかの形式となります。

例：

http://example.com/~username/

http://example.com/users/username/

●サーバーログに、エージェント/参照元/画像 についてのアクセスを記録するか選択。

●エージェント：閲覧している Web ブラウザのタイプを記録します。

●参照元：表示したページがリンクされていた参照元 URL を記録します。

●画像：表示したページに含まれる画像の URL を記録します。

●リモートホスト名の逆引きについて選択します。

サーバーログで、「記録しない」を選択した場合

リモートホスト名の逆引きをしない場合

「アクセス統計」においてレポート内容が正しく表示されなくなる可能性があります。

逆引きを有効にした場合、Web サーバーのパフォーマンスが低下する場合があります。

お客様のサーバー内の bind にて named を設定、DNS を構築されている場合、逆引きは行えません。

弊社 Rimnet に DNS サーバーを依存している場合は、弊社既定の逆引きが行われます。

別途、逆引きのレコードを変更されたい場合はお問い合わせをして頂く必要があります。

サーバーログ形式

●エージェントを「記録する」に設定した場合

URL にアクセスしたブラウザや巡回ロボットのアプリケーション名、バージョン情報などが記録されます。

●参照元を「記録する」に設定した場合

URL にアクセスするために表示していたページのアドレスが記録されます。

●画像を「記録する」に設定した場合

ページ中に表示される画像ファイルへのアクセスがログに記録されます。

●ログファイルの保存形式

ログファイルの形式を変更します。

通常は、`/var/log/httpd/access_log` といった形式で保存され、`logrotated` の処理対象となります。

年毎、月毎、日毎にすると、それぞれ

`access_log-年`、`access_log-年-月`、`access_log-年-月-日` というファイル名で

`/var/log/httpd/accesslog/` 以下に保存されますが、`logrotated` の処理対象とはなりません。

この設定はアクセスログ (`access_log`) とエラーログ (`error_log`) に適用されます。

●リモートホスト名の逆引き

`HostnameLookup` を設定します。

逆引きを行うと、アクセスログにリモートホストがホスト名で記録されます。

逆引きを行うと、Web サーバーのパフォーマンスが低下する可能性があります。

※お客様のサーバー内の `bind` にて `named` を設定、DNS を構築されている場合、逆引きは行えません。

リムネットに DNS サーバーを依存している場合は、リムネット既定の逆引きが行われます。

別途、逆引きのレコードを変更されたい場合はお問い合わせをして頂く必要があります。

●サーバーバージョン表示

サーバーのレスポンスヘッダやエラーメッセージにサーバーのバージョンを表示したくない場合は、チェックを入れます。

サーバーのバージョンを表示する場合は、チェックをはずします。

●TRACE メソッドの使用

HTTP の TRACE メソッドの使用を禁止する場合は「禁止する」にチェックを入れます。

TRACE メソッドの使用を許可する場合はチェックをはずします。

※クロスサイトトレーシングなどの TRACE メソッドを使用した攻撃手法が存在するため、

特別な理由がない限り TRACE メソッドの使用を禁止することをお勧めします。

この設定は Apache のバージョンが 2.0.55 以上の場合のみ表示されます。

設定が正しければ「設定する」をクリックして設定を終了します。

■エラーメッセージの設定

基本設定 詳細設定 エラーメッセージの設定

エラーメッセージの設定

アドレス(URL)が正しく指定されていなかった場合などに表示するエラーメッセージを指定することができます。

- ブラウザーの言語設定に合わせる
- エラーメッセージを日本語にする
- エラーメッセージを英語にする

エラーメッセージの場所を指定する?

ファイルが見つからない(404)

アクセス不許可(403)

サーバーエラー(500)

設定する

リクエストされた Web サイトのアドレスが間違っている場合表示するエラーメッセージを設定します。
エラーメッセージの言語を選択します。

●エラーメッセージが記録されたファイルの場所を指定する場合

- 1 : 「エラーメッセージの場所を指定する」を選択
- 2 : ファイルの保存されているパスを、それぞれの項目に入力します。
- 3 : 「設定する」をクリックして設定を終了します。

●エラーメッセージが記録されたファイルの場所を指定する場合は、

「エラーメッセージの場所を指定する」を選択
ファイルの保存されているパスを、以下のそれぞれの項目に入力。

「ファイルが見つからない(404)」 / 「アクセス不許可(403)」 / 「サーバーエラー(500)」

設定が正しければ「設定する」をクリックして設定を終了します。

●suEXEC 設定

suEXEC 機能を有効にすることで、CGI または SSI を一般ユーザー権限で実行することができます。

URL	リアルドメイン	バーチャルドメイン
/username/	apache権限	apache権限
/users/username/	apache権限	apache権限
その他	apache権限	apache権限

但し、suEXEC 機能を有効にするとバーチャルドメインの admin ユーザーを除く一般ユーザーは CGI・SSI 自体が実行されなくなります。

リアルドメインの一般ユーザー権限かバーチャルドメインの admin ユーザー権限で CGI・SSI を実行したいときのみ有効にしてください。

1-3. ディレクトリ管理

Web サーバーで公開するディレクトリの設定を行います。

●CGI・SSI の設定

CGI SSI 絶対ディレクトリパス アクション

CGI SSI /home/lcvirtualdomain/example.jp/htdocs/ 編集 削除

CGI および SSI を設定する場合は「CGI」「SSI」をクリックします。

「許可」に設定されるとボタンが点灯した状態に変わります。

「設定する」をクリックして終了します。

※拡張子.cgi のファイルのみが実行可能です。

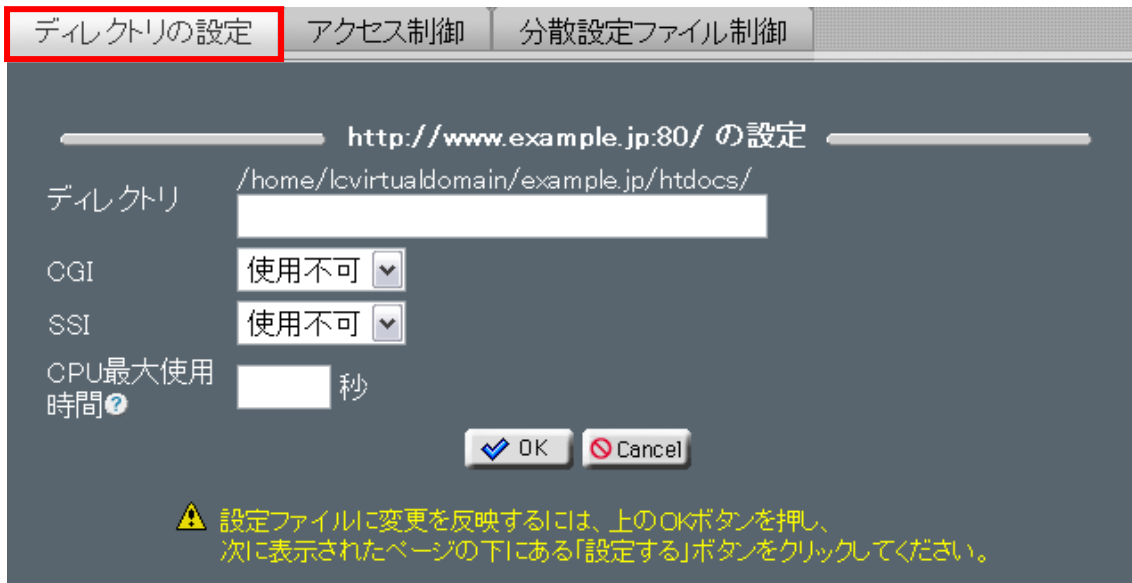
その他の形式のファイルを実行する場合は、MIME タイプを設定してください。

●ディレクトリの設定

Web サーバーのディレクトリを編集します。

ディレクトリの一覧から、「編集」をクリックすると、

「ディレクトリの設定」画面が表示されます。



「ディレクトリ」にパスを入力します。

「CGI」「SSI」それぞれの、「使用可」「使用不可」を選択します。

「CGI」や「SSI」のCPU使用時間を制限したい場合は「CPU 最大使用時間」に使用を許可する最大の時間を秒単位で設定します。

これはCGIなどが実際にCPUを使用した時間であり、起動してからの経過時間ではないことに注意してください。

何も指定しない場合は無制限となります。

「設定する」をクリックして終了します。

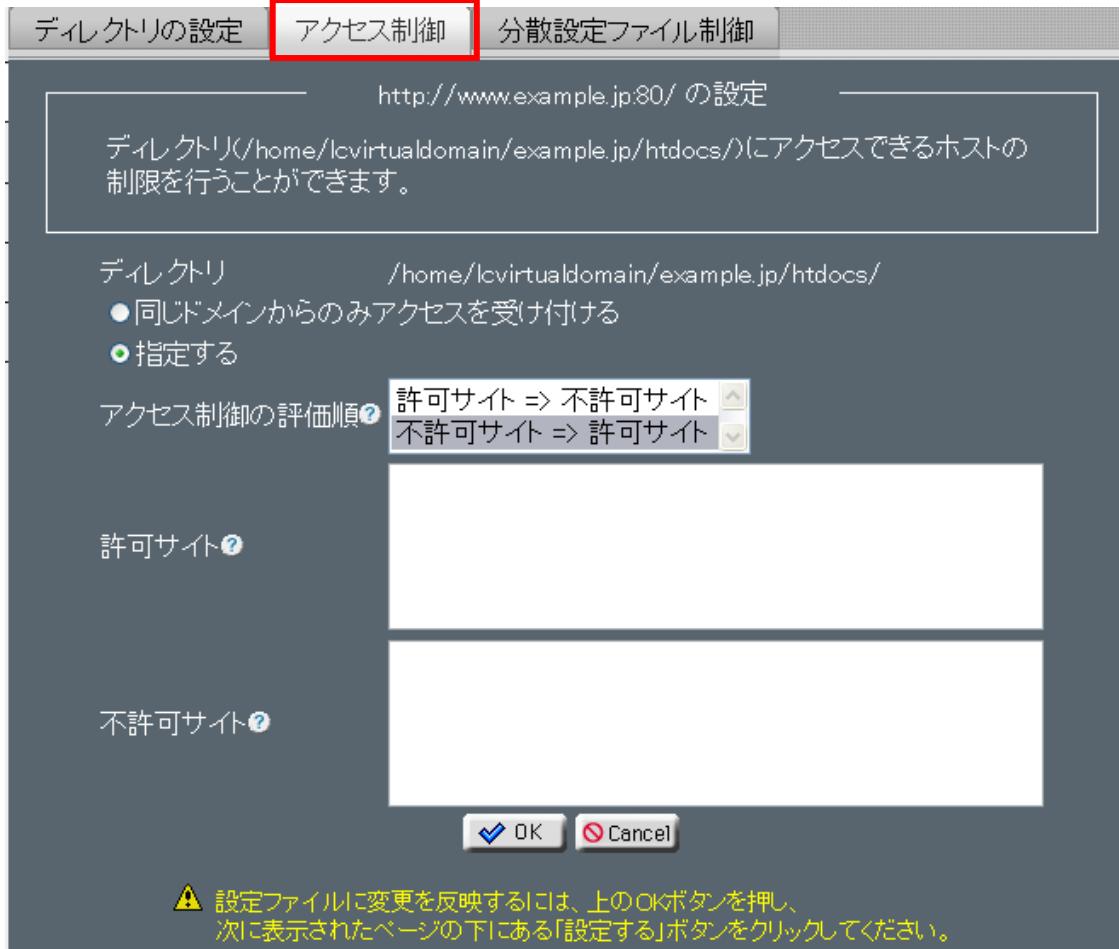
●アクセス制御

ディレクトリのアクセス制御設定をします。

ディレクトリの一覧から、「編集」をクリックします。

「ディレクトリの設定」画面が表示されます。

「アクセス制御」タブをクリックして設定画面を切り替えます。



同じドメインのみアクセスを許可する場合は、

「同じドメインからのみアクセスを受け付ける」を選択します。

制御対象を指定する場合は「指定する」を選択します。

「アクセス制御の評価順」メニューから、許可サイトと不許可サイト

どちらの評価を優先するか選択し、

「許可サイト」「不許可サイト」それぞれに制御対象となるアドレスを入力します。

「OK」をクリックして、ディレクトリ一覧画面に戻ります。

ディレクトリ一覧画面に戻り「設定する」をクリックして終了します。

アクセス制御に入力できる形式

ホスト名	host.example.com
IPアドレス	192.168.0.1
IPアドレスの一部	192.168.0.
IPアドレス/ネットマスク	192.168.0.0/255.255.255.0
複数の指定	192.168.0.0./24 172.16.0.0/16 (それぞれスペースで区切るか改行)
全てを指定	all (全てのホストに対して設定します。)
ドメイン名	.example.com

●分散設定ファイル制御 (htaccess)

ディレクトリの AllowOverride ディレクティブを設定します。

AllowOverride ディレクティブは、分散設定ファイル(.htaccess というファイル名で知られています)によって設定の変更が可能なディレクティブを指定するものです。

ディレクトリの設定 アクセス制御 分散設定ファイル制御

分散設定ファイル制御

ディレクトリ /home/|cvi rtual domain/example.jp/ht docs/ の AllowOverride ディレクティブを設定します。 AllowOverride ディレクティブは、分散設定ファイル(.htaccess というファイル名で知られています)によって設定の変更が可能なディレクティブを指定するものです。

このディレクトリに対して何も設定しない場合は、このディレクトリの上位(親)ディレクトリの設定を継承します。 上位ディレクトリの、現時点で有効な設定を以下に示します。

- ◆ **None:** 分散設定ファイルは使用できません。

設定方法を選択してください

- **None:** 分散設定ファイルを使用できないようにする
- **All:** 分散設定ファイルで設定できる全てのディレクティブを使用可能にする
- **このディレクトリには設定しない**
- **以下のリストから選択する**

- **AuthConfig:** 認証に関するディレクティブを使用可能にする
- **FileInfo:** ドキュメントタイプを操作するディレクティブを使用可能にする
- **Indexes:** ファイル・ディレクトリ一覧に関するディレクティブを使用可能にする
- **Limit:** ホストへのアクセス制御に関するディレクティブを使用可能にする
- **Options:** 特定のディレクトリにおける機能を操作するディレクティブを使用可能にする

OK Cancel

⚠ 設定ファイルに変更を反映するには、上のOKボタンを押し、次に表示されたページの下にある「設定する」ボタンをクリックしてください。

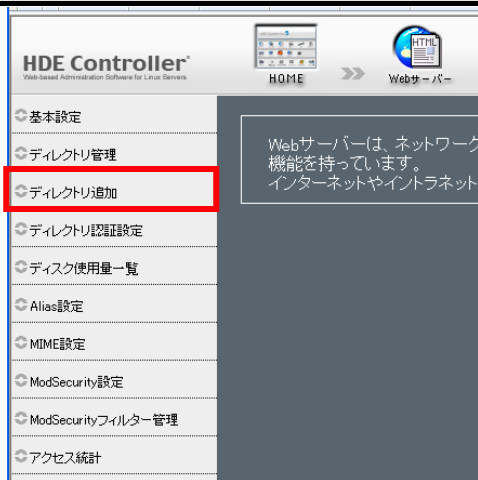
このディレクトリに対して何も設定しない場合は、
このディレクトリの上位(親)ディレクトリの設定を継承します。

分散設定ファイル制御を下記の設定方法から選択することができます。

None	分散設定ファイルを使用できないようにします
All	分散設定ファイルで設定できる全てのディレクティブを使用可能にします
このディレクトリには設定しない	上位(親)ディレクトリの設定を継承します
以下のリストから選択する	<p>下記に示されたリストより設定方法を選択します</p> <p>AuthConfig: 認証に関するディレクティブを使用可能にする</p> <p>FileInfo: ドキュメントタイプを操作するディレクティブを使用可能にする</p> <p>Indexes: ファイル・ディレクトリ一覧に関するディレクティブを使用可能にする</p> <p>Limit: ホストへのアクセス制御に関するディレクティブを使用可能にする</p> <p>Options: 特定のディレクトリにおける機能を操作するディレクティブを使用可能にする</p>

正しければ「OK」をクリックします。

1-4. ディレクトリ追加



Web サーバーを通して公開するディレクトリを追加します。

Web サーバーで公開するディレクトリを追加し、CGI・SSI の許可を設定します。

http://www.example.jp:80/ の設定

公開するディレクトリの中で個別に設定をおこなうディレクトリをここで指定します。また、このディレクトリでCGIとSSIの実行を許可するかどうかを設定します。

ディレクトリ /home/localhost/example.jp/htdocs/ ディレクトリ選択

CGI

SSI

CPU最大使用時間 秒

分散設定ファイル制御

None
 All
 このディレクトリには設定しない
 右のリストから選択する

AuthConfig
 FileInfo
 Indexes
 Limit
 Options

追加するディレクトリのパスを、「ディレクトリ」に入力するか、

「ディレクトリ選択」をクリックし、ディレクトリ選択画面から選択します。

「CGI」や「SSI」のCPU使用時間を制限したい場合は、「CPU 最大使用時間」に使用を許可する最大の時間を秒単位で設定します。

これはCGIなどが実際にCPUを使用した時間であり、起動してからの経過時間ではないことに注意してください。

何も指定しない場合は無制限となります。

分散設定ファイル制御を下記の設定方法から選択します。

None	分散設定ファイルを使用できないようにします
All	分散設定ファイルで設定できる全てのディレクティブを使用可能にします
このディレクトリには設定しない	上位(親)ディレクトリの設定を継承します
以下のリストから選択する	下記に示されたリストより設定方法を選択します AuthConfig: 認証に関するディレクティブを使用可能にする FileInfo: ドキュメントタイプを操作するディレクティブを使用可能にする Indexes: ファイル・ディレクトリ一覧に関するディレクティブを使用可能にする Limit: ホストへのアクセス制御に関するディレクティブを使用可能にする Options: 特定のディレクトリにおける機能を操作するディレクティブを使用可能にする

「進む」をクリックして次の設定へ進みます。

http://www.example.jp/80/ の設定

ディレクトリ(/home/lcvirtualdomain/example.jp/htdocs/example.com)にアクセスできるホストの制限を行うことができます。

ディレクトリ /home/lcvirtualdomain/example.jp/htdocs/example.com

同ドメインからのみアクセスを受け付ける

指定する

アクセス制御の評価順?

許可サイト?

不許可サイト?

戻る

ディレクトリのアクセス制御を設定します。

同じドメインのみアクセスを許可する場合

「同じドメインからのみアクセスを受け付ける」を選択。

制御対象を指定する場合

「指定する」を選択。

「アクセス制御の評価順」メニューから、
許可サイトと不許可サイトどちらの評価を優先するか選択し、
「許可サイト」「不許可サイト」それぞれに制御対象となるアドレスを入力します。
正しければ「設定する」をクリックして設定を終了します。

アクセス制御に入力できる形式

ホスト名	host. example. com
IPアドレス	192. 168. 0. 1
IPアドレスの一部	192. 168. 0.
IPアドレス/ネットマスク	192. 168. 0. 0/255. 255. 255. 0
複数の指定	192. 168. 0. 0. /24 172. 16. 0. 0/16（それぞれスペースで区切るか改行）
全てを指定	all（全てのホストに対して設定します。）
ドメイン名	. example. com

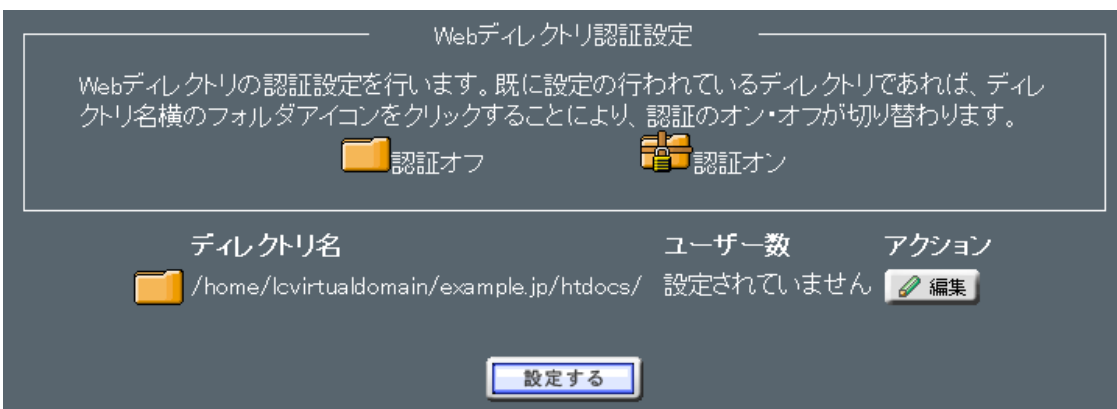
「設定する」をクリックし設定を終了します。

1-5. ディレクトリ認証設定



Web サーバーで公開するディレクトリの、認証設定を行います。

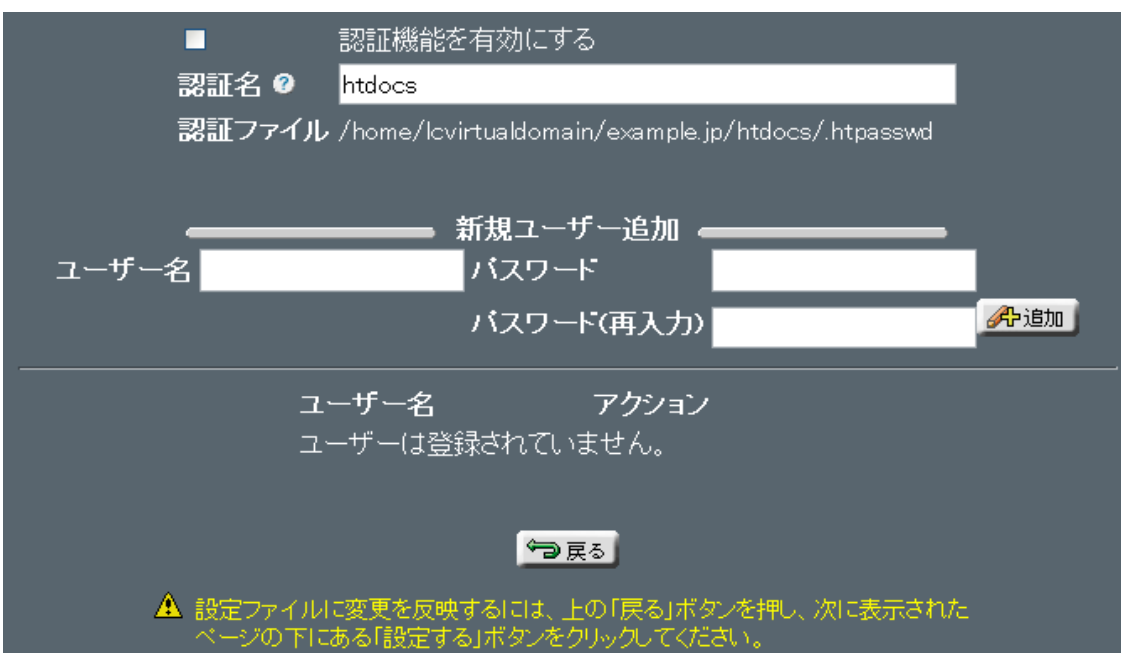
(アカウント・パスワードを要求するブラウザの設定)



●ディレクトリ認証の設定

Web ディレクトリの一覧より、認証を設定するディレクトリの、「編集」をクリックします。

認証内容の設定画面が表示されます。



- 「認証名」に認証時に表示する内容を入力します。(例：ENTER PASSWORD)
- 認証の為の「ユーザー名」「パスワード」をそれぞれ入力
「追加」をクリックすると、設定が追加されます。
- 追加した認証を使用する場合は、「認証機能を有効にする」を選択します。
- アクセス可能なユーザーを追加する場合は、
「ユーザー名」「パスワード」を入力し、「追加」をクリックして、追加します。
- 追加されたユーザーのパスワードを変更する場合は、編集をクリックし
編集を行います。
- 「戻る」をクリックし、ディレクトリ一覧画面に戻ります。
- 「設定する」をクリックして設定を終了します。
- 既に認証が設定されているディレクトリについては、ディレクトリ一覧画面で、
フォルダのアイコンをクリックすることにより認証の有効/無効を切り替えること
ができます。

1-6. ディスク使用量一覧



ユーザーの Web スペース使用量を一覧表示します。

ディスク使用量一覧

ユーザー毎のWebスペースのディスク使用量を表示します。

ユーザーの検索 表示件数 10

最小表示件数 1

全 2 件
ユーザー名の頭文字 **a-f** 全て表示 [?]

ユーザー名	ディレクトリ	ディスク使用量(MBytes)
admin	/home/lcvirtualdomain/example.jp/public_html/	0.02
ftp	/home/lcvirtualdomain/example.jp/users/ftp/public_html/	0.01

- ユーザーを検索する場合

「ユーザーの検索」に検索キーワードを入力します。

●検索結果の表示件数を変更する場合

「表示件数」の値を変更します。システムアカウントは通常表示されません。

●システムアカウントを検索結果として表示させる場合

「システムアカウントも表示する」を選択します。

「検索」をクリックして、検索を実行します。

●ユーザー名の頭文字から検索する場合

「ユーザー名の頭文字」に表示される、頭文字の範囲をクリックします。

●全てのユーザーを一度に表示する場合「全て表示」をクリックします。

ユーザー名、ディスク使用量については、項目名をクリックすることで、表示を降順/昇順に切り替えることができます。

1-7. Alias 設定

●Alias 設定



ここでは、Web サーバーへのアクセスに対して、アドレスの変換を行う Alias の追加を行います。

Alias の追加

●評価順

評価順には、新しい Alias 設定を挿入する場所を指定します。

すでに同じ値の Alias 設定がある場合は、指定した場所に新しいものが挿入され、

以降が一つずつ下にずれます。

The image shows a screenshot of the 'Aliasの追加' (Add Alias) form. The form has a table-like structure with columns: 評価順 (Evaluation Order), Aliasタイプ (Alias Type), 変換元URL (Source URL), and アクション (Action). The '評価順' column has a text input field containing '1'. The 'Aliasタイプ' column has a dropdown menu with 'Alias' selected. The '変換元URL' column has an empty text input field. The 'アクション' column has a button with a plus sign and the text '追加' (Add). Below the table, there is a '変換先Path' (Destination Path) text input field and a 'ディレクトリ選択' (Select Directory) button.

●Alias タイプ

Alias タイプには、下記のディレクティブから、

Alias

Alia

sMatch

ScriptAlias

ScriptAliasMatch のいずれかを選択します。

Alias	URLの特定のパターンを、特定のディレクトリ・ファイルに割り当てます。 変換元URLにマッチするパターンが、そのまま変換先Pathに置き換わります。
AliasMatch	機能としてはAliasと同じですが、変換元URLを正規表現で指定する点が異なります。 変換先Pathでは、後方参照として\$1, \$2...が使用できます。
ScriptAlias	値の指定はAliasと同じですが、変換先Pathにあるファイルが、CGI等のスクリプトであることを暗黙に指定できるので、拡張子が.cgiでないCGIファイルを実行したい場合に便利です。
ScriptAliasMatch	機能としてはScriptAliasと同じですが、変換元URLを正規表現で指定する点が異なります。 変換先Pathでは、後方参照として\$1, \$2...が使用できます。

●変換元 URL

変換元 URL には、アクセスされる URL を入力します。

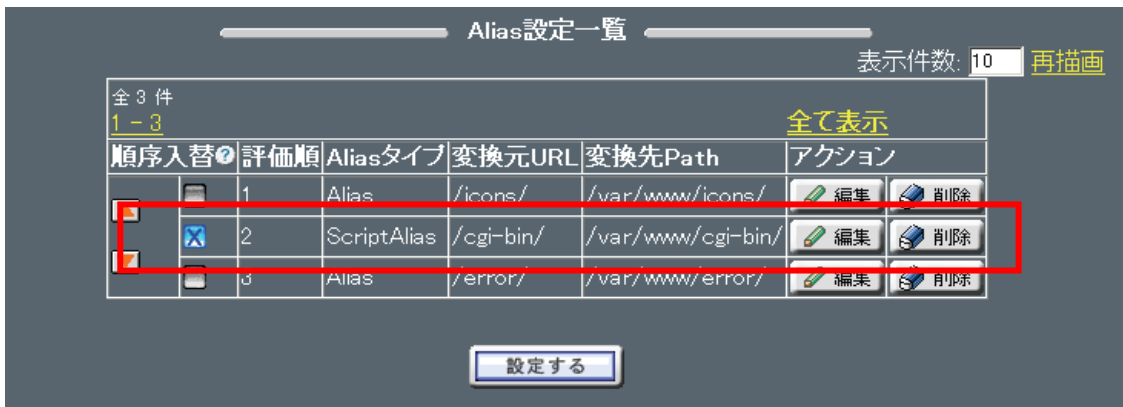
●変換先 Path

変換先 Path には、そのアドレスにアクセスした場合に実際にアクセスされる
ファイルシステム上の Path を入力または、「ディレクトリ選択」より選択します。

●Alias の評価順変更

追加された Alias 設定の評価順を変更します。

評価順を変更する行を選択し(複数選択可能)、上下ボタンを押すことにより、その行の評価順を上下に移動することができます。



移動し終わったら、「設定する」をクリックします。

Alias 設定は、評価順の昇順に評価されます。

すなわち、より上位にある Alias 設定のサブセットを、それよりも下位に指定しても有効になることはありません。

例) この場合、/abc/def にアクセスしても、より上位にある/abc のルールにマッチしてしまうため、/var/www/def へはアクセスされず、/var/www/abc/def にアクセスされます。

評価順	Aliasタイプ	変換元URL	変換先Path
1	Alias	/abc	/var/www/abc
2	ScriptAlias	/abc/def	/var/www/def

●Alias の編集

追加された Alias 設定の値を変更します。

一覧から編集したい行の「編集」をクリックします。

Alias タイプ、変換元 URL、変換先 Path を変更し、「OK」をクリックします。

全ての編集が終了したら、「設定する」をクリックします。

正しければ「OK」をクリックします。

ディレクトリ一覧画面に戻り「設定する」をクリックして終了します。

1-8. MIME 設定

●MIME 設定



ここでは、Web サーバーがデータ形式を認識するための、MIME タイプの設定を行います。

MIME タイプとは、Web サーバーのアクセスされるファイルがどんな性質なのかを定義するもので、「タイプ名/サブタイプ名」の形式の文字列で表します。

ファイルの関連付け情報である MIME タイプを正しく設定することで、閲覧者に正しく情報を提供することができます。

●MIME タイプの検索

登録されている MIME タイプを検索します。

検索条件として、「MIME タイプのカテゴリ」をメニューから選択します。

「MIME タイプの検索」に検索キーワードを入力します。

検索結果の表示件数を変更する場合は、「表示件数」の値を変更します。

「検索」をクリックして、検索を実行します。

MIME タイプの頭文字から検索する場合は、「MIME タイプの頭文字」に表示されている頭文字の範囲をクリックします。

登録されている全ての MIME タイプを一度に表示する場合は、「全て表示」をクリックします。

●MIME タイプの追加

MIME タイプを追加します。

MIMEタイプの追加

MIMEタイプ 拡張子 追加

全 3 件MIMEタイプの頭文字 a-t全てのカテゴリ

MIMEタイプ	拡張子	アクション
application/x-compress	<input type="text" value=".Z"/>	<input type="button" value="削除"/>
application/x-gzip	<input type="text" value=".gz .tgz"/>	<input type="button" value="削除"/>
text/html	<input type="text" value=".shtml"/>	<input type="button" value="削除"/>

MIME タイプ

「MIME タイプ」に追加する MIME タイプを入力します。（例:video/mpeg）

●拡張子

「拡張子」に追加する MIME タイプを割り当てるファイルの拡張子を入力します。（例:.mpeg）

「追加」をクリックして、MIME タイプを追加します。

登録されている MIME タイプに割り当てられている拡張子を変更する場合は、検索した MIME タイプの一覧から修正できます。

※MIME タイプを削除する場合は、「削除」をクリックします。

削除を取り消す場合は、再度ボタン(「取消」)をクリックします。

「設定する」をクリックして、設定を終了します。

1-9. ModSecurity 設定



ここでは、ModSecurity の設定を行います。

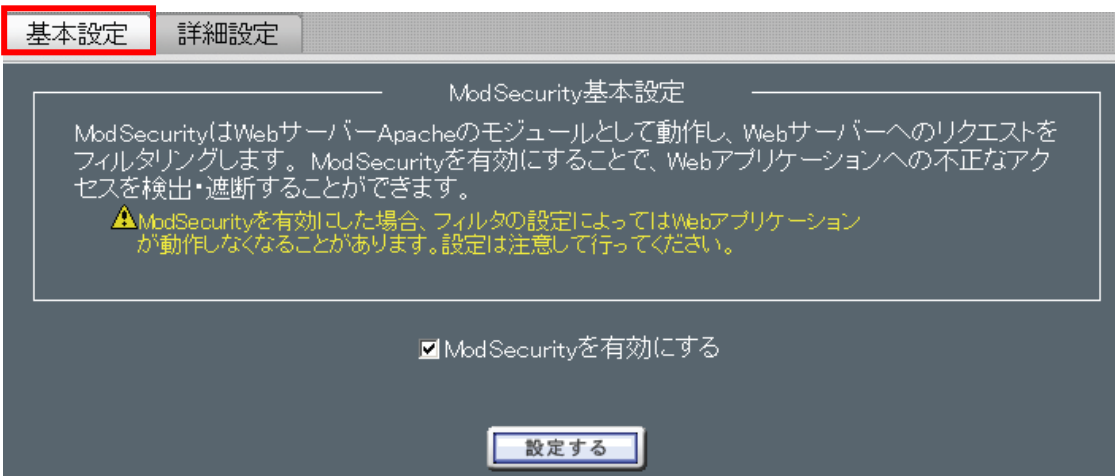
ModSecurity は Web サーバー Apache のモジュールとして動作し、Web サーバーへのリクエストをフィルタリングします。

ModSecurity を利用することで、Web アプリケーションへの不正なアクセスを検出・遮断することができます。

●基本設定

「ModSecurity を有効にする」をチェックし、「設定する」をクリックすると ModSecurity が有効になります。

※ModSecurity を有効にした場合、フィルタの設定によっては Web アプリケーションが動作しなくなることがあります。



●詳細設定

ModSecurityの詳細な設定を行います。

通常は特に設定を変更する必要はありません。

基本設定 **詳細設定**

ModSecurity詳細設定

ModSecurityの詳細な設定を行います。

フィルタリング設定

すべてのリクエストを検査?	<input type="checkbox"/> 有効にする
リクエストのボディを検査?	<input checked="" type="checkbox"/> 有効にする
URLエンコーディングを検査?	<input checked="" type="checkbox"/> 有効にする
Unicodeエンコーディングを検査?	<input type="checkbox"/> 有効にする
リクエスト長制限?	255 バイト
拒否時のステータスコード?	403

監査ログ設定

監査ログを記録?	<input checked="" type="checkbox"/> 有効にする
ログファイル名:	logs/audit_log <input type="button" value="選択"/>

※この項目は、基本設定で「ModSecurity を有効にする」にチェックが入っている場合のみ表示されます。

●すべてのリクエストを検査

すべてのリクエストを検査したい場合は有効にしてください。

有効にしない場合はCGIなどで動的に生成されたリクエストのみを検査します。

動的に生成されたリクエストのみを検査することで、リソースを節約することができます。

●リクエストのボディを検査

リクエストのボディを検査したい場合は有効にしてください。

GETメソッドのリクエストではボディにはなにも含まれませんが、POSTメソッドのリクエストではボディにデータが格納されています。

POSTされたデータを検査するには有効にする必要があります。

●URL エンコーディングを検査

URL エンコーディングが有効であるか確認します。

●Unicode エンコーディングを検査

Unicode エンコーディングが有効であるか確認します。

●リクエスト長制限

許可するリクエストの最大長さ(バイト)を指定します。

ただし、multipart/form-data(ファイルのアップロードなどに使用されます)が使用されたデータは制限の対象になりません。

●拒否時のステータスコード

ルールにマッチし拒否したリクエストに対して返すステータスコードを指定します。

●監査ログを記録

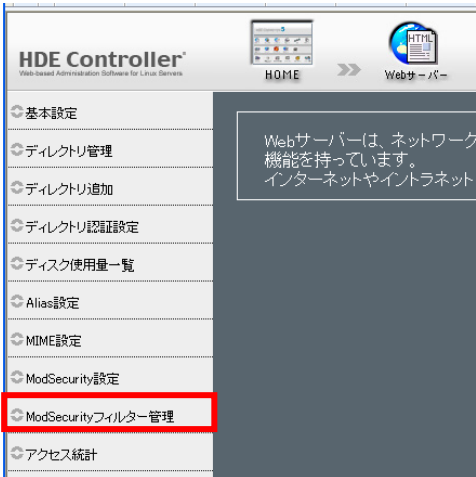
ルールにマッチし拒否したリクエストをログに記録したい場合は有効にしてください。

●ログファイル名

監査ログを記録するファイル名を指定します。

1-10. ModSecurity フィルター管理

●ModSecurity フィルター管理



ModSecurity のフィルタリングルールを設定します。

複数のルールをまとめたものをフィルターとして管理します。

●フィルターの追加

フィルターの追加を行います。



「優先度」、「フィルター名」を指定し、「追加」をクリックするとフィルターが追加されます。

フィルターを追加しただけでは、ルールは登録されていません。

「編集」をクリックしてルールの登録を行います。

●優先度

指定した優先度の位置にフィルターが挿入され、既存のフィルターがある場合は1つずつ後ろにずれます。

フィルターは優先度順に適用されます。

●フィルター名

フィルター名には、英数字と「-」「_」が使用できます。

フィルター名は、20文字以内で指定してください。

※「フィルターの一覧」の「有効」にチェックが入っていないフィルターは、有効になっていません。
有効にするには「有効」にチェックを入れ、「設定する」をクリックしてください。

●ルールの追加

追加したフィルター名の「編集」を押し、ルールを追加します。

ModSecurityフィルター編集

ルールの設定を行います。

フィルター設定

フィルター名: Recommended 有効: 有効にする

ルールの追加

優先度?:	6	+追加
検査対象?:		
文字列?:		
処理?:	deny	

「優先度」「検査対象」「文字列」「処理」を指定「追加」をクリックするとルールが追加されます。

●優先度

指定した優先度の位置にフィルターが挿入され、

既存のフィルターがある場合は1つずつ後ろにずれます。

フィルターは優先度順に適用されます。

●検査対象

検査する対象を指定します。

パイプ「|」で区切ることで、複数を指定することができます。

特に指定しない場合はリクエストすべてを検査対象にします。

詳細な記述方法は ModSecurity のマニュアルの「Request filtering」「Advanced filtering」の項を参照してください。

●文字列

検索する文字列です。正規表現が使用できます。

●処理

deny	リクエストを拒否します。「ModSecurity設定」「詳細設定」「拒否時のステータスコード」で指定したステータスコードを返します。
pass	「ModSecurity設定」「詳細設定」「監査ログを記録」が有効な場合は、リクエストのログ

	を記録します。
allow	リクエストを許可します。以降のルールは適用しません。
chain	そのルールにマッチした場合のみ、次のルールを適用します。

●設定の削除と編集方法

フィルターおよびルールについて、削除を行いたい場合

「削除」をクリックした後に、「設定する」もしくは、「OK」をクリックしてください。

フィルターおよびルールについて、編集を行いたい場合

「編集」をクリックした後に、追加と同様の画面が表示されます。

追加の項目を見ながら、必要な項目を編集してください。

フィルターの一覧

#	フィルター名	ルール数	有効	アクション
1	Recommended	5	<input checked="" type="checkbox"/>	編集 削除
2	Directory	1	<input type="checkbox"/>	編集 削除
3	XSS	1	<input type="checkbox"/>	編集 削除
4	SQL	3	<input type="checkbox"/>	編集 削除
5	CS_Command	1	<input type="checkbox"/>	編集 削除

ルールの一覧

#	検査対象	文字列	処理	アクション
1	REQUEST_METHOD	!(GET HEAD)\$	chain	削除
2	HTTP_Content-Type	!(application/x-www-form-urlencoded\$ ^multipart/form-data,)	deny	削除
3	REQUEST_METHOD	^POST\$	chain	削除
4	HTTP_Content-Length	^\$	deny	削除
5	HTTP_Transfer-Encoding	!^\$	deny	削除

●●フィルター設定例●●

例

ある Web アプリケーションの管理者アカウント

特定の IP アドレスからのみログインできる

その他の IP アドレスからのアクセスを拒否したい場合のフィルターを設定。

- 1 : フィルターを追加します。
- 2 : 「ModSecurity フィルター管理」の画面を表示してください。
- 3 : フィルター名は「admin」、優先度は「6」にすることにします。

4 : フィルター名を入力し、優先度を選択。

5 : 「追加」をクリックしてください。

ModSecurityフィルター管理

ModSecurityのフィルター管理を行います。フィルターは複数のルールから構成されます。

フィルターの追加

優先度?	6	フィルター名?	admin	+	追加
------	---	---------	-------	---	----

6 : フィルターの一覧に追加したフィルターが表示されます。

7 : 次にルールを登録します。「編集」をクリックしてください。

8 : 優先度は「1」を選択し、検査対象に「ARG_username」を入力、
文字列に「admin」を入力、処理は「chain」を選択。

9 : 「追加」をクリックしてください。

検査対象の「ARG_username」とは、username という名前の変数を表します。

ここで追加したルールは、username という変数に admin という文字列が含まれていた場合、この次のルールを適用するということを意味します。

ルールの追加

優先度?	1	+	追加
検査対象?	ARG_username		
文字列?	admin		
処理?	chain		

10 : 優先度は「2」を選択し、検査対象に「REMOTE_ADDR」を入力

文字列にコマンド「!^192.168.0.2\$」を入力、処理は「deny」を選択
「追加」をクリックしてください。

検査対象の「REMOTE_ADDR」はアクセス元の IP アドレスを表します。

ここで追加したルールは、アクセス元の IP アドレスが 192.168.0.2
に一致しない場合、アクセスを拒否するということを意味します。

ルールの追加

優先度?	2	+	追加
検査対象?	REMOTE_ADDR		
文字列?	~192.168.0.2\$		
処理?	deny		

11 : ルールを登録したら、「OK」をクリックします。

「フィルターの一覧」の「有効」にチェックが入っていることを確認。

12 : 「設定する」をクリックしてください。



1-11. アクセス統計

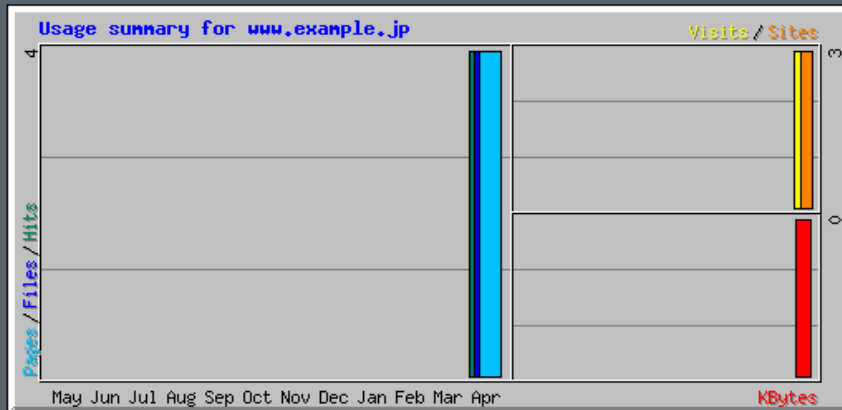


Web サーバーのログを解析し、解析結果を表示します。

月の統計、日ごとの統計、時間ごとの統計、ヒット数ランキング (URL、エントリー、Exit、サイト)、リファラー、検索文字列、ユーザーエージェント、国別統計が利用できます。

利用統計 www.example.jp

統計期間: 過去12ヶ月
作成日時 24-Apr-2008 23:33 JST



月の統計										
月	一日あたりの平均				月合計					
	Hits	Files	Pages	Visits	Sites	KBytes	Visits	Pages	Files	Hits
Apr 2008	4	4	4	3	3	0	3	4	4	4
総合計						0	3	4	4	4

Generated by [Webalizer Version 2.01](#)

表示される指標の意味は以下の通りです。

Hits	エラーを含む、Webサーバーへの全アクセス数
Files	Hitsのうち、正常なアクセスの数
Pages	Hitsのうち、HTMLページの数
Visits	訪問者数 (30分以内で同一のIPアドレスからのアクセスはカウントしない)
Sites	訪問者数 (同一のIPアドレスからのアクセスはカウントしない)
KBytes	転送したデータ量

月の統計以外の統計については、各月のリンクをクリックすると表示されます。

利用統計 www.example.jp

統計期間: April 2008
作成日時 24-Apr-2008 23:33 JST

[\[日ごとの統計\]](#) [\[時間ごとの統計\]](#) [\[URL\]](#) [\[エントリー\]](#) [\[Exit\]](#) [\[サイト\]](#) [\[リファラー\]](#) [\[検索文字列\]](#) [\[国\]](#)

月の統計 April 2008		
全ヒット数	4	
全ファイル数	4	
合計 Pages	4	
合計 Visits	3	
全 KBytes数	0	
個別サイト数	3	
個別URL数	1	
個別リファラー数	1	
	平均	最大
一時間あたりのヒット数	0	4
一日あたりのヒット数	4	4
一日あたりのファイル数	4	4
一日あたりのページ数	4	4
一日あたりの訪問者数	3	3
一日あたりのKBytes数	0	0
レスポンスコードごとのヒット数		
Code 200 - OK	4	

マイサーバーサービス 利用マニュアル (root 権限者用 Web サーバー設定) マイサーバーVPS compact

発行元 : 株式会社イージェーワークス

発効日 : 2010 年 7 月 9 日 rev1

リムネット カスタマーサポートセンターの連絡先

電話窓口 : 0120-678-309

ファックス : 045-472-2777

メール : support@rim.or.jp

受付時間 : 24 時間 365 日

本マニュアルに記載されている内容の著作権は、原則として株式会社イージェーワークスに帰属します。
著作権法により、当社に無断で転用、複製等することはできません。