2. セキュア Web サーバー

2. セキュア Web サーバー

1. 基本設定

セキュア Web サーバーの基本的な設定を行ないます。

■ 基本設定

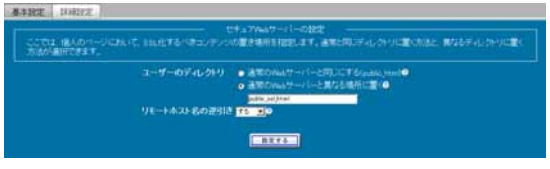
「サーバー名」「管理者メールアドレス」を入力します。

「設定する」ボタンをクリックして、設定を終了します。

root ユーザーはポート番号を変更することもできます。

■ 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。



通常の Web サーバーと同じ設定(public_html)にする場合は、

「通常の Web サーバーと同じにする」を選択します。

通常の Web サーバーと異なるディレクトリを指定する場合は、

「通常の Web サーバーと異なる場所に置く」を選択し、ディレクトリ名を入力します。

リモートホスト名を逆引きする場合は「リモートホスト名の逆引き」を「する」に設定します。「する」に設定した場合、アクセス元のホスト名が、アクセスログに記録されますが、Web サーバーのパフォーマンスが低下することがあります。

正しければ「設定する」ボタンをクリックして、設定を終了します。

2. 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。

■ 基本設定

CGI、および、SSI を有効にする場合は「CGI」「SSI」をクリックします。ボタンが点灯した状態に変わります。
正しければ「設定する」ボタンをクリックして設定を終了します。

■ 詳細な設定

詳細な設定を行う場合は、ディレクトリ一覧画面から「編集」ボタンをクリックします。
「ディレクトリの設定」「アクセス制御」の設定タブが表示されます。

「ディレクトリの設定」メニューでは、ディレクトリの変更、CGI・SSI の使用可否を設定します。
ディレクトリを変更する場合は、ディレクトリの場所を修正します。
CGI・SSI の使用許可を設定します。
設定が正しければ「OK」ボタンをクリックしてディレクトリ一覧画面に戻ります。
「設定する」ボタンをクリックして設定を終了します。

アクセス制御メニューでは、ディレクトリのアクセス制限を設定します。

同じドメインのみ許可する場合は、「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、許可サイト優先か、不許可サイト優先か選択し、「許可サイト」「不許可サイト」それぞれに適切な値／ドメイン名を入力します。
正しければ「OK」ボタンをクリックします。

2. セキュア Web サーバー

● **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

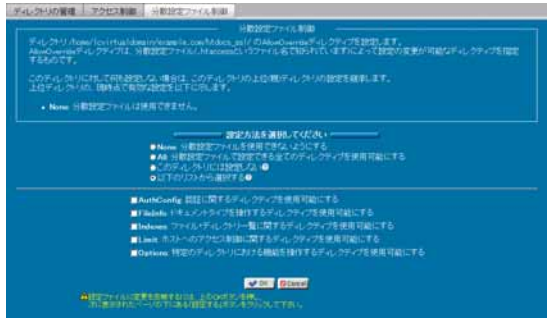
ディレクトリー一覧画面に戻り「設定する」ボタンをクリックして設定を終了します。

■ 分散設定ファイル制御

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。

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	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

正しければ「OK」ボタンをクリックします。

ディレクトリ一覧画面に戻り「設定する」ボタンをクリックして終了します。

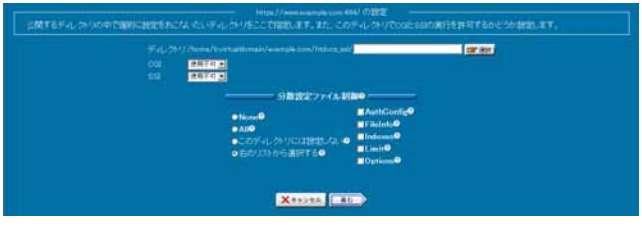
2. セキュア Web サーバー

3. ディレクトリ追加

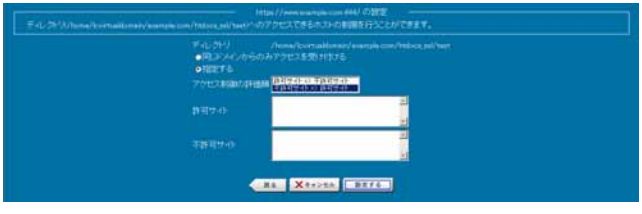
セキュア Web サーバーのディレクトリを追加します。

■ ディレクトリの追加

セキュア Web サーバーを通して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。



公開するディレクトリのパスを「ディレクトリ」に入力するか、「選択」ボタンをクリックして、ディレクトリ選択画面から選択します。
CGI・SSI の使用を、「使用可」「使用不可」から選択します。
「進む」ボタンをクリックして、次の設定へ進みます。



ディレクトリのアクセス制御を設定します。

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」ボタンをクリックして、次の設定へ進みます。

同じドメインのみ許可する場合は、「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優先か、不許可サイト優先か選択し、「許可サイト」「不許可サイト」それぞれに適切な値/ドメイン名を入力します。
「設定する」ボタン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

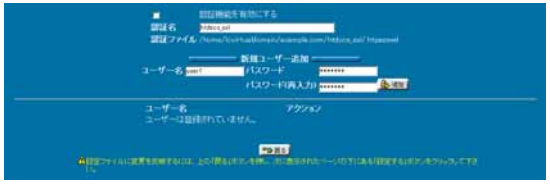
2. セキュア Web サーバー

4. 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。

■ 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」ボタンをクリックします。



「認証名」に認証時、認証ダイアログ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」をそれぞれ入力し「追加」ボタンをクリックします。設定が追加されます。

追加する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。

「戻る」ボタンをクリックし、ディレクトリー覧画面に戻ります。

「設定する」ボタンをクリックして設定を終了します。

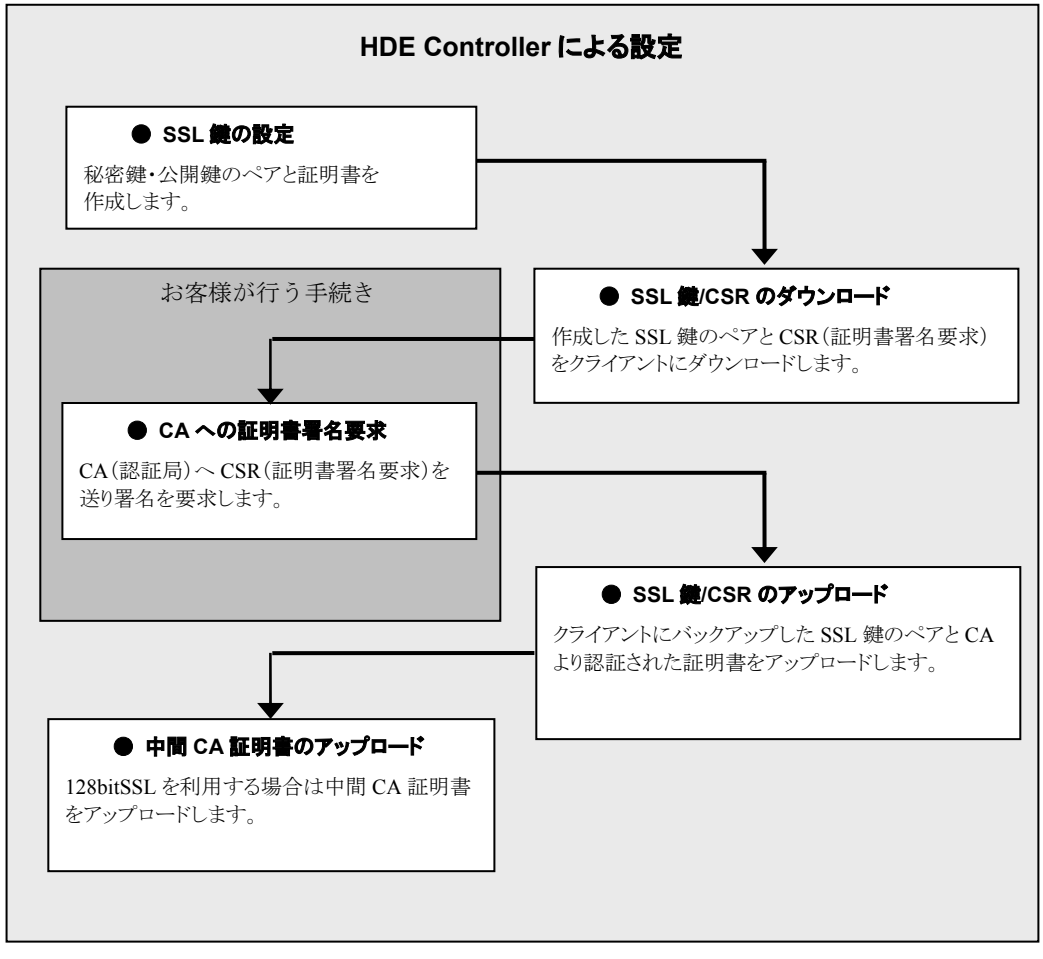
既に認証が設定されているディレクトリについては、ディレクトリー覧画面で、フォルダのアイコンをクリックすることにより認証の有効／無効を切り替えることが出来ます。

5. 鍵と証明書の設定

セキュア Web サーバーの SSL 暗号化の為の秘密鍵・公開鍵の設定を行ないます。

■ 設定の流れ

鍵と証明書の設定の流れは以下のようになります。



2. セキュア Web サーバー

■ 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。

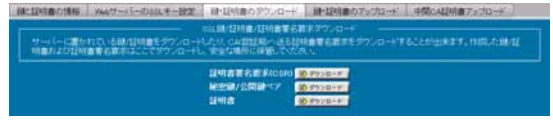
「国名／都道府県名／市町村名／組織名／サーバー名とドメイン名／E-mail アドレス」を正しく入力します。

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

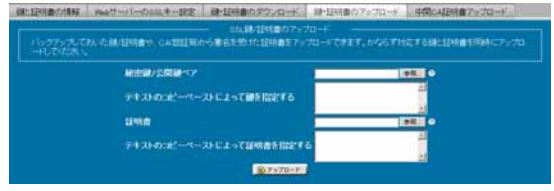
上記の情報を更新します。SSL 鍵のペアと証明書が作成されることはありません。	既に設定されている証明書の情報のみを更新します。
新しい SSL 秘密鍵／公開鍵のペアと、証明書を作り直します。	新規に SSL 秘密鍵／公開鍵、証明書を作成します。初めて設定する場合や証明書を変更する場合は必ず行ないます。
上記の情報を用いて、証明書のみを作り直します。	既に設定されている鍵／証明書情報を元に、証明書のみを作り直します。

■ SSL 鍵/証明書/CSR ダウンロード



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ないます。
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ないます。
「ダウンロード」ボタン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

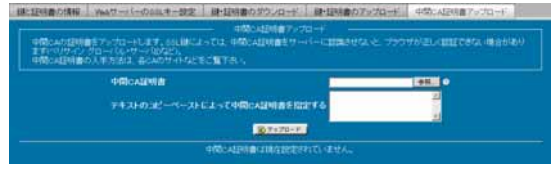


SSL 鍵・証明書をクライアントからアップロードすることができます。
アップロードする鍵、証明書は必ず対応するものを同時にアップロードします。
ファイルの保存されているパスを、「秘密鍵／公開鍵ペア」「証明書」それぞれに入力するか「参照」ボタンをクリックし直接ファイルが存在するディレクトリを指定します。
テキストを直接入力することも可能です。

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な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。
Web ブラウザが正しく認証を行なうために中間 CA 証明書が必要な SSL 鍵の場合、必要になります。
（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）