

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

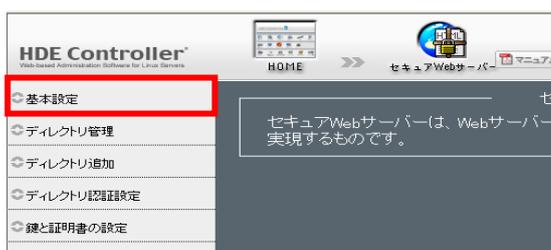
はじめに	1
目次	1
1. セキュア Web サーバー	2
1-1. 概要	2
1-2. 基本設定 (セキュア Web サーバー)	2
1-3. ディレクトリ管理・追加・ディレクトリ認証設定・アクセス統計	4
1-4. 鍵と証明書の設定	9

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あります。

●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。

The screenshot shows a dialog box titled 'セキュアWebサーバーの設定' (Secure Web Server Settings). At the top, there are two tabs: '基本設定' (Basic Settings) and '詳細設定' (Detailed Settings), with the latter highlighted in red. The main content area contains the following text: 'ここでは、個人のページにおいて、SSL化するべきコンテンツの置き場所を指定します。通常と同じディレクトリに置く方法と、異なるディレクトリに置く方法が選択できます。' (Here, in a personal page, you specify the location for content to be SSL-ized. You can choose between the usual method of placing it in the same directory or a different one.) Below this is a warning icon and text: 'ユーザー領域のURLタイプ(/username/, /users/username/)は「Webサーバー」->「基本設定」の「詳細設定」で設定できます。' (The URL type for the user area (/username/, /users/username/) can be set in 'Web Server' -> 'Basic Settings' -> 'Detailed Settings'.) The 'ユーザーのディレクトリ' (User Directory) section has two radio buttons: '通常のWebサーバーと同じにする(public_html)' (checked) and '通常のWebサーバーと異なる場所に置く' (Place in a different location than the usual web server). A text input field below contains 'public_ssl_html'. The 'リモートホスト名の逆引き' (Reverse lookup of remote host name) section has a checked checkbox and a dropdown menu set to 'する' (Do). At the bottom is a '設定する' (Set) button.

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。

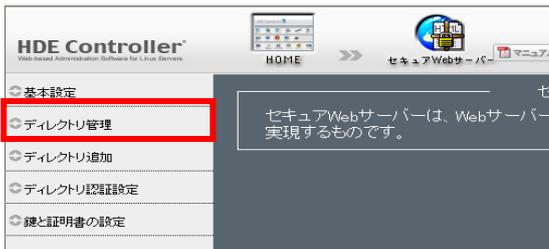
デフォルトでは、通常の Web を公開するディレクトリと同じに設定されていますが、異なるディレクトリを利用したい場合は「通常の Web サーバーと異なる場所に置く」にチェックをして、ディレクトリを入力します。

「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

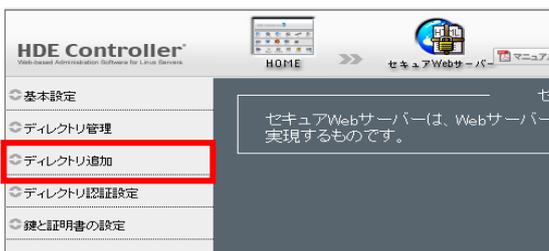
●ディレクトリ管理



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。

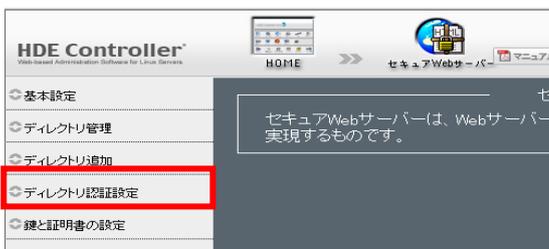
●ディレクトリ追加



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/追加を行います。

■ディレクトリ管理

●CGI・SSI の設定

http://www.example.jp:80/ の設定

個別に設定をおこなうディレクトリに関する情報です。
「CGI」「SSI」などに関してはクリックすることで設定の変更が可能です。また、詳細な設定を行なう場合は「編集」ボタンを押してください。

CGI	SSI	絶対ディレクトリパス	アクション
<input type="checkbox"/>	<input type="checkbox"/>	/home/lcvirtualdomain/example.jp/htdocs/	<input type="button" value="編集"/> <input type="button" value="削除"/>

⚠ 設定ファイルに変更を反映するには、下の「設定する」ボタンをクリックしてください。

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。

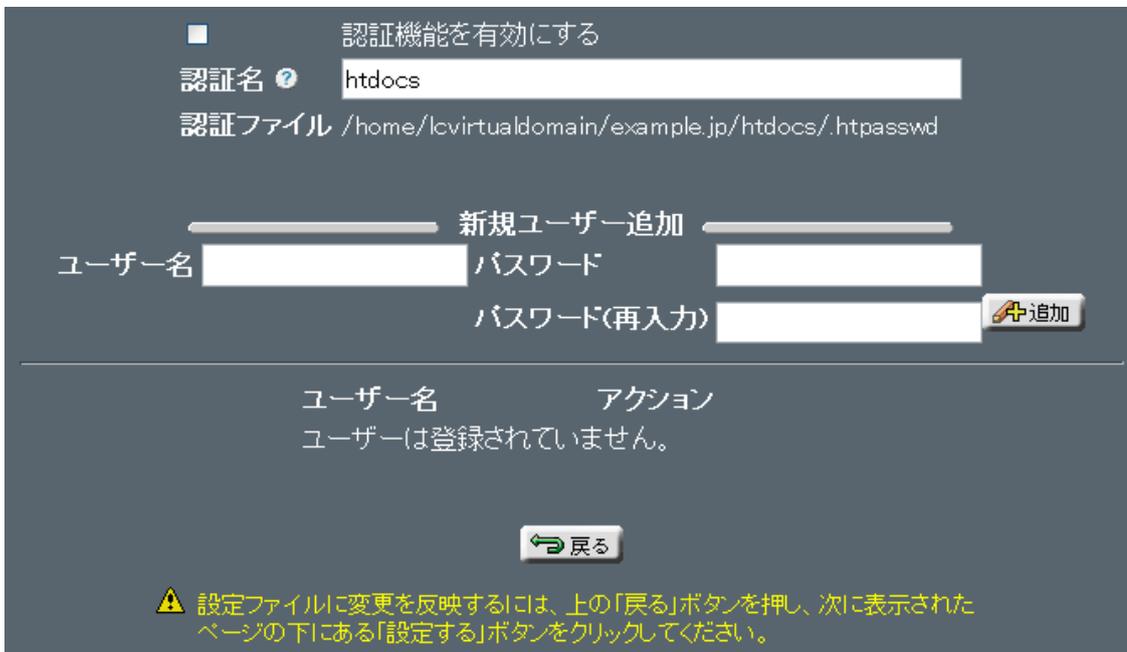
バーチャルドメインのユーザーにCGI/SSIを許可する設定は、リアルドメインからのみ行えます。

■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

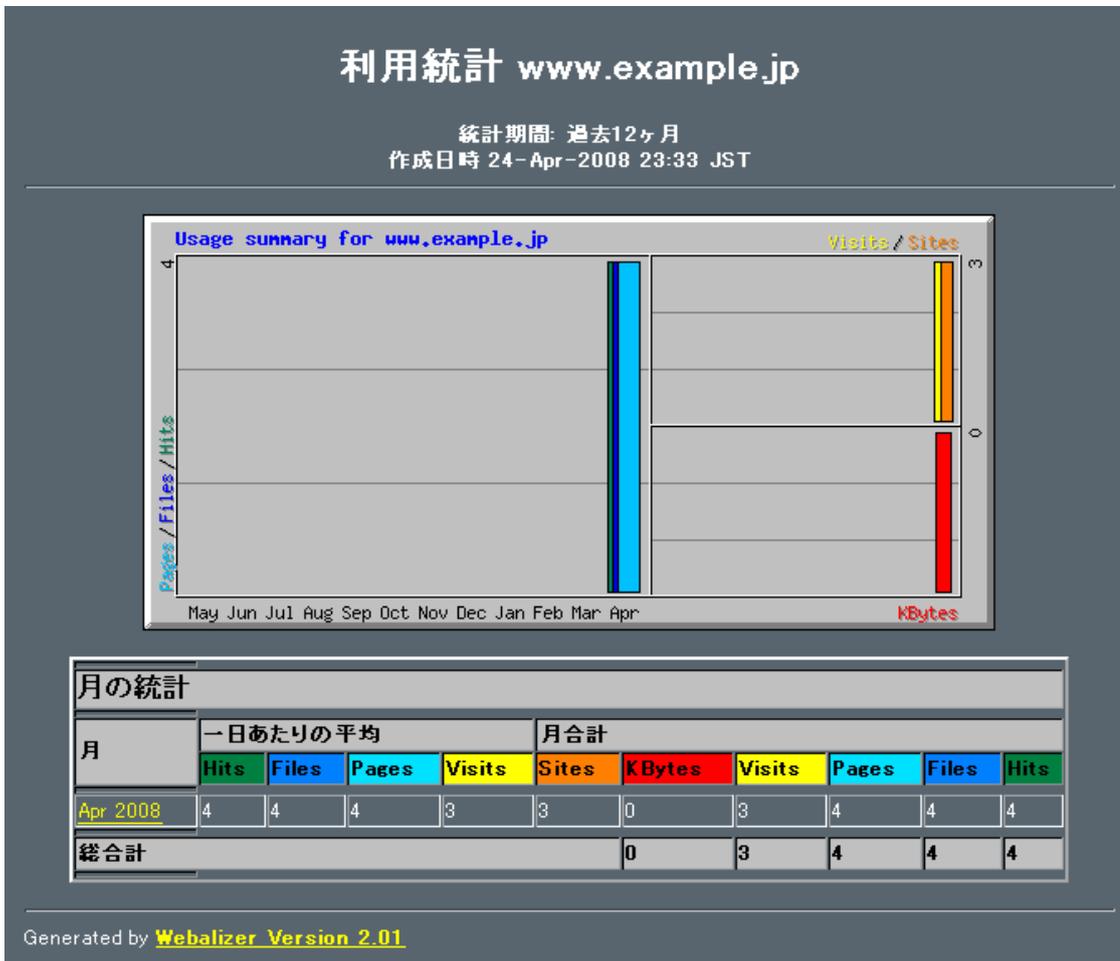


- 1 : 「ディレクトリ追加」画面で、認証を設定したいディレクトリを追加します。
- 2 : 「ディレクトリ認証設定」画面で、追加しておいたディレクトリ名のフォルダアイコンか「編集」をクリックします。
- 3 : 「認証機能を有効にする」にチェックをして、ユーザー名とパスワードを入力して「追加」をクリックします。複数のユーザー名とパスワードを設定したい場合は、繰り返し追加してください。
- 4 : 追加が完了しましたら、「戻る」をクリックして「設定する」をクリックしてください。

■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

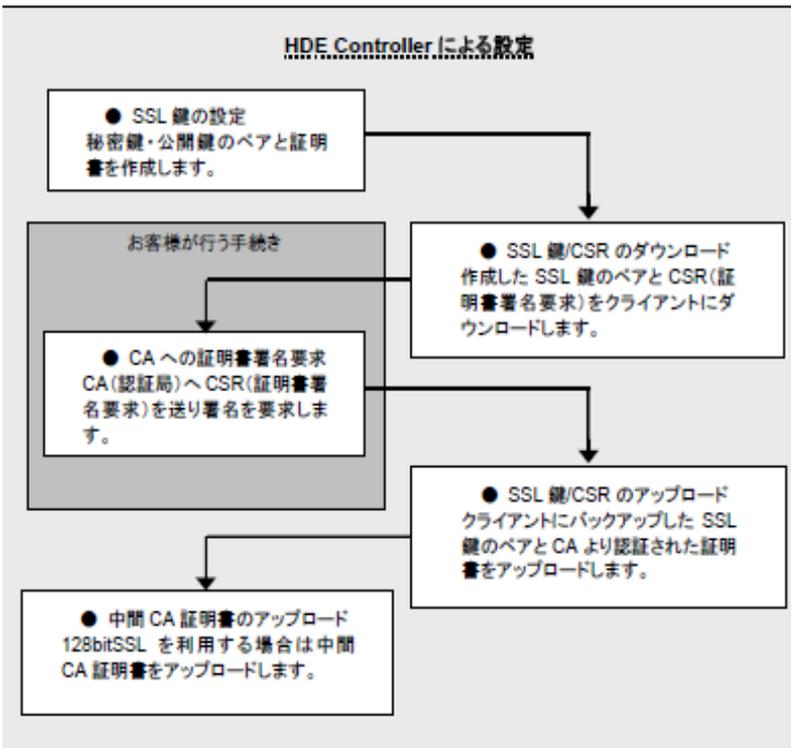
[\[日ごとの統計\]](#) [\[時間ごとの統計\]](#) [\[URL\]](#) [\[エントリー\]](#) [\[Exit\]](#) [\[サイト\]](#) [\[リファラー\]](#) [\[検索文字列\]](#) [\[国\]](#)

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。

鍵と証明書の情報 WebサーバーのSSLキー設定 鍵・証明書のダウンロード 鍵・証明書のアップロード 中間CA証明書アップロード

鍵と証明書の情報

ここでは、WebサーバーをSSL化するための秘密鍵/公開鍵のペア、および鍵の証明書の作成を行います。鍵および証明書は、一度作成すれば証明書の有効期限が切れるまでは変更の必要はありません。証明書の有効期限が切れたとき、あるいは、以下の設定に誤りがある場合のみ、新しい鍵および証明書の作成を行うようにしてください。

現在の証明書の情報

	受領者①	発行者②
国名	JP	JP
都道府県名	Tokyo	Tokyo
市町村名	Shibuya-ku	Shibuya-ku
組織名	HDE	HDE
部署名	HDE TEST CERTIFICATE PUBLISHER	HDE TEST CERTIFICATE PUBLISHER
サーバ名とドメイン名	example.com	example.com
E-mail アドレス	root@example.com	root@example.com

●SSL 鍵の設定

セキュア Web サーバー用の SSL 鍵を設定します。

鍵と証明書の情報 WebサーバーのSSLキー設定 鍵・証明書のダウンロード 鍵・証明書のアップロード 中間CA証明書アップロード

WebサーバーのSSLキー設定

WebサーバーへのアクセスをSSL化させるために秘密鍵/公開鍵および証明書の発行が必要です。例に従って正確に情報を入力してください。

国名	<input type="text" value="JP"/>	記入例	JP
都道府県名	<input type="text" value="Tokyo"/>		Tokyo
市町村名	<input type="text" value="Shibuya-ku"/>		Shibuya-ku
組織名	<input type="text" value="HDE"/>		HDE
部署名	<input type="text" value="HDE TEST CERTIFICATE PUBLISHER"/>		Development
サーバ名とドメイン名	<input type="text" value="example.com"/>		www.hde.co.jp
E-mail アドレス	<input type="text" value="root@example.com"/>		webmaster@hde.co.jp

●上記の情報を更新します。SSLキーペアと証明書が作成されることはありません。(デフォルト)
●新しいSSL秘密鍵/公開鍵のペアと、証明書を作り直します。
●上記の情報をを用いて、証明書のみを作り直します(キーペアは変更されません)。

⚠ 新しい鍵を作成すると、ブラウザによってはWebサーバーにアクセスできなくなることがあります。この場合は、ブラウザに記録されている古い鍵を削除し、ブラウザを再起動してください。

設定する

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

鍵と証明書の情報 WebサーバーのSSLキー設定 **鍵・証明書のダウンロード** 鍵・証明書のアップロード 中間CA証明書アップロード

SSL鍵/証明書/証明書署名要求ダウンロード

サーバーに置かれている鍵/証明書をダウンロードしたり、CA(認証局)へ送る証明書署名要求をダウンロードすることができます。作成した鍵/証明書および証明書署名要求はここでダウンロードし、安全な場所に保管してください。

証明書署名要求(CSR)

ダウンロード

秘密鍵

ダウンロード

証明書

ダウンロード

○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。

○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。

○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。

○「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

鍵と証明書の情報 WebサーバーのSSLキー設定 鍵・証明書のダウンロード **鍵・証明書のアップロード** 中間CA証明書アップロード

SSL鍵/証明書のアップロード

バックアップしておいた鍵/証明書や、CA(認証局)から署名を受けた証明書をアップロードできます。かならず対応する鍵と証明書を同時にアップロードしてください。

秘密鍵

参照...

テキストのコピーペーストによって鍵を指定する

証明書

参照...

テキストのコピーペーストによって証明書を指定する

アップロード

- 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。
- 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。
- 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。
- 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場合があります。(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ください。

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

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。