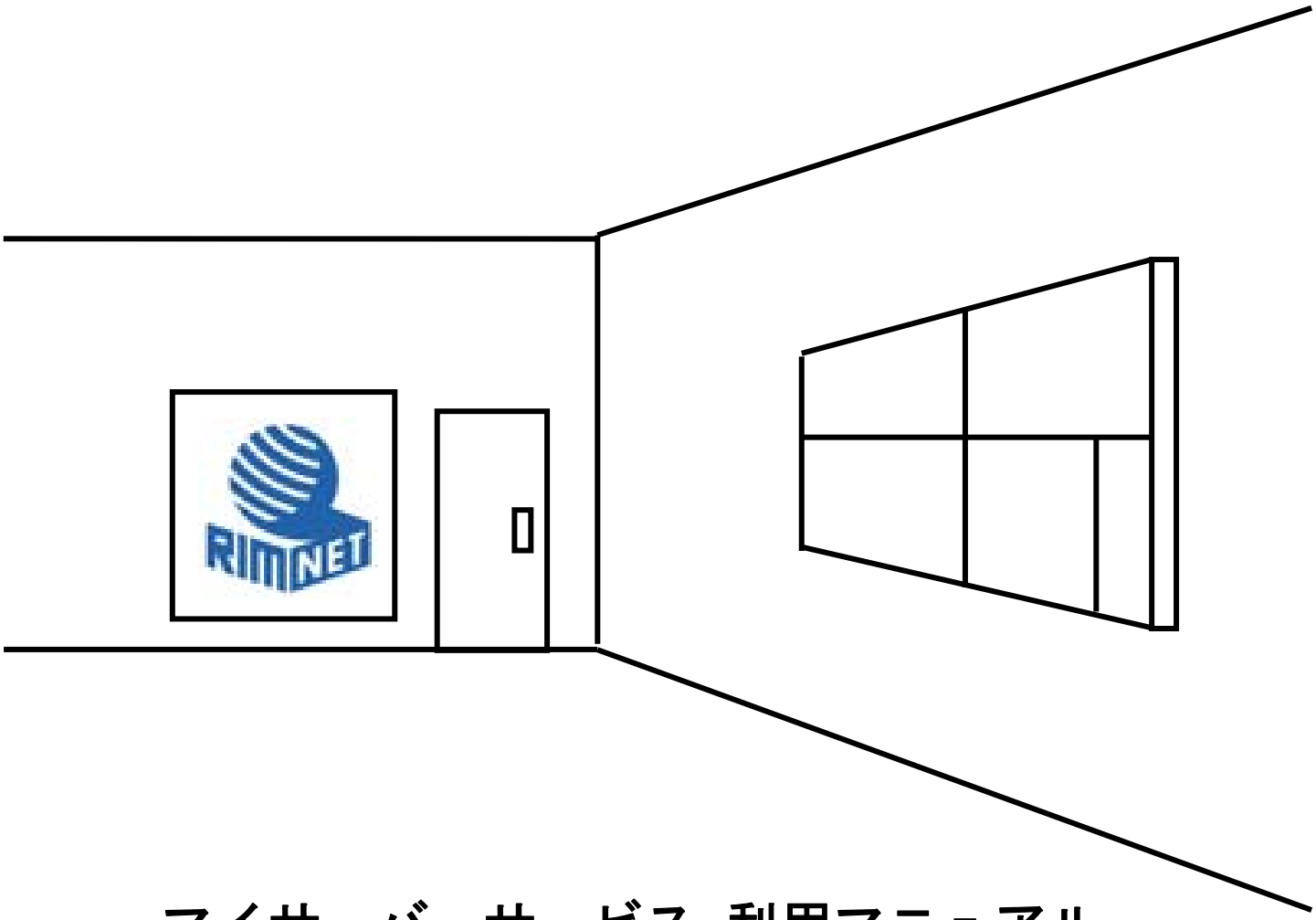


マイサーバーサービス 利用マニュアル

（セキュア 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、マイサーバーVPS compactの「セキュアWebサーバー」の設定を解説します。

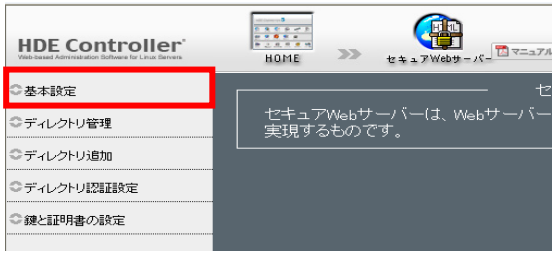
目次

１．セキュア Web サーバー

１－１．概要

HDE Controller にログインし、「セキュア Web サーバー」のアイコンをクリックします。
次項の項目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（セキュア Web サーバー）



●「サーバー名」「ポート番号」「管理者メールアドレス」「ドキュメントルート」の各項目を正しく入力します。

●サーバー名
外部に公開するサーバー名を入力します。（この例では www.example.com と指定）

●ポート番号
通常は 443 です。
変更した場合は、このサーバーにアクセスする URL が https://www.example.com:443/
のように、「：」の後に指定したポート番号を入力する必要が出てきます。

●管理者メールアドレス
管理者メールアドレスには、Web 管理者のメールアドレスを入力します。
多くの場合、ここには個人のアドレスではなく「webmaster@example.com」等のような管理者用のアドレスを入力します。
（これらのアドレスは最終的にはメールサーバーの設定や、メーリングリストを使用して管理者に届くように設定します。）

●ドキュメントルート

Web サーバーとして公開したいディレクトリを指定します。

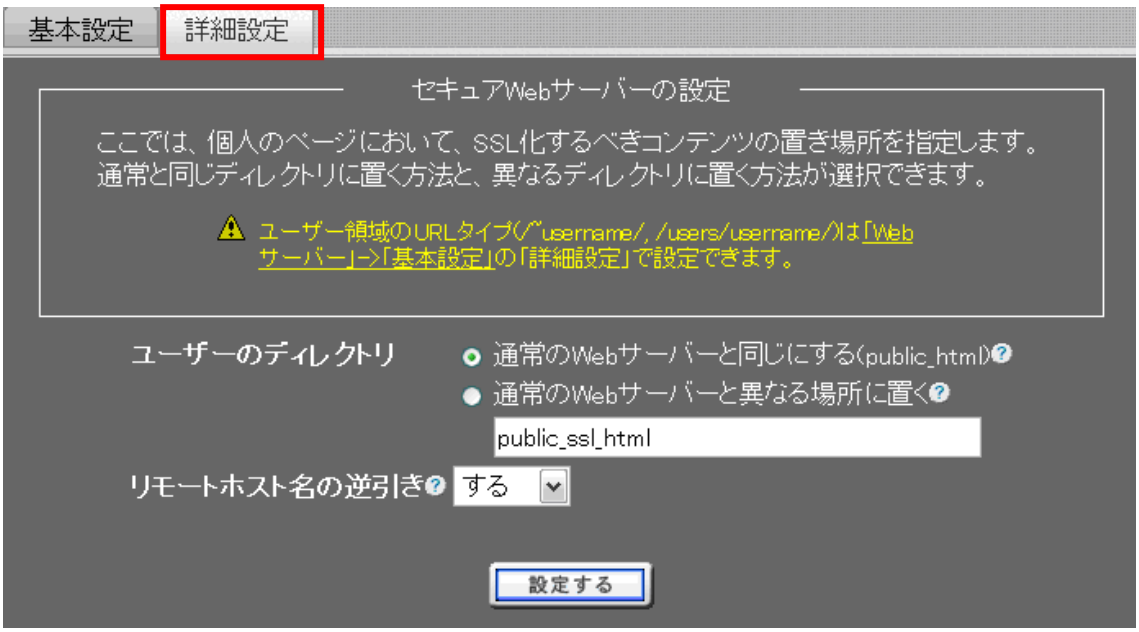
ドキュメントルートを管理するユーザーのホームディレクトリにディレクトリを作成し、そのディレクトリをドキュメントルートとして FTP でファイルをアップロードすると表示が可能となります。

※「ポート番号」「ドキュメントルート」は通常は変更する必要はありませんが、 Web サイトの管理者とサーバー管理者が異なる場合は、ドキュメントルートを Web サイト管理者のホームディレクトリに変更すると便利です。

「設定する」をクリックし、設定を完了します。

●詳細設定

セキュア Web サーバーを通して公開する、ユーザーのディレクトリを設定します。



バーチャルドメインのユーザーが、SSL 化された Web を公開する際に html ファイルをアップロードする場所を指定できます。

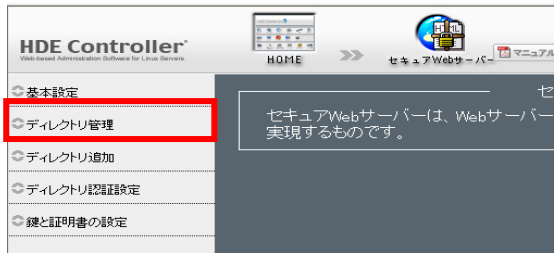
デフォルトでは、通常の Web を公開するディレクトリと同じに設定されていますが、異なるディレクトリを利用したい場合は「通常の Web サーバーと異なる場所に置く」にチェックをして、ディレクトリを入力します。

「設定する」をクリックすると設定が完了します。

ユーザーごとに設定することはできません。全てのユーザーに対して有効になります。

１－３．ディレクトリ管理・追加・ディレクトリ認証設定・アクセス統計

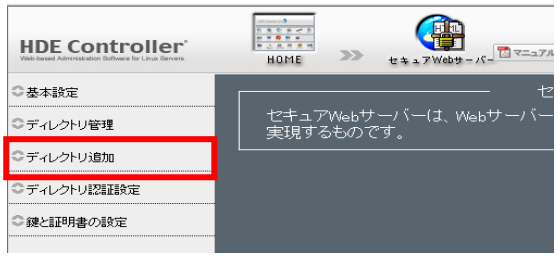
●ディレクトリ管理



セキュア Web サーバーのディレクトリについて個別に管理・設定します。

「 Web サーバー」の「ディレクトリ管理」をご参照ください。

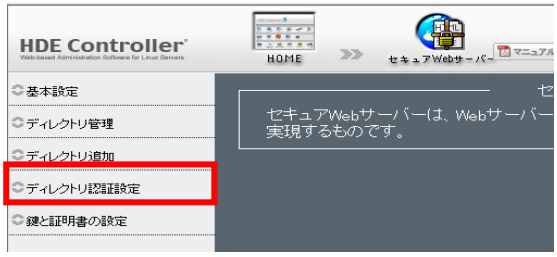
●ディレクトリ追加



セキュア Web サーバーのディレクトリについて個別に追加します。

「 Web サーバー」の「ディレクトリ追加」をご参照ください。

●ディレクトリ認証設定



セキュア Web サーバーのディレクトリの認証設定をします。

「 Web サーバー」の「ディレクトリ認証設定」をご参照ください。

●ディレクトリ管理・追加・認証設定・アクセス統計の復習及び説明

■エラーメッセージの設定

運用ポリシーに合わせて選択をしてください。

「設定する」をクリックすると設定が完了します。

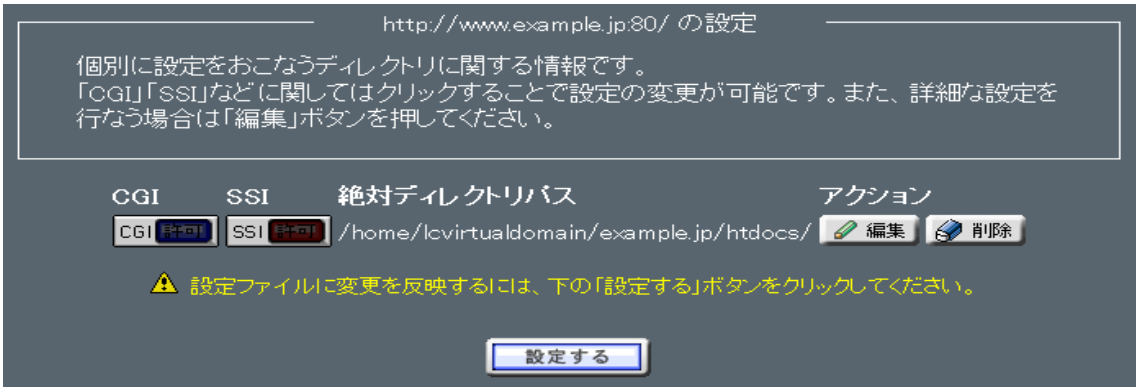
■CGI/SSI の設定について

HDE Controller では、ドキュメントルートの下(/home/lcvirtualdomain/ドメイン名/htdocs/cgi-bin)に cgi-bin ディレクトリが設定済ですが、ディレクトリを事前に作成しておく必要がありますので、FTP クライアントソフトやファイルマネージャーを利用して htdocs の下に cgi-bin ディレクトリを作成する必要があります。

上記以外のディレクトリやドキュメントルートに対して CGI/SSI を有効に設定する場合は、ディレクトリの管理/追加で行います。

■ディレクトリ管理

●CGI・SSI の設定



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。

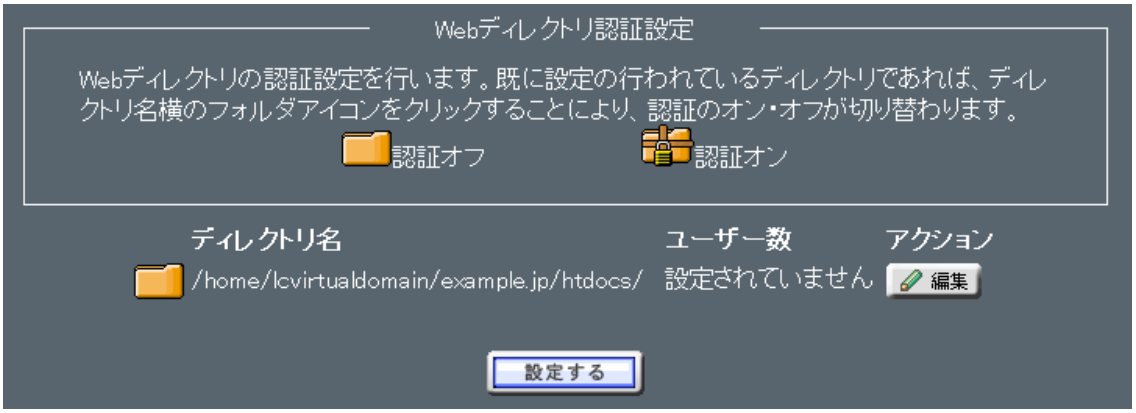
追加したディレクトリにホストの制限をかけない場合は、ホストの制限はデフォルトのままにしておきます。

設定の変更は、「ディレクトリ管理」画面より行うことができます。

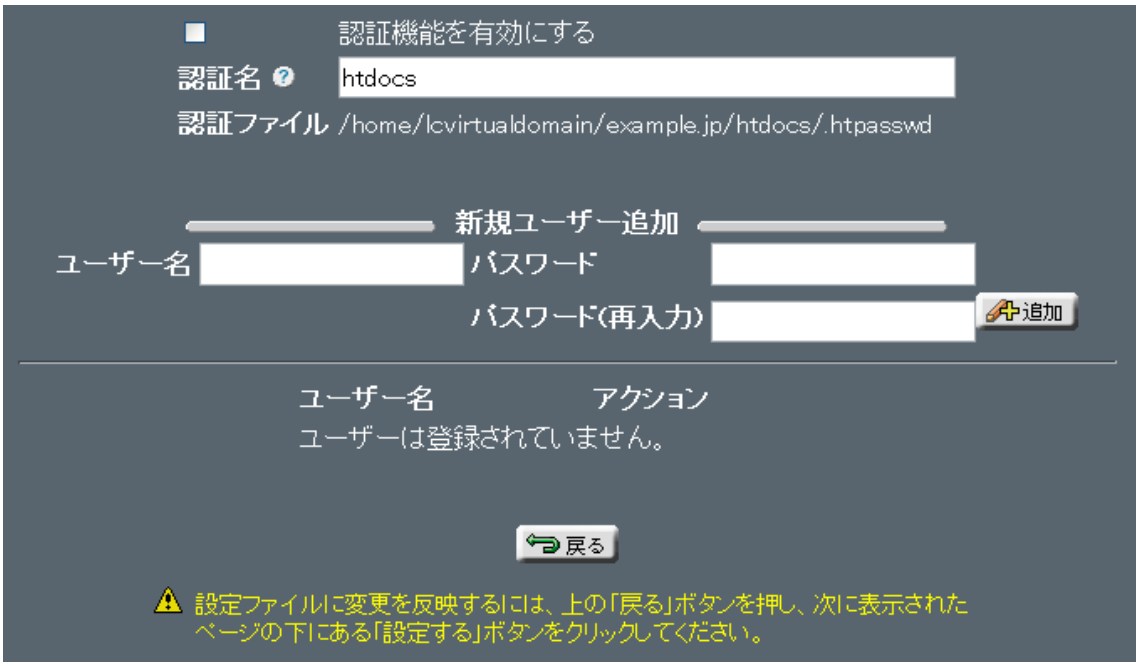
バーチャルドメインのユーザーにCGI/SSIを許可する設定は、リアルドメインからのみ行えます。

■ディレクトリ認証について

特定のディレクトリにアクセスした際に、ログイン名とパスワードの入力を求めるように設定するには「ディレクトリ認証設定」画面で行います。



設定を行う方法



１：「ディレクトリ追加」画面で、認証を設定したいディレクトリを追加します。

２：「ディレクトリ認証設定」画面で、追加しておいたディレクトリ名のフォルダアイコンか「編集」をクリックします。

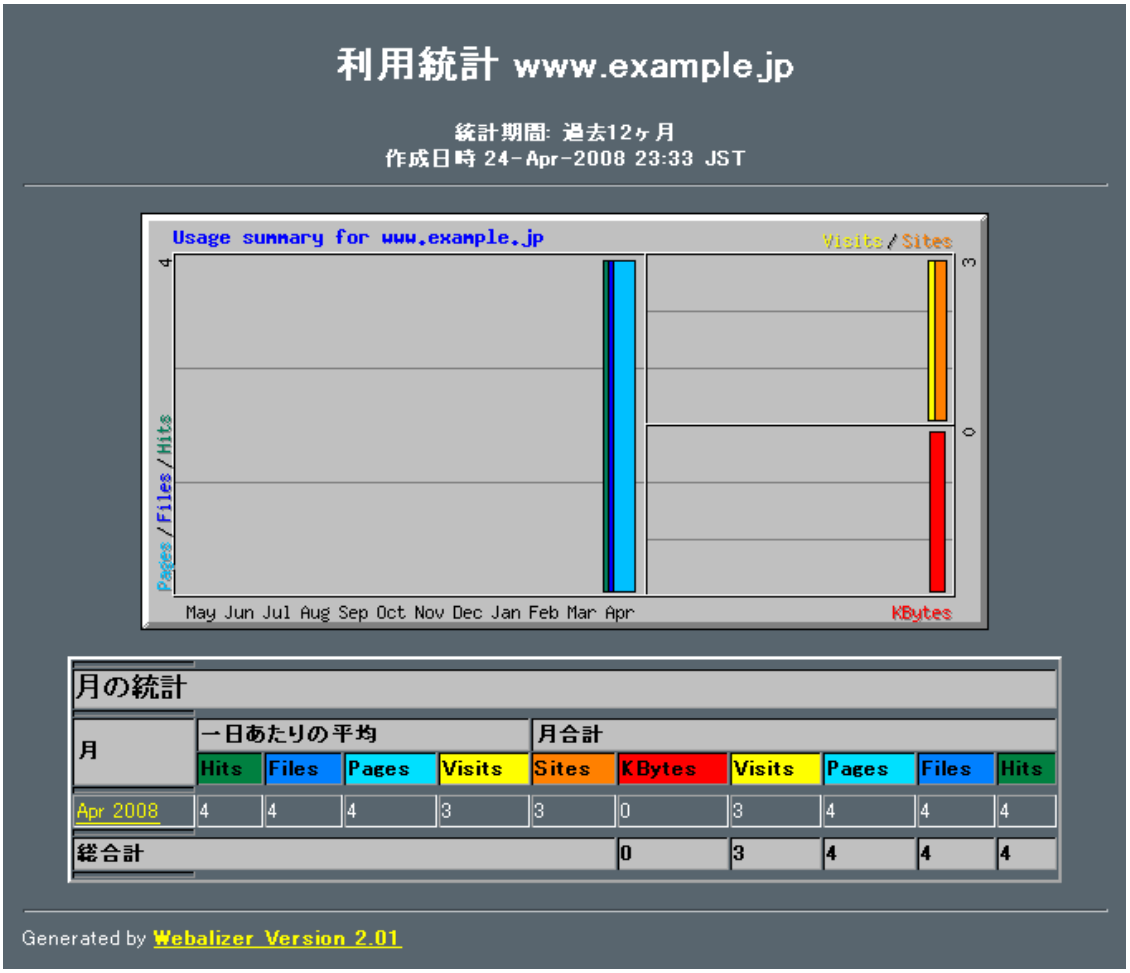
３：「認証機能を有効にする」にチェックをして、ユーザー名とパスワードを入力して「追加」をクリックします。
複数のユーザー名とパスワードを設定したい場合は、繰り返し追加してください。

４：追加が完了しましたら、「戻る」をクリックして「設定する」をクリックしてください。

■アクセス統計について

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。



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

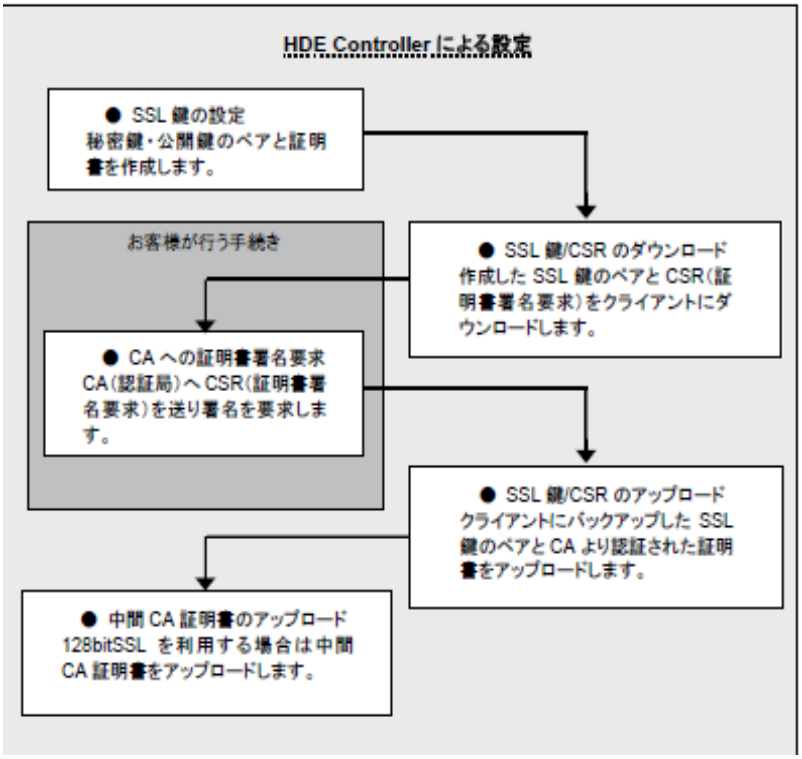
[日ごとの統計] [時間ごとの統計] [URL] [エントリー] [Exit] [サイト] [リファラー] [検索文字列] [国]

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	

１－４．鍵と証明書の設定

■鍵と証明書（SSL）設定

●設定の流れ



●既にサイト証明書を取得している場合

「鍵・証明書のアップロード」よりアップロードをおこなってください。

※重要※

●新規にサイト証明書を取得する場合

以下の手順で証明書署名要求(CSR)を作成して、お申し込みください。

１：「Web サーバーの SSL キー設定」画面で、必要事項を入力

２：「新しい SSL 秘密鍵/公開鍵のペアと、証明書を作り直します。」にチェック

３：「設定する」をクリックします。

４：証明書署名要求(CSR)が作成されます。
「鍵・証明書のダウンロード」画面より証明書署名要求(CSR)をダウンロードして証明書発行機関に申請してください。

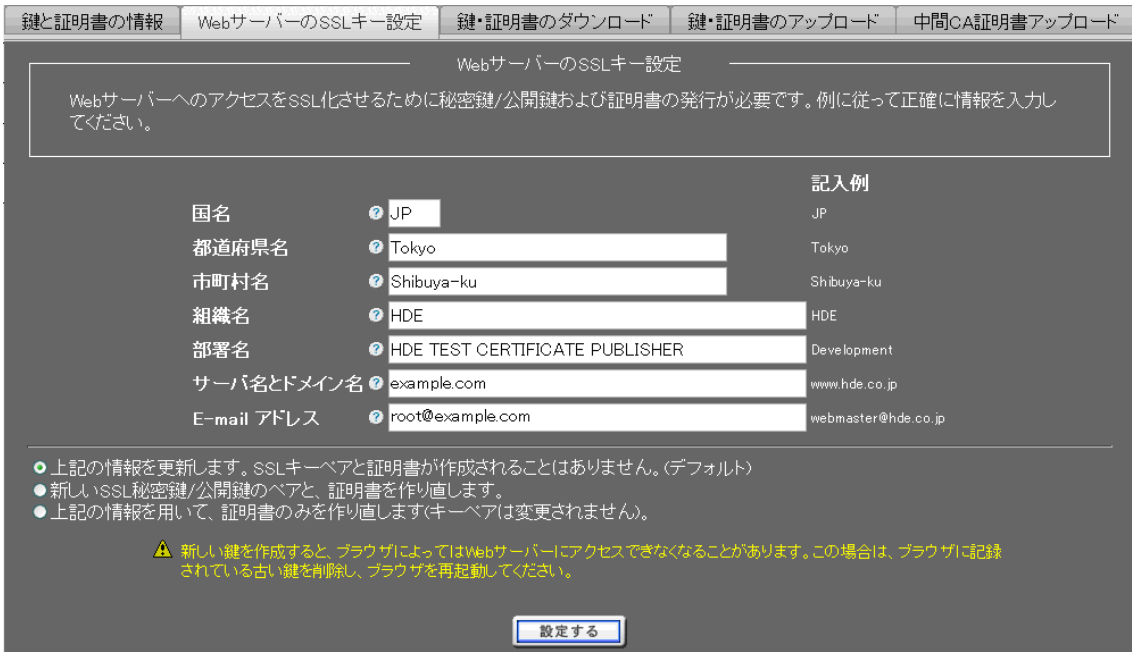
５：証明書発行機関より発行されたサイト証明書を「鍵・証明書のアップロード」よりアップロードを行ってください。

●現在の証明書の情報

現在設定されている証明書の情報が表示されます。

●SSL 鍵の設定

セキュア Web サーバー用の SSL 鍵を設定します。



Web サーバーへのアクセスを SSL 化させるため

この設定により秘密鍵／公開鍵および証明書の発行が必要です。

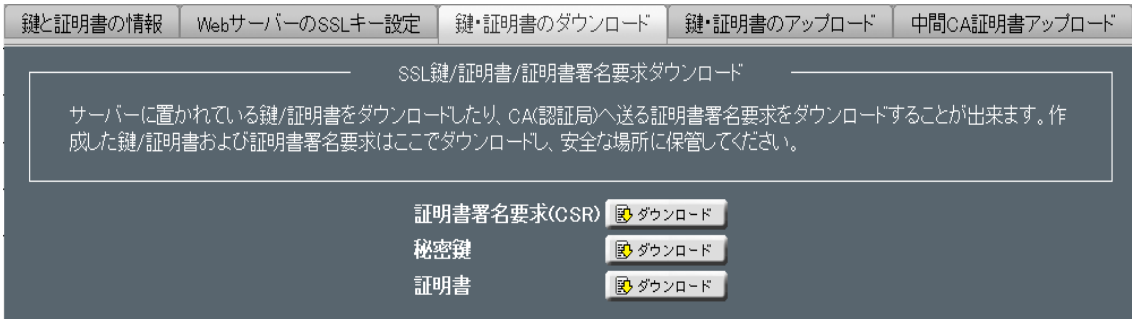
「国名／都道府県名／市町村名／組織名／サーバー名とドメイン名／E-mail アドレス」を正しく入力します。

設定方法として、下表のいずれかから選択します。

●SSL 鍵の設定方法

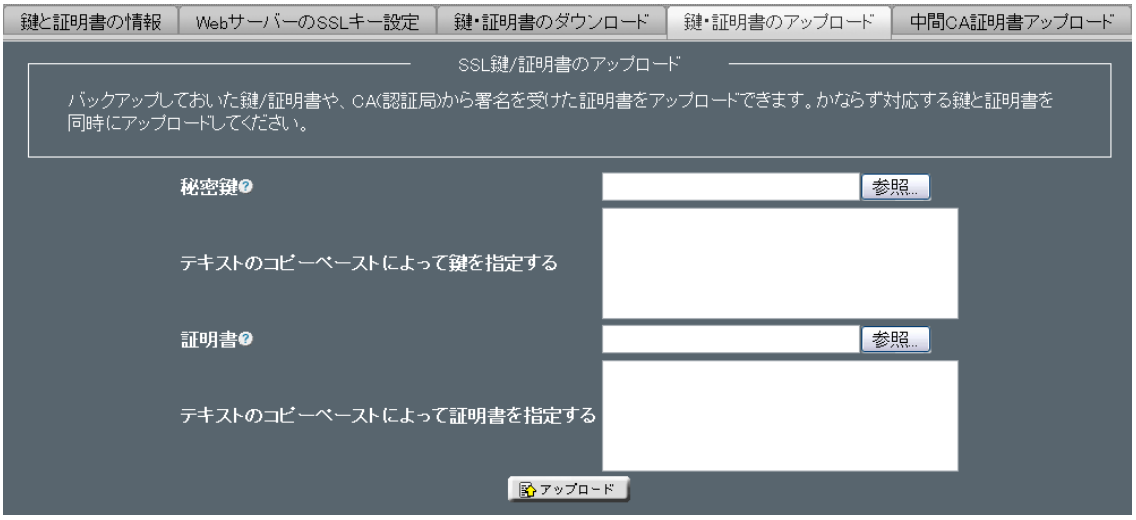
チェックボックスの選択肢	動作の概要
上記の情報を更新します。 SSL鍵のペアと証明書が作成される ことはありません。	既に設定されている証明書の情報のみを更新します。
新しいSSL秘密鍵／公開鍵のペアと 証明書を作り直します。	新規にSSL秘密鍵／公開鍵、証明書を作成します。 初めて設定する場合や証明書を変更する場合は必ず行ないます。
上記の情報を用いて、証明書のみを 作り直します。	既に設定されている鍵／証明書情報を元に、証明書のみを 作り直します。

●SSL 鍵/証明書/CSR ダウンロード



〇SSL 鍵・証明書と CSR（証明書署名要求）をクライアントにダウンロードすることができます。
〇CSR は CA（認証局）へ送付するためにダウンロードを行います。
〇秘密鍵・公開鍵ペア、および、証明書はバックアップのためにダウンロードを行います。
〇「ダウンロード」をクリックするとファイルをダウンロードすることができます。

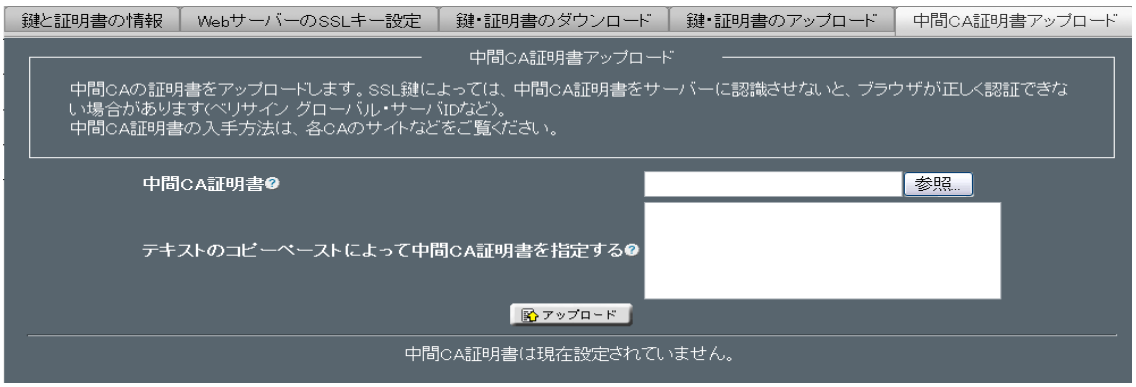
●SSL 鍵/証明書アップロード



〇SSL 鍵・証明書をクライアントからアップロードすることができます。
〇アップロードする鍵、証明書は必ず対応するものを同時にアップロードします。
〇ファイルの保存されているパスを、「秘密鍵／公開鍵ペア」「証明書」
　それぞれに入力するか「参照」をクリックし直接ファイルが存在するディレクトリを指定します。
〇テキストを直接入力することも可能です。

※ファイルを指定する方法と、直接入力する方法を同時に行うことはできません。
※パスフレーズ付きの秘密鍵は利用することができません。

●中間 CA 証明書アップロード



中間 CA 証明書をアップロードします。
SSL の鍵の一部には、Web ブラウザが正しく認証を行うために「中間 CA 証明書」のアップロードを必要とするものがあります。(128bit SSL を利用する場合に必要になります。)
ベリサイングローバルサーバーID など、中間 CA 証明書の入手方法は、各 CA のサイトなどをご覧下さい。

マイサーバーサービス 利用マニュアル
(セキュア Web サーバー)
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